Illicit Trade and Sanctions Evasion in Strategic Goods: Constructing a Crime Script from Court Documents

Christopher Nelson
Strategic Trade Control Research Group LLC

Abstract

Crime scripts have been used to break down complex criminal acts into sequences of actions and decision points, which used to identify common behaviors and practical intervention points to disrupt crimes in progress. Crime scripts have been employed to study a wide-range of crimes, such as illicit drug trafficking, wildlife poaching, and illegal waste disposal, but not illicit trade in dual-use goods to this point. This study seeks to create a practical crime script using 66 court cases from around the world involving illegal trade in strategic goods and sanctions evasion. Through these open-sources, the crime will be broken down into individual Acts that highlight common decision points that bad actors must consider to successfully complete the crime. These commonalities will be used to highlight global patterns in nuclear-related, dual-use trade and identify key intervention points for providers and authorities to disrupt these attempts. This paper provides a baseline and jumping off point for integrating crime analysis techniques and crime script analysis into strategic trade control enforcement efforts.

Introduction

Aspects of illicit trade have been studied using crime analysis techniques, usually with regard to areas such as narcotics, human, or even wildlife trafficking. In this paper, we seek to apply one crime analysis technique, Crime Script Analysis (CSA) specifically to illicit trade and sanctions evasion related to strategic goods that can support a nuclear weapons program. To do so, we have identified 66 relevant criminal court cases prosecuted around the world from 2003 to 2023. The cases are identified in the appendix of this paper. The openly available court documents from these cases allow us to identify common entity types, actions, and decisions bad actors take in attempting to illicitly trade and evade sanctions on strategic goods. From there, we are able to create a generalized script that can be used by authorities to design targeted disruption strategies to prevent future crimes. To do this we will first introduce the concept of CSA and its benefits. The article will then identify the key pressure points within the illicit trade and sanctions evasion script and describe a selection of them in-depth with examples from the criminal cases. Finally, we will present a few areas for future application of this crime script and recommendations for future research in the area.

Introduction to Crime Script Analysis

CSA seeks to understand a crime through a deliberate enumeration of actions and parties involved in executing the act successfully. CSA is a technique derived from the combined principles of situational crime prevention and rational choice perspective. Situational crime prevention is an approach which holds that crimes can be prevented by understanding, managing, and manipulating the environment in which they occur. The rational choice perspective assumes that an actor will undertake a cost-benefit analysis at each decision-making point and proceed to choose the option that provides the greatest benefit for them. D.B. Cornish was one of the forerunners in applying

these combined approaches to crime analysis in the form of CSA (Cornish 1994). This approach holds that

Crime scripts help us detail "how decisions that an offender makes are influenced by other decision-making across the activity and how the activities of an individual is associated with that of another because of the roles that each perform" (Chainey and Berbotto 2021). The end product of CSA is a set of scenes that provide standardized paths of decisions and actions to be taken, which can be filled in with available information throughout an investigation. Doing so not only highlights areas where bad actors need to make key decisions, which lead us to identification of disruption points in the crime.

Crime scripts need to be broad enough to encompass the broad scope of potential actions involved in a particular crime, but narrow enough to focus on a specified "theme" of an offense. In other words, a script is not useful if it seeks to cover everything, for example trying to create a script to evaluate both drug trafficking and art smuggling. The script needs to be focused on a distinguishable crime to take into account the unique actions that characterize it. A review of current scholarship in CSA shows it applied to drug manufacturing, counterfeit products, arms trafficking, and car theft (see for example, Leclerc and Wortley 2013, Chiu et al 2011). To create a crime script, we want to analyze multiple instances of the particular crime in question and then aggregate common behaviors. This study begins with individual criminal court cases upward toward a general, adaptable script that highlights the major "pressure points" where bad actors need to make decisions or commonly have high-stakes interactions with other parties.

