Intelligence

STRATEGIC BORDER THREAT ASSESSMENT 2023

RELEASED UNDER THE OFFICIAL INFORMATION ACT 1982

NZ Customs Strategic Intelligence
6(c) [redacted]
December 2023

This document is the property of the New Zealand Customs Service (NZ Customs) and is classified as ~~RESTRICTED~~. No reclassification, duplication or dissemination of this document, or the intelligence it contains, can occur without express permission of the Manager, Intelligence, NZ Customs. This intelligence is to be deleted/destroyed once it has been used for the purpose for which it was produced.

Foreword

Kia ora kou tou

I am pleased to present the Strategic Border Threat Assessment 2023 (SBTA), New Zealand Customs Services' (NZ Customs) overarching strategic intelligence assessment. Unlike other countries, the Immigration and Customs functions in New Zealand are operated by separate agencies, and as such, this assessment focuses primarily on threats under the remit of NZ Customs.

Strategic Intelligence has previously produced an annual assessment of significant risks that may impact NZ Customs in the following one to two years, however this is NZ Customs' first attempt at a true SBTA. The data is based on the calendar year 2022 but pulls in trends from across four years (2019-2023). The SBTA has been written in a period post COVID-19, where the focus has been on economic recovery. Many of the threats identified are well known and remain priorities for the New Zealand Government.

New Zealand's geographical location and large maritime domain is both a hindrance and a help. It assists with protecting our borders from illicit actors trying to access our market/population due to the delay it provides in the introduction of people and goods to our country. It is also a hindrance as our maritime domain is repeatedly exploited by drug traffickers and requires more resources to mitigate increased threats. Our extended supply chains are also at threat from interruption and interdiction by illicit actors.

Illicit actor infiltration of legitimate supply chains will be an ongoing issue as the threat caused by trusted insiders becomes more prevalent. Threat actors are also able to obfuscate their activities amongst the high volumes of legitimate trade, which can be expected to increase in the next three to five years. This will lead to resource pressures if traditional approaches to compliance are used to identify illicit activity.

While large scale illicit drug importations continue to make headlines, the risk to New Zealand also covers mid-tier to lesser-but-frequent importations across a range of border risks, which completes the NZ threat landscape. This means that all streams are susceptible to being used in attempts to circumvent Customs controls, requiring NZ Customs to work smarter to counter the various threats.

Developing deep and enduring partnerships with industry partners will benefit both commercial outcomes and border security. Accessing information and capabilities available to private enterprises may also improve our ability to detect and respond as threat actors shift their methodologies.

This initial assessment is a foundational one and as such is a lengthy document, while establishing this as a baseline it is anticipated future iterations will be able to be condensed and be more focussed.

The SBTA reflects significant subject matter expertise, analytical rigour, and comprehensive consultation. I would like to thank my staff for their commitment to identifying and understanding the threats to the New Zealand border, and our partner agencies who have contributed to this assessment.



Bruce Berry
Manager Intelligence
New Zealand Customs Service

RELEASED UNDER THE OFFICIAL INFORMATION ACT 1982

Contents

Foreword 2
Introduction 4
Threat Ratings 4
Strategic Context Themes 5
Key Judgements 7
Illicit Goods Movement 10
Illicit Drugs & Precursors 10
Firearms/Parts and Other Weapons 16
Objectionable Material 20
Intellectual Property Rights 23
Hazardous Goods 26
CITES (Convention on International Trade in Endangered Species) 29
Revenue & Illicit Value Movement 31
Revenue/Economic Threats 31
Illicit Money and Value Instruments Movement 35
National Security 40
Terrorism & Extremism 40
Strategic & Proliferation-related Goods 44
Special / Supplementary Topic 47
Cyber-enabled Threats 47
Threat Rating Methodology Explanation 52
Threat Scoring Method 53
Intent and Capability Survey Statements 53
APPENDIX A 58

RELEASED UNDER THE OFFICIAL INFORMATION ACT 1982

Introduction

The purpose of the Strategic Intelligence Strategic Border Threat Assessment (SBTA) 2023 is to inform policy makers and leadership with key strategic intelligence and insights to assist in decision-making and to aid the development of strategic direction, programs, policies and legislation in order to achieve long-range NZ Customs' objectives.

The SBTA assesses the key threats and threat actors targeting the New Zealand border and their associated illicit activities in 2022. The threat assessment uses data, information, and intelligence comment for the year 1 January to 31 December 2022, updated by events and information in 2023 as appropriate. It examines threat actor intent and capability (see below) and uses this to inform the three year Outlook as to what NZ Customs might expect to see.

The threat categories are rated and ranked according to a survey process, which provides analytical rigour and consistency to the process of threat assessment. The survey statements used to assess the drivers and factors influencing threat activity can be found in the *Threat Rating Methodology Explanation.* The survey process is supplemented by further analysis and informed comment in the body of each threat section. Each section includes an Outlook which assesses and anticipates the direction of the threat in the following one to two years. Each Outlook will be reviewed, adjusted, and updated year on year as further analysis is undertaken.