There are no uniform set of steps or rules in creating a crime script, but there are some general practices we will follow. Scripts are divided into major acts that flow from one another. Within each act, there are individual components or actions. These are categorized in more detail, highlighting starting points, actions, decisions, and looping behaviors. This approach helps identify common pressure points that have presented themselves in numerous real-world criminal cases, allowing us to target strategies toward disrupting future instances of illicit trade and sanctions evasion that could lead to nuclear proliferation.

Construction of the Crime Script

For this study, we reviewed the 66 court cases related to contemporary export control and sanctions violations. A benefit of using court documents in CSA is that they are well-structured around the timeline of the crimes, which allows us to begin to distinguish the different acts or phases. Indictment documents are particularly useful in this regard. In the United States, these generally have the following structure:

- Overview of the relevant laws that are alleged to be broken;
- Relevant information about the defendant(s), including citizenship, location, and pertinent connections to other persons and/or entities;
- The conspiracy, which is a high-level summary of the objectives, manner, and means of the crime;
- Overt acts, which walkthrough in detail the commission of the crime; and
- Criminal counts being charged.

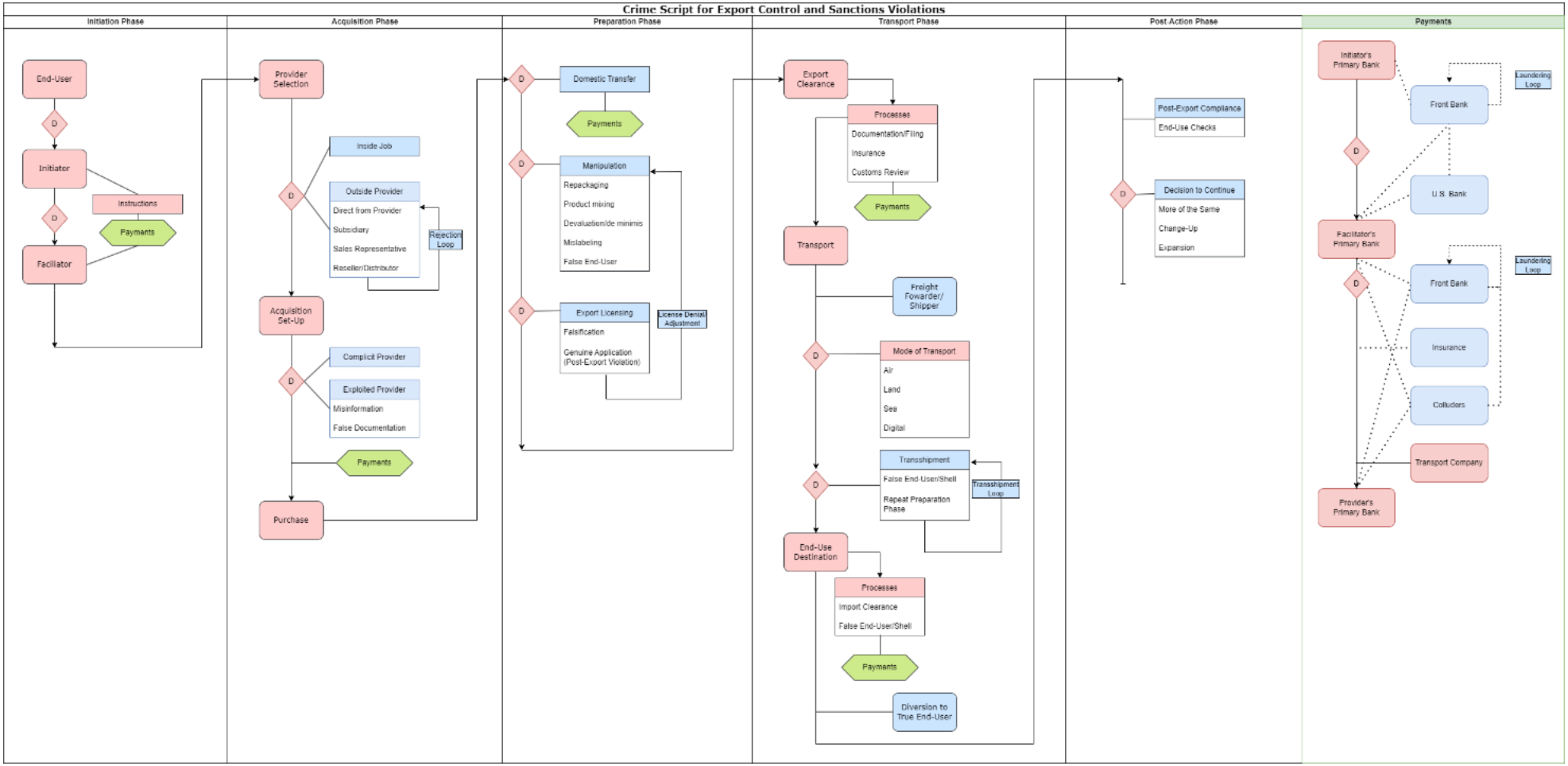
Reviewing each of the cases brought common patterns, pressure points, and actions to the fore. From there, a crime script was created, dividing the criminal act into five consecutive acts, plus a sixth act that occurs concurrently within the others:

I. Initiation Phase
II. Acquisition Phase
III. Preparation Phase
IV. Transport Phase
V. Post-Action Phase
VI. Payments

The full script is included in the figure below.

In the crime script, the red boxes are mandatory pieces of the crime that must be present at some level in an export control or sanctions violation. The red diamonds are decisions that must be assessed by the actors in the crime. For example, in the Preparation Phase, there is a decision point to engage or not to engage in the export licensing process. The blue boxes represent options for the actors. They do not have to choose these options, but they have been taken in some of the cases reviewed for this study. Finally, the green boxes show generally where the Payments actions show up throughout the process. Any international trade transaction involves money transfers and a clandestine, illicit one usually requires a few more payoffs to different entities throughout the process.

For our purposes, the key to the crime script are the pressure points, the decisions and loops within the acts. In situational crime prevention, we want to increase the friction for bad actors at these points, thus increasing the likelihood that they will fail to successfully transfer strategic goods and evade export controls and sanctions. The full list of pressure points in our crime script are below. The rest of this paper will examine just a part of the script, the Preparation Phase, as an example.


Crime Script for Export Control and Sanctions Violations
Initiation Phase
Acquisition Phase
Preparation Phase
Transport Phase
Post-Action Phase
Payments
End-User
D
Initiator
Instructions
D
Payments
Facilitator
Provider Selection
D
Inside Job
Outside Provider
Direct from Provider
Subsidiary
Sales Representative
Reseller/Distributor
Rejection Loop
Acquisition Set-Up
D
Complicit Provider
Exploited Provider
Misinformation
False Documentation
Payments
Purchase
D
Domestic Transfer
Payments
D
Manipulation
Repackaging
Product mixing
Devaluation/de minimis
Mislabeling
False End-User
D
Export Licensing
Falsification
Genuine Application (Post-Export Violation)
License Denial Adjustment
Export Clearance
Processes
Documentation/Filing
Insurance
Customs Review
Payments
Transport
Freight Fowarder/ Shipper
D
Mode of Transport
Air
Land
See
Digital
Transshipment
D
False End-User/Shell
Repeat Preparation Phase
Transshipment Loop
End-Use Destination
Processes
Import Clearance
False End-User/Shell
Payments
Diversion to True End-User
Post-Export Compliance
End-Use Checks
D
Decision to Continue
More of the Same
Change-Up
Expansion
Initiator's Primary Bank
Front Bank
Laundering Loop
D
U.S. Bank
Facilitator's Primary Bank
D
Front Bank
Laundering Loop
Insurance
Colluders
Transport Company
Provider's Primary Bank