Threat Ratings

The threat rating methodology is outlined in *Threat Rating Methodology Explanation*. Arrows indicate threat rating changes from the previous SBTA. NC is No Change in the rating. New threat topics are denoted by NEW.

Illicit Drugs & Precursors	6(c) [redacted]
Revenue/Economic Threats	
Strategic & Proliferation-related Goods	
Objectionable Material	
Terrorism & Extremism	
Firearms/Parts and Other Weapons	
CITES	
Hazardous Goods	
Illicit Money and Value Instrument Movement	
Intellectual Property Rights	
Cyber-enabled Threats	

Threat is defined as the current and future assessed *intent* and *capability* of actors undertaking deliberate non-compliant activity that is likely to impact strategic and operational objectives of NZ Customs.

> ***Intent*** *is a function of the assessed desire and confidence of deliberate non-compliant actors.*
>
> ***Capability*** *is a function of the resources and knowledge available to these actors.*

The SBTA is a threat assessment. The SBTA *not* a risk assessment since risk is a function of the interaction of hazard frequency and impact (denoted by likelihood and consequence).

[1] This rating is assessed by MFAT and is used in the HINT Joint Strategic Threat Assessment (JSTA).
[2] This rating is assessed by NZ Customs only and is not the combined NZCS-MBIE rating used in the HINT JSTA.

RELEASED UNDER THE OFFICIAL INFORMATION ACT 1982

Strategic Context Themes

- **Geopolitical, climate and global economic (post-pandemic) issues impact threat actors at New Zealand's border.**
  Geopolitical developments in the Pacific and Asia, and in a global context, will impact on illicit commodity trafficking and threat actor activity across New Zealand's (NZ) border. Not only will Organised Crime Groups (OCGs) exploit any opportunities afforded by countries to promote their own interests in Asia and the Pacific, 6(a) [redacted] The developing strategic context in Asia and the Pacific and shifts in economic power mean NZ will unlikely avoid being targeted by some countries, 6(a) [redacted] or a variety of threat actors keen to exploit these factors. Additionally, economic uncertainty and global recession will exacerbate some threat activity against NZ, influencing people into illicit activity and driving threat actors to see NZ as a profitable illicit goods selling market. Climate change impacts may drive some similarly into illicit activity, most immediately and near in Asia and the Pacific.

- **Climate change impacts and the 'greening' of technology and products will begin to impact on imports and exports.**
  Climate change responses, environmentally responsible manufacturing and consumerism, and energy saving technologies will drive 'green' or environmentally friendly technology and product requirements for NZ. These will likely impact what NZ permits as legal imports and exports. Older, obsolete and less 'green'-compliant goods will require disposal, likely resulting in attempts to export scrap, hazardous, redundant, and non-compliant goods illicitly. Import checks may also be required to prevent unwanted products, including banned products, from entering NZ.

- **The Pacific region and Pacific Island Countries (PIC) are a close and evolving threat environment.**
  The Pacific region is a well-established vector for funnelling threat commodities from other regions to NZ. But commodity threat actors are using the PIC more as both transit points and bases to target NZ. The Pacific, and PIC themselves, are a difficult region to maintain a border agency watch over, and there are many pathways and methods for commodity trafficking through them. 6(c) [redacted] outlines the variety of threat actors and activity operating in PIC and also highlights new potential threat activity and vectors NZ will likely need to monitor. Developing geopolitical and climate change issues, as well technological uptake (e.g. internet, digital currency) in PIC over the next five years, will likely be exploited and drive more threat activity in PIC themselves.

- **Greater OCG and Transnational Organised Crime (TNOC) group connectivity and activity is occurring in NZ, Pacific and globally.**
  OCGs continually attempt to widen and secure their influence both domestically and overseas, expanding into new markets and territories wherever they can. Some New Zealand-based OCGs, Outlaw Motorcycle Gangs (OMCGs) and NZ Adult Gangs (NZAGs) are establishing chapters overseas, most recently in Europe and the Pacific.

- **The professionalisation of organised criminal activity is progressively occurring.**
  OCGs and TNOC groups have implemented an era of outsourcing and leveraging skilled facilitators to assist them in commodity trafficking and managing the illicit funds generated. OCGs/TNOC groups are making more concerted efforts to utilise trusted insiders in supply chains, border facilities and other professions, and to employ the skills and services of a

RELEASED UNDER THE OFFICIAL INFORMATION ACT 1982

wide range of professional facilitators, sometimes used unwittingly. TNOCs are run like modern businesses, advertising, manufacturing and supplying products, outsourcing requirements where they do not possess in-house capability, employing strategic planning and conducting sophisticated financial management programmes.