Illicit Trade and Sanctions Evasion Crime Script: Pressure Points

Act I – Initiation Phase	Act II – Acquisition Phase	Act III – Preparation Phase	Act IV – Transport Phase	Act V – Post-Action Phase	Payments
Decision A – Undertaking the Crime	Decision A – Provider Selection	Decision A – Domestic Transfer	Decision A – Mode of Transport	Decision A – Continuation, Expansion, or Change-Up	Decision A+B – Use of Front Banks
Decision B – Facilitator Selection	Decision B – Exploitation or Co-option	Decision B – Manipulation	Decision B – Transshipment		Money Laundering Loop
	Provider Rejection Loop	Decision C – Export Licensing	Multiple Transshipment Loop		

Pressure Points Discussion for Act III

Act III comprises three optional decisions. These are all related to different methods that are used to prepare the strategic goods for a "successful" illicit transfer. At this point, the goods have already been purchased from the provider. As such, each of the Act III decisions involve ways to reduce or deflect scrutiny by State authorities in advance of the physical export of the goods.

Decision Point III-A

Some bad actors decide to have the strategic goods physically transferred to them or a front/shell company after they make the purchase from the Provider and before they export. This gives them physical control of the product and a layer of separation between them and the Provider. With a domestic transfer, the Facilitator may be able to deceive the Provider into thinking there is no export planned at all, reducing their due diligence inquiries. Physically controlling the goods before export also allows for some other manipulation steps contained in Decision Point III-B, such as repackaging and product mixing.

One interesting example of these domestic transfers is seen in the somewhat unique case of Access USA Shipping. Over a two-year period from 2011 to 2013, Access USA allowed foreign customers to purchase export controlled strategic goods from U.S. Providers without them knowing that they were intended for export. Access USA actually facilitated Decision Point III-A for dozens of bad actors by providing them with a physical address in the United States where commodities could be delivered, manipulated by Access USA staff, and exported in a manner to evade U.S. customs authorities. Access USA presented itself as a front for non-U.S. purchasers, hiding funding from non-U.S. sources and using contact information for their CEO as the false U.S.-based customer and end-user. They ended up settling with U.S. Department of Commerce, Bureau of Industry and Security for US$27 million over 129 counts of export control evasion involving purchasers in at least 32 countries.

Decision Point III-B

This decision point revolves around the optional steps that bad actors might take in hiding the strategic goods in plain sight among the broader flow of exports. While there are others, most of the methods seen in the cases reviewed for this study fall into the following groups:

Repackaging. This involves the Facilitator or one of their agents taking possession of the strategic goods before export and altering or completely redoing the packages they came in. This tactic involves any step to alter the physical appearance of the products to obfuscate the true nature of their contents during the export and transport process. This can involve removing descriptive labels/pictures of the product, brand names, or any other identifying details. It might also include putting the goods in another packaging with no or false identifiers.

Product Mixing. Another tactic is to mix the strategic goods with similar, non-strategic components. For obvious reasons, this is most effective when dealing in controlled or restricted commodities that are shipped in high volumes, such as electronic components or metals. Hiding a small amount of strategic goods among non-strategic goods is a useful tactic to frustrate attempts at in-depth customs inspections of cargo.

Devaluation/De Minimis. Bad actors understand that most customs authorities build their reporting requirements and audit procedures around a minimum value which is based on exporter self-reporting. While not foolproof, this is a relatively simple exploit that is used not only in export control and sanctions evasion, but nearly all forms of illicit trafficking, particularly to minimize taxes and tariffs on goods. In the United States, for example, if a commodity is valued at under US$2,500 then no Electronic Export Information (EEI) filing is required. EEIs are submitted to the Automated Export System, which allows U.S. authorities to monitor and track exports of goods. Electronic Export Information forms are required to be filed when: (i) an item required an export license; (ii) was bound for an embargoed country; or (iii) the value of the item(s) was greater than $2,500 (U.S.). While filing an EEI is required no matter what the value if the commodity requires an export license, if the bad actor is going to ignore license requirements anyway, they might seek to devalue the goods as well to further reduce the paper trail related to their transactions. Devaluation of products further reduces the risk of being flagged or stopped by customs authorities. Significantly, devaluation changes the profile of strategic goods shipments from a data perspective; most strategic goods are shipped in lower volumes at higher values than their non-strategic counterparts. Devaluing shipments on shipping documentation has the dual “benefit” either avoiding the export reporting requirements altogether or making the shipment blend in with the typical profile of non-strategic goods.