- **Threat actors increasingly leverage technological developments, often faster than border agencies.**
  New technology developments, especially with dedicated encrypted communication devices (DECD), tracking equipment, and in the cyberspace, are adopted and utilised by threat actors much quicker than Law Enforcement Agencies (LEAs). While not all threat actors use the latest technology, and some fail to use it successfully, LEAs are always confronted with some OCGs and threat actors that are one step ahead in their technology use, enabling them to consistently defeat border systems and scrutiny. With ever more technology being developed and refined, threat actors always have some innovation they can adopt and adapt to assist them, which LEAs then have to identify and respond to.

- **New Zealand's geographical location and large maritime domain both assist in border protection but also offer threat actors opportunities for illicit activity.**
  New Zealand has no land borders to be exploited, and its distance from most other nations causes some difficulties for threat actors operating here. However, its long coastline, total reliance on air and marine traffic, and close proximity to PIC and its goods and passenger pathways provide threat actors with many avenues to use for illicit activity. In particular, NZ's maritime domain is repeatedly exploited by drug traffickers, while air travel and freight provide further avenues to import, and export, a wide range of illicit goods. In a modern world of global travel and freight supply NZ's distance from markets provides no barrier to threat actors.

- **The global growth of online shopping, and freight and mail services set up to expedite supply, is exploited not only by illicit commodity traffickers but also by consumers and businesses**. Consumers can source their own illicit goods quickly and from many places, businesses are able to exploit freight volumes and border processes expediting fast delivery to commit fraud, and organised criminal threat actors are able to source and supply illicit goods quickly from many places using large volumes of freight, fast freight and mail to conceal their activities.

- **Drug and tobacco consumption and pricing trends in NZ are attractive to traffickers and provide lucrative opportunities for exploitation.**
  New Zealand has well-established drug and tobacco consumption markets using many products. Drug use is expanding across more products and increasing for some main drugs, and tobacco consumption in several forms, including vaping, is unlikely to disappear entirely. Threat actors are likely to continue exploiting the strong profitability potential of both markets.

RELEASED UNDER THE OFFICIAL INFORMATION ACT 1982

Key Judgements

- **Border drug activity is constantly changing, with ever higher quantities of methamphetamine, cocaine, GBL (gamma-butyrolactone) and MDMA (Methylenedioxymethamphetamine) arriving in varying consignment sizes and from a greater variety of source and transit countries than before, and increasingly imported by consumers themselves.** A steady stream of lower quantity drugs (e.g. synthetics, PIEDs) as well as more new drugs are arriving, mostly consumer-acquired, including fentanyl and other opioids. Import quantities exceed consumption trends, indicating that stockpiling, close-to-market supply models, market price manipulation or other dynamics (including some exporting) are likely also occurring.

- **Drug trafficking OCGs are leveraging more sophisticated techniques and technologies, as well as outsourcing and professionalising activity that helps facilitate trafficking and drug profit management.** While many consumers or opportunists importing small drug quantities use low sophistication methods to attempt to evade border regulations, OCGs use a wide variety of more sophisticated import methods, some well-known and others not seen before. OCGs are increasingly leveraging a range of supply chain and professional facilitators, including more common use of trusted insiders, and employing new technologies, including encrypted communication devices (DECD) and social media platforms, sophisticated concealment methods, GPS locators and tracking devices, and some cyber-enabled crime techniques.

- **Illicit parts importing, more than smuggled firearms, is the most likely increasing firearms threat in the next few years.** These will mostly be parts difficult to obtain, or are unobtainable, domestically, and many will likely be upgrade parts, accessories, and conversion kits. Personally-made firearms (PMF) manufacturing is not noted in NZ. However, overseas LEAs report increasing firearms conversion and PMF manufacture, and it is possible NZ-based threat actors unable to obtain firearms otherwise will import parts to accessorise domestically-obtained firearms or to make PMFs. 3D-printed parts, imported and domestically made, are a common element in PMFs overseas, and are also used in many other firearm types, and will almost certainly increase in NZ. The mid- to long-term future of illicit firearms importing will largely depend on whether grey and black markets, and other domestic sources, sufficiently meet illicit firearms demand. The new Firearms Registry intends to make firearms diversion to criminal actors more difficult, which could result in threat actors sourcing more firearms overseas or assembling their own.

- **Although overseas trafficking of Convention on International Trade in Endangered Species of Wild Fauna and Flora (CITES) goods is significant and hugely lucrative, activity across NZ's border mostly results from occasional non-compliance, much of it unintentional or careless.** Organised criminal activity is low, and includes infrequent instances of small-scale wildlife exporting, but unintentional non-compliance on imports is the biggest threat. However, there is no shortage of international websites to order CITES goods from and social media avenues that facilitate supply, and online importing is a quick and easy way for all threat actors to import goods, mostly arriving in mail and air freight.

- **Revenue evasion is a top border threat, especially as the government prioritises economic recovery, but it is mostly undertaken by individuals and businesses rather than by organised criminal actors.** Much of it is hard to identify, goes undetected, or is low level and written off. Threat actors right across the spectrum, from large businesses to small importers/consumers, will continue to be driven by high profit-making or cost-saving

RELEASED UNDER THE OFFICIAL INFORMATION ACT 1982

potential, much of it achieved by relatively simple revenue evasion techniques (e.g. misdeclaration, undervaluation, misdescription). The pandemic years and recent economic downturn have only entrenched and sharpened this intent. Some commercial threat actors will also continue to leverage or exploit professional services/methods to help reduce large revenue payments. However, the amount of revenue evasion occurring with lower volume importers and individual consumers is likely to be a substantial portion of overall evasion.

- **Cash, precious metals and high value goods, both manufactured and raw, are increasingly seen crossing the border, to move and launder illicit funds, including to and from PIC.** It is often difficult to distinguish money laundering movements from those of other threat actors moving money for personal or business reasons (e.g. tax evasion). The introduction of the Financial Crime Unit (FCU) has improved intelligence and investigations experience in recent years, however money laundering offences take significant amounts of time and evidence to prove. Threat actors, using both simple and sophisticated methods to disguise and move illicit cash, with some OCGs also utilising professional facilitators to assist, are still able to continue operating successfully and present an ongoing challenge for NZ Customs and partner agencies.

- **The objectionable material threat at the border mostly occurs with physical imports on digital devices, and most of this is sex-related material.** There is little violent extremism or terrorism material detected. Travellers arriving from PIC with child sex exploitation material (CSEM) on digital devices will possibly increase following a reported rise in child exploitation material (CEM) activity in PIC in recent years.

- **Small-scale commercial intellectual property rights (IPR) infringing imports will continue to arrive and will account for most seizures.** A significant quantity of IPR-infringing goods will likely also be imported by private (internet) consumers for personal use, with little prospect of interdiction.

- **Most hazardous goods illicit importing and exporting activity will continue to result from erroneous, careless or uninformed non-compliance.** Imports of cheaper, substitute, or substandard goods containing hazardous materials or that fail NZ safety and/or health standards will continue to occur, especially if there are supply shortages of similar goods. Threat actors will also likely exploit domestic requirements to introduce expanding ranges of climate-change and environment-friendly technologies and goods to replace older products. This includes attempts to illegally export obsolete and non-compliant goods and technologies that require permits.

- **Increased global online connectivity between Motivated Violent Extremists (MVE), supporters and sympathisers has likely elevated the extremist travel and goods threat across the NZ border over the next 1-3 years.** Faith-Motivated Violent Extremists (FMVE) and Identity-Motivated Violent Extremists (IMVE) are currently the predominant extremist ideology threat actors encountered at the border. However, recent heightened domestic interest in several controversial issues that appeal to MVE activists and supporters could result in the attention and arrival of international sympathisers, speakers and protest advocates who promote violent activity.

- **Technology and research targeting by state and non-state actors, mostly to gain economic advantage but including some dual-use goods also, is a high threat to NZ's security and economy.** New Zealand continues to develop and manufacture innovative and cutting-edge technologies (e.g. rocket/aviation technology, food/agricultural products, electronic goods) that are attractive to strategic goods and knowledge threat actors,

RELEASED UNDER THE OFFICIAL INFORMATION ACT 1982

increasing both foreign attention and illicit removal activity. 6(a) [redacted] Global crisis events, such as the pandemic and Ukraine war, may create goods supply shortages and difficulties elsewhere that could be potentially alleviated by accessing NZ goods, especially if NZ is perceived to be less vigilant than other countries.

- **Cybercrime and cyber-enabled threat actors will continue attempting to penetrate border-related systems to compromise and disable core networks, gain access to information, or exploit access to move goods or people illicitly across the border.** Supply chain systems penetration will occur, both from external threat actors and trusted insiders, to track, hide, disguise, relocate and move goods, and to gain privileged or restricted access to border-related supply chain systems or facilities. Attacks on border systems under direct NZ Customs control can also be expected as they become more accessible digitally, automated, and utilise biometrics.

RELEASED UNDER THE OFFICIAL INFORMATION ACT 1982

Illicit Goods Movement

Illicit Drugs & Precursors

Threat Rating	6(c)

Organised drug threat actors continue to traffic and import drugs and precursors. It is almost certain threat actors will import high drug volumes, and possibly more types of drugs. It is almost certain threat actors will continue to exploit mail and fast freight streams, to facilitate regular small-scale imports (as has occurred in recent years), to use trusted insiders, and to expand their trafficking capabilities.

Intent

- Threat actors, especially OCGs, maintain high intent to use sea and air cargo to import prohibited substances, and it will be strengthened with the almost certain return of air couriers as air routes open.
- Threat actors exhibit increased intent by the increasing use of regular small-scale imports, especially from Europe, increasing volumes and drug types imported from Africa, and more attempts to use trusted insiders.