Mislabeling. Similar to devaluation, mislabeling is a common practice involving altering the descriptive fields on export documentation that identify the product. This can involve altering the commodity description or the HS code the products are classified under. Both of these fields are self-reported by the exporter, giving a bad actor ultimate flexibility to deceive authorities as long as they are willing to take the risk of getting caught. In our court case examples, mislabeling is typically done by making the product description “in the neighborhood” of the strategic goods without invoking any of the characteristics or technical thresholds that would advertise their potential to be controlled. Since many dual-use products are controlled due to their technical thresholds or material composition, which are not readily visible to the human eye, they can be easily mislabeled to pass basic inspection.

False End-User. The declaration of a false end-user for the products is one of the most prevalent forms of deception in export controls and sanctions violations. This trend extends to export documentation as well. A false end-user could be a different entity in the same destination country, an entity in a different destination country, or a fabricated front/shell company. The purpose of this tactic is to indicate that the shipment is going to an end-user that does not exhibit any concerns from

the authorities' perspective. Listing a trading or shipping company as the ultimate consignee on an export license or declaration has been noticed, although not consistently, by customs authorities leading to interdiction or seizure. Bad actors will also use this approach to ensure the designated end-user is not an entity on any denied parties or sanctions list, which would be a major red flag.

Any of the above methods of deception are common and often used in conjunction with one another. The 2017 case of U.S. v. Chen illustrates many of these behaviors in action, including a domestic transfer from Decision Point III-A. Si Chen, aka "Cathy Chen," acted as Facilitator on behalf of unspecified Chinese end-users to acquire U.S. origin microwave components, traveling wave tubes, low noise amplifiers, and digital-to-analog converters, all subject to U.S. export controls. In doing so, Chen used altered documentation to rent an office in the name of Archangel Systems Space, Inc. (ASSI) in California. She purchased controlled components from U.S. Providers and had them transferred domestically to ASSI's address, which was really Chen's residence. On physically acquiring the goods, Chen exported them to Hong Kong for eventual transshipment to China. In the shipping documentation, she mislabeled and devalued the goods. For example, in one shipment, she falsely valued an export of microwave components worth US$25,778 as only worth US$100 and did not file an EEI with U.S. Customs. She also provided a false end-user in Hong Kong to facilitate the illicit export. In another case, Chen removed six stickers from the packaging of U.S.-origin digital-to-analog converters that indicated that the package was subject to U.S. export controls and required a license to ship. Overall, based on the criminal indictment, Chen facilitated her export control evasion using repackaging, devaluation, mislabeling, and false end-users - and her efforts were repeatedly successful. Chen was able to conduct at least four shipments valued at over US$100,000 before she was caught and sentenced to 46 months in prison.

Decision Point III-C

The final decision point in Act III is whether or not a bad actor wants to engage with the export licensing process in a State. There are many factors that go into this decision:

- Is there a presumption of license denial for the product to the stated destination country? If so, any engagement with the licensing process would need to identify a credible false end-user in another country and arrangements for illicit transshipment need to be made.
- Is an export license for the product to the end-use country likely to be approved? If so, getting a license for the shipment might be beneficial. Using a false end-user in the end-use country might get the product there and then it can be illicitly transferred to the true end-user.
- Does the facilitator have a credible front/shell entity in an export "friendly" country? If so, an export license may be beneficial as well. The licensed export to the intermediary country could then be re-exported to the true end-user.
- Is there a need to keep all entities and relationships in the transaction a secret? If so, there should be no attempt to engage with export licensing and the detailed documentation required.