Capability

- Mexican OCGs have expanded illicit drug production and trafficking capabilities to many global destinations.
- African-related OCGs' trafficking capability has increased, shown by growing drug production, expanding transport/supply routes through Africa, and rising use of air fast freight and mail streams to NZ. Increased capability includes trafficking multiple drug types across Africa, African manufacture of some drug types, exporting from several African nations, and using encrypted communications and many concealment methods.
- NZ-based OCGs are also exploiting drug knowledge provided by 501 deportees returning from Australia to NZ and continue to develop their overseas presence and/or associations.

OUTLOOK AND OPPORTUNITIES SUMMARY

1. Threat actors will continue importing increasing amounts of drugs from and through a widening number of countries across the world. In particular, methamphetamine, as well as cocaine and other drugs, will arrive from Europe, and through Africa and the Middle East. Attempts to increase illicit fentanyl imports, both directly and as adulterants in other drugs can likely be expected. Threat actors will continue to adapt to a changing logistics environment as air services and sea cargo continue to adjust from recent disruptions. This will include a continuation of small scale, regular imports, many organised by OCGs. Alongside this will be an increase in drugs imported directly by consumers, purchased online, mostly in small quantities through mail and air freight. Mexican and Asian OCGs, will almost certainly remain the principal drug importing groups, but domestic adult gangs and OMCGs will continue to assist in drug importing, especially as they are establishing overseas Chapters, notably in Europe and PIC. Attempts to export drugs from NZ, most likely to Australia, and to use NZ as a transit route to other markets will likely be made.

2. It is possible that more drug stockpiling and manufacturing closer to NZ will occur, both most likely in PIC. Concerted OCG efforts to exploit more trusted insiders in many facilities will likely be attended by greater use of cybercrime techniques to exploit or bypass border systems. Increasing use of DECD and tracking technology, including not previously noted innovations, to disguise, hide and more easily facilitate drug trafficking will almost certainly occur.

3. Continuing to identify changes in international and regional drug trends in Europe, Africa and West Asia will assist in understanding and targeting emerging illicit drug and precursor trafficking threat actors and imports to NZ. Ongoing work to identify specific supply chain vulnerabilities and trusted insider threat actors, and where such actors will most likely operate, will assist in hardening the border to these threats. Strengthening information sharing between

RELEASED UNDER THE OFFICIAL INFORMATION ACT 1982

NZCS and its liaison officers (LO), and with foreign LEAs, will enable more nuanced understandings of threat trends that are beginning to and will continue to emerge.

ANALYSIS

4. **2022 drug seizure volumes rose substantially from 2021, easily surpassing the near-record amounts seized pre-COVID-19 in 2019.** The total volume of illicit drugs and precursors seized in 2022 was 4,104kg and 2098L, an increase of 159% and 90% respectively on 2021. The increase likely reflects continuing use of trafficking strategies developed during the pandemic, as well as reviving previous trafficking routes and using pre-pandemic methods. In 2022, the highest drug volumes were seized in the air cargo stream, sea cargo and mail, with most seizures occurring in the mail stream.

5. **In 2022, the main imported illicit drug and precursor types did not change.** Drug seizures (by volume) were dominated by methamphetamine, GBL, and cocaine. MDMA, Khat and GABA were the next most seized drugs (by volume). Pseudoephedrine (PSE) was the most seized meth precursor (by volume).

   - Methamphetamine seizures continue to increase and precursor seizures are increasing again after declining over the pandemic period. The top countries of export for methamphetamine (grams only) in 2022 were Malaysia, Iran, US, Canada, China.
   - MDMA seizures increased in 2022, in both volume (grams) and item numbers (e.g. tablets). Cocaine seizure volumes in 2022 were significantly higher than 2021 levels, with several very large volume seizures made. The return of social gatherings and large volumes of both drugs available globally likely partly account for import increases.
   - Synthetic cathinone seizures increased in volume and numbers in 2022, compared with 2020 and 2021. In 2022, the main cathinone seized was dimethylpentylone.
   - In 2022, 49kg of opioids were seized across 95 seizures (additionally, approx. 7649 tablets and seven litres of liquid opioids also seized). 2022 seizures included: heroin, codeine, tramadol, opium, morphine, etonitazene, hydromorphone, tapentadol, and oxycodone. Whilst opioid seizures (e.g. heroin) have remained low in recent years, other drugs have increased. Heroin seizures (by volume) are small, but increased in 2022 (504g) from 2021 (75g). Morphine seizures fell slightly compared to 2021, but codeine seizures increased (both items and millilitres seized).
   - Fantasy-type substance seizure volumes and quantities continue to increase (e.g. GBL, 1,4-butanediol (1,4-BD) and ketamine). In 2022, NZ Customs seized 1854L of GBL, a substantial increase from 2021 (1062L). Ketamine seizures (by kg) almost doubled compared with 2021 figures.
   - In 2020 and 2021, precursor seizures declined compared with volumes seized in 2018-19, but in 2022 PSE seizure volumes increased 800% on 2021 volumes. Ephedrine (EPH) seizures decreased in 2022 compared to 2021.

6. **NZ's illicit market for fentanyl is small and despite isolated instances of harm, there has been no increase in the misuse, demand for and supply of fentanyl over the last three years.**[3] No border seizures of illicit fentanyl occurred in the last two years. Low levels of misuse are reflected by only two known domestic seizures of fentanyl (2ml in each seizure) by New Zealand Police (Police) since 2021. Multiple fentanyl overdoses occurred in the Wairarapa region in June 2022 resulting in 12 hospitalisations. The fentanyl was misrepresented and sold as methamphetamine and cocaine, and was almost certainly imported illicitly. This highlights

[3] National Drug Intelligence Bureau, 2022. Fentanyl Misuse: Intelligence Assessment July 2022.

RELEASED UNDER THE OFFICIAL INFORMATION ACT 1982

the possibility that some future illicit imports may also arrive similarly misrepresented as other drugs or as adulterants to other drugs, most likely from North America.

7. **Changes occurred to illicit drug and precursor source, export, and transit countries, with increasing quantities arriving from Europe.** Asia and North, Central and South America continue to be NZ's primary drug sources, especially for methamphetamine and cocaine. Top export countries for all drugs (by volume) in 2022 were Ecuador, Malaysia, India, Iran, China. During COVID-19, Africa, Europe and the Middle East grew as drug export regions to NZ.[4] Europe has risen as a methamphetamine, MDMA and cocaine exporting region,[5] and African exports grew for more varieties of drugs, especially methamphetamine, possibly as a result of more Afghanistan methamphetamine transiting the region.[6] In 2022, Laos continued as a top methamphetamine export country in SE Asia (likely originating in Myanmar), a trend begun in 2021 and likely influenced by impacts from Myanmar's military coup.[7] In 2021 Hong Kong and China were top precursor suppliers (by seizure volume), but in 2022 both countries declined markedly, with India replacing them as the top exporter to NZ.

8. **The most significant threat actors are still Mexican OCGs, Asian OCGs, and NZ-based OCGs (including Comancheros, Bandidos).** Asian OCGs are a prominent supplier of precursors, fantasy-type substances, methamphetamine, and synthetic cathinones. New Zealand-based OCGs have well-established links to many offshore OCGs and facilitators organising illicit imports. The influx of 501 deportees with gang associations has almost certainly increased drug trafficking knowledge, experience, and leadership in domestic gangs, and this likely has ongoing downstream impacts. 501 deportees almost certainly maintain links to offshore OMCGs and threat actors.[8] The Comancheros were a prominent NZ-based OCG in 2021, importing or conspiring to import large quantities of illicit substances. Members planned to import huge quantities of methamphetamine and cocaine by a small marine craft after transferring from a mothership.[9] Many members or affiliates of other gangs have been noted for imports and acting as facilitators at air and sea ports.

9. **During 2022 threat actors exploited online and Dark web drug ordering, an extension of methods used during pandemic conditions, significantly increasing regular small-scale imports via air fast freight and mail.** Drug traffickers especially exploit the returning high volumes of air cargo and postal deliveries to hide illicit activity. Additionally, trusted insider threat actors at airports are used, likely also at sea ports, especially as airport and sea port freight traffic returned after pandemic disruptions.

10. **An increase in regular small scale drug importing occurred in recent years, significantly supplemented by many consumers now sourcing drugs online.** Many of these consumer-importers will have no criminal history or links, and some likely acted as opportunistic and entrepreneurial vendors supplying the domestic market.

11. **In recent years, new concealment methods have been noted, often in regular small-scale importing, indicating increasing sophistication and collaboration by drug traffickers.** Sophisticated methods include deep concealments within machinery, and in liquid food and beverages. The same concealment and packaging techniques and types are also noted in imports from different regions. Using the same packaging methods indicates highly

[4] NDIB Annual Report 2021, National Drug Intelligence Bureau.
[5] Notes for the Minister's Brief, June 2022, NZ Customs.
[6] 'JNAC Afghan Methamphetamine Threat – June Conference Summary', August 2022, NZ Customs.
[7] HINT AWG Illicit Drugs and Precursor Assessment – NZCS Submission, July 2022.
[8] HINT AWG Illicit Drugs and Precursor Assessment – NZCS Submission, July 2022.
[9] Operation VAN; 'New Zealand Police operations deal huge blow to organised crime, 35 arrests, $3.7 million in assets seized', June 2021, NZ Police.

RELEASED UNDER THE OFFICIAL INFORMATION ACT 1982

organised drug concealment techniques in different regions, possibly organised by a single TNOC or by different drug suppliers using the same method and packaging supplier.[10] Threat actors are certainly sharing ideas, and some coordination is likely occurring between them.