Receiving an export license is a major boon to the potential success rate of the illicit transaction. With an export license, the products can legally leave the country of initial jurisdiction, reducing a great deal of the potential complications and deceptions involved with this step. In fact, the crime becomes a diversion after the fact. An export license is not a blanket agreement to allow the export of strategic goods - it is specific to the declared end-use destination and end-user for the specified

end-use. The crime comes in when these stated facts are subverted to transfer the goods to the true end-user. In most of the cases reviewed for this study, bad actors decided not to risk the export licensing system of the Provider State.

We can look at the Tokyo Boeki case in Japan as an example of where there was an export license sought. In 2008, North Korean officials directed one of their Chinese-based fronts, New East International, to use their Japanese contacts to acquire magnetometers for use in their missile guidance systems. New East International is on Japan's restricted end-users list for their ties to North Korea, so evasion was required. Tokyo Boeki was contacted to facilitate the transaction by purchasing the magnetometers through Taikyo Sangyo. They filed an export license to ship the controlled goods to a false end-user in Myanmar with transshipment through Malaysia. In effect, the export license removed any overt ties between the export and entities with connections to the North Korean missile program. Ultimately, this attempt was not successful as the companies in Myanmar who arranged parts of the transaction had known ties to the North Korean government as well. The shipment was ultimately seized by Japanese customs. Rather than fully subvert the system, Tokyo Boeki tried to play just outside of the rules and were ultimately caught.

Recommendations

This article only contains a small part of the insights and examples from the creation of this crime script. Our goal for future research is to identify specific disruption strategies that target each of the pressure points in the script. By increasing friction here, we can increase the chance that attempts at illicit trade and sanctions evasion will be detected, interrupted, or at a minimum, be more difficult to execute. Some top-level strategies have been identified thus far and are divided into provider focused and authorities focused as follows:

Provider Focused

- Developing a robust, standard definition of due diligence;
- Creating a provider self-assessment of illicit trade and sanctions evasion risk;
- Securing the distribution/subsidiary supply chain;
- Record keeping and data management; and
- Information sharing and tip-offs to authorities.

Authorities Focused

- Modus operandi identification and deployment of resources;
- Data collection strategies; and
- Revamped and targeted outreach efforts.

Another key recommendation is for interested parties to continue to examine illicit trade in strategic goods and sanctions evasion from different perspectives that have shown promise in other areas. Crime analysis in general, and CSA in particular, have been used effectively to develop preventive situational crime mitigation strategies in many other areas. Researchers confronting the danger of illicit trade in strategic goods for nuclear end-uses should continue to draw from other areas of research, such as crime analysis, social network analysis, open-source intelligence, and more.

References

Chainey, Spencer Paul and Arantza Alonso Berbotto, "A structured methodical process for populating a crime script of organized crime activity using OSINT," *Trends in Organized Crime* 25 (2021): 272 - 300.

Chiu, Yi-Ning, Benoit Leclerc, and Michael Townsley. "Crime Script Analysis of Drug Manufacturing in Clandestine Laboratories: Implications for Prevention," *The British Journal of Criminology*, Vol. 51, Issue 2, March 2011.
Cognition and Crime: Offender Decision Making and Script Analyses, Edited by Benoit Leclerc and Richard Wortley, Routledge, 2013.
Cornish, D. B., "The procedural analysis of offending and its relevance for situational prevention," in *Crime prevention studies Volume 3*, edited by R.V. Clarke. (Monsey: Criminal Justice Press, 1994).