- Across 2020 to 2022 a notable increase in corflute packaging concealments occurred, using many different colours, but arriving from different parts of the world.[11]
- In recent years, drug concealments in similar beauty products were exported from several countries in different regions (e.g. GBL in eyelash remover products and nail polish remover ex South Korea; cocaine in false eyelash sets from UK; eutylone in eyelash curlers from China/Hong Kong).
  - In 2022 and 2023, different import packaging and taping methods were noted from several regions (e.g. neat cardboard boxing and taping from Europe; wrap-around taping from India), but repeated use of such methods by different threat actors indicates some level of coordination, or certainly copycat activity.
- Heavy machinery used in several drug intercepts occurred from several countries, indicating copycat activity at least, and possibly intentional sharing of techniques.

12. **An increasing use of sophisticated technology by overseas drug traffickers is occurring and will likely be used at NZ's border in the near future.** This technology includes growing use of DECD, tracking devices (to both monitor progress and locate packages), cybercrime technology and techniques to gain access to or bypass cargo tracking systems, as well as assisting in the development of some sophisticated concealment methods. Tracking equipment is likely used where trusted insiders are unavailable or are unnecessary.

13. **OCGs using trusted insiders pose an increasing threat of supply chain infiltration.**[12] Over the last three years, NZ-based OCGs have persistently used trusted insiders to avoid detection in airports, seaports and CCAs (Customs Controlled Area). In 2021, a criminal syndicate used Auckland airport baggage handlers to import almost 500kg of methamphetamine from Malaysia and the United States (US).[13] OCGs have particularly sought to recruit individuals with no criminal history or associations, exploiting their 'clean' status after security and vetting checks.[14]

14. **Some NZ OMCGs and Adult Gangs have established Chapters and other OCG associations overseas, and continue to develop these, likely including opportunities for illicit activity.** Pre-COVID-19, OMCGs and NZAG members travelled to Europe,[15] Middle East and Southeast Asia (e.g. Thailand), likely partly to help establish Chapters in other countries, but also likely to enable drug trafficking, money laundering and other illicit activity. As pandemic travel restrictions ceased NZ-based OMCG and NZAG members have been noted travelling again, to similar destinations. Recent reporting notes OMCG and NZAG members travelling to Pacific Island nations, some for the purpose of attempting to establish gang Chapters.[16] It is almost certain that gang travel to Asia, Europe and Pacific includes attempts to arrange drug imports to NZ. Increased drug manufacture in Europe and Africa has seen increased drugs

[10] HINT AWG Illicit Drugs and Precursor Assessment – NZCS Submission, July 2022.
[11] 6(c) [redacted]
[12] Supply Chain Infiltration: An ongoing risk, 19-20-00405, NZ Customs.
[13] HINT AWG Illicit Drugs and Precursor Assessment – NZCS Submission, July 2022.
[14] Global Drug & Smuggling Trends, INT-22-1375, NZ Customs.
[15] New Zealand Gangs and European Travel, 19-20-00504, NZ Customs.
[16] NZTCU IR 23-48 Op KOTAHI Gang Member travel to Samoa 1 January – 31 May 2023; NZTCU INTSUM 23-037 Intelligence Summary 3 Comanchero MC 'Kingdom Chapter' Tonga, 29 May 2023; Australia and New Zealand: Threats to the border from the South Pacific, 2407 IA-2023-00002.

RELEASED UNDER THE OFFICIAL INFORMATION ACT 1982

arriving from there, and it is possible that NZ OMCG/gang travel has helped influence increased targeting of NZ by OCGs in Europe at least.

OUTLOOK

15. **Drug threat actors, for the most part, adapted to the changing pandemic environment, and will likely consolidate and extend successful practices, methods and supply routes into the near future.** Threat actors will likely continue reviving historic trafficking methods (e.g. air couriers, catchers) while new methods successfully implemented during the pandemic will continue (e.g. exploiting high-frequency low-volume mail imports, online ordering, and trusted insiders). Threat actors will also likely vary drug routes, using different export and transit countries (e.g. methamphetamine through Laos[17]; MDMA ex Europe[18]; cocaine ex Panama), and 're-exporting' (noted in Mexican OCGs smuggling methamphetamine to Australia).[19]

16. **Threat actors will likely continue increasing trafficking capability, especially varying concealment techniques and coordinating methods across several countries or regions.** New concealment methods will likely emerge and be used across multiple consignments from multiple countries, as is already likely indicated with organised, and possibly centralised, use of corflute packaging. Following global trends, threat actors will likely continue exploiting a range of licit products for concealment (e.g. banana shipments, beauty products), 6(c) [redacted] 're-exporting', where a new airway bill is created for each shipping leg, will likely also be used more 6(c) [redacted]