Appendix

Case Name	Prosecution Country	End-Use Countries	Case Number(s)	Year
Frosch	Austria	Iran	Unknown	2012
AAE Chemie Trading et al	Belgium	Syria	Unknown	2019
Deland et al	Canada	UAE, Columbia	2020 QCCA 655	2020
Lee Specialties	Canada	Iran	Unknown	2014
Yadegari	Canada	Iran	2001 ONCA 287	2011
Jilin Tumen Chemical	China	North Korea	Unknown	2006
Zibo CHEMET Equipment Company	China	Iran	Unknown	2008
Afrasiabi et al	Germany	Iran	C-72/11	2011
Alexander J	Germany	Iran	Unknown	2021
Rudolf M et al	Germany	Iran	Unknown	2013
Mitutoyo Corporation	Japan	Iran, Malaysia, Libya, China, Vietnam	Unknown	2006
Toko Boeki	Japan	North Korea	Unknown	2009
Tokyo Vacuum et al	Japan	North Korea	Unknown	2008
Rechtbank Noord	Netherlands	Saudi Arabia, Russia	15/994176-17	2017
Slebos	Netherlands	Pakistan	14.038044-04	2005
Venlo Euroturbine	Netherlands	Iran	Unknown	2019
Chaandrran	Singapore	Syria	DAC 57653/2005, MA 183/2006	2006
Fluval Spain SL	Spain	Iran	Unknown	2013
ONA Electroerosion SA	Spain	Iran	Unknown	2014
Delta Pacific Manufacturing	United Kingdom	Iran	Unknown	2014
Knight	United Kingdom	Kuwait	Unknown	2007
NDT Mart	United Kingdom	Iran	Unknown	2010
Nik et al	United Kingdom	Iran	Unknown	2009
Pouladian-Kari	United Kingdom	Iran	2011/07118	2013
Salashoor	United Kingdom	Iran	Unknown	2008
Ali	United States	China	2:16cr00142	2016
Astafanos et al	United States	Egypt	1:13mj00851	2013
Bahram Mechanic et al	United States	Iran	4:15cr00204	2015
Baier et al	United States	UAE	1:21cr00577	2021
Bo	United States	China	1:19cr00400	2019
Brazhnikov	United States	Russia	2:15cr00300	2015
Caby et al	United States	Syria, China	1:16cr20803	2016

Chen	United States	China	2:17cr00254	2017
Cheng et al	United States	Iran	1:13cr10332	2013
Fishenko et al	United States	Russia	1:12cr00626	2012
Fokker Services B.V.	United States	Iran	1:14cr00121	2014
Gohman et al	United States	Russia	2:21cr00259	2021
Green Wave Telecommunication et al	United States	Iran	0:15cr00329	2015
Hamade-Berro	United States	Lebanon	0:15cr00237	2017
Hashemi-Khan	United States	Iran	2:19cr00254	2019
Huang	United States	Iran	1:20mj00225	2020
Kafrani-Mirnezami	United States	Iran	1:21cr00501	2021
Kaiga	United States	Iran	1:13cr00531	2013
Kanev	United States	Russia	1:17cr00018	2021
Kazhdan	United States	Russia	0:22cr60060	2022
Keshari et al	United States	Iran	1:08cr20612	2008
Khan	United States	Pakistan	Unknown	2003
Kral Aviation-Larijani	United States	Iran	1:15cr00053	2015
Mustafaev et al	United States	Russia	3:22cr00110	2022
Orekhov et al	United States	Russia, China	1:22cr00434	2022
Qin et al	United States	China	1:18cr10205	2018
Ramor Dis Ticaret, Ltd. et al	United States	Iran	2:17cr00122	2017
Rohollahnejad	United States	Iran	1:19cr00073	2019
Roth	United States	Iran	3:08cr00069	2008
Sepehri-Shayan	United States	Iran	1:16cr00081	2016
Sery	United States	China, India, Taiwan	3:21cr02898	2021
Shih-Mai	United States	China	2:18cr00050	2018
Sudarshan et al	United States	India	1:07cr00051	2007
Tsai	United States	North Korea	1:12cr00829	2013
Ugur	United States	Turkey	1:21cr10221	2021
Wei	United States	Iran	1:14cr00144	2014
Xian-Li	United States	China	1:10cr00207	2010
Yip et al	United States	Iran	5:11cr00516	2011
Yu	United States	China	6:16cr00023	2016
Yu-Lee	United States	China	1:20mj08202	2020
ZTE Corporation	United States	Iran	3:17cr00120	2017