17. **NZ-based OCGs will likely become more active overseas and/or possibly collaborate with foreign OCGs to import drugs.** Mexican, North American and Asian OCGs, with assistance from NZ-based foreign OMCGs and domestic OMCGS and NZAGs, will almost certainly remain the principal drug importers. But some drug manufacturing TNOC groups are willing to share production expertise across the globe (particularly Mexican OCGs), especially into countries with significant chemical production capabilities (e.g. SE Asia, India) or have favourable environments for establishing drug manufacture (e.g. Netherlands).[21] International drug suppliers are also gravitating towards manufacturing drugs closer to markets (e.g. methamphetamine/cocaine manufacture in Europe, methamphetamine manufacture in Africa, precursor and synthetics manufacture in an increasing number of countries).[22] It is possible NZ OMCGs based overseas could exploit new source opportunities to supply back to NZ. In some countries drug manufacture for export has begun where no, or almost no, domestic market existed for that product (e.g. Netherlands methamphetamine manufacture).[23] It is possible NZ-based OMCGs and NZAGs will be enticed by similar opportunities in NZ.

18. **It is likely illicit drug import volumes will sustain, possibly increase, especially for the highest seized commodities (GBL, methamphetamine, and MDMA) but possibly also for GABA and cocaine.** These increases are likely due to the large amounts of

[17] HINT AWG Illicit Drugs and Precursor Assessment – NZCS Submission. July 2022.
[18] MDMA seizures ex Europe, March 2022, NZ Customs.
[19] Mexico: Drug trafficking to Australia 2021/22, Intelligence Assessment, August 2022, Australian Federal Police. 'Re-exporting' involves creating a new airway bill at each leg of shipping, designed to further obfuscate the consignments origin.
6(c) [redacted]
[21] EU product, NZCS, 2023 [no formal product title to date];
[22] Illicit drug smuggling from Africa to New Zealand, INT-22-11085, NZ Customs; EU product, NZCS, 2023.
[23] Illicit drug smuggling from Africa to New Zealand, INT-22-11085, NZ Customs; EU product, NZCS, 2023.

RELEASED UNDER THE OFFICIAL INFORMATION ACT 1982

methamphetamine and cocaine in global circulation, the demand for GBL and its precursor GABA in NZ, and MDMA's likely increased usage as more large social gatherings (e.g. festivals, concerts, nightclubs) occur now restrictions are removed. MDMA will continue arriving in regular small-scale imports mainly from Europe. If the availability of some commonly used 'social' drugs (e.g. MDMA) is disrupted, some alternative/substitute 'party' drugs and synthetics (e.g. gamma-butyrolactone (GBL), 1,4-butanediol (1,4-BD), ketamine, dimethylpentylone) will likely be imported in greater quantities.

19. **NZCS will likely continue to seize smaller volumes of a wide variety of other drugs (e.g. synthetic cathinones and cannabinoids, opioids, performance and image-enhancing drugs (PIEDs), new psychoactive substances (NPS), cannabis, ketamine, and pharmaceuticals).** Of these, synthetic cathinone volumes will possibly increase, most likely from China, but possibly also from a variety of other countries where these are produced. It is more likely increases will occur when availability of other 'party' drugs such as MDMA are low, with synthetic cathinones being misrepresented as these.[24] Ketamine seizures will likely increase, as they have since 2019.

20. **It is possible, although not expected, that fentanyl will pose an elevated threat at the border over the next year.** Domestic diversion of legitimate supply will likely continue to be the main source of fentanyl in NZ's illicit market over the next year. No border seizures of fentanyl have occurred in recent years, but several domestic seizures and harm incidents indicate fentanyl is imported illicitly. In 2022, 12 people in Wairarapa were hospitalised after using fentanyl described as methamphetamine and cocaine, almost certainly imported. It is likely the most immediate next illicit imports and any increased consumption will occur from fentanyl substances misdescribed or from its use as an adulterant in other drugs. North America is the most likely source for such imports. But more illicit fentanyl imports will highly likely appear in the future, most likely in mail since the quantities required for use are small.

21. **Europe and Africa will likely continue to develop as major drug export or transit regions for NZ imports.** In addition to cocaine and MDMA, Europe will possibly become a key export region for GBL, 1-4-BD, GABA, and methamphetamine, due to large scale synthetic drug production capabilities (some of them recently established, e.g. methamphetamine). Large amounts of cocaine are also exported from Europe, some of which arrives in NZ. Africa is an emerging major exporter of methamphetamine and other drugs noted in recent seizures, which will likely continue. African methamphetamine exporting likely results from increased methamphetamine production in the Middle East (Afghanistan), methamphetamine imports from Central America, and possibly supplemented by methamphetamine production in Europe. Africa is also developing its own domestic methamphetamine manufacture. Cocaine transhipping occurs through Africa, but it is unlikely cocaine exporting in any major quantities will occur to NZ in the near future. It is likely that higher illicit import volumes of methamphetamine, MDMA, and cocaine, as well as host of PIEDs and NPS variants will continue out of and through Europe and Africa, some of it by way of the United Arab Emirates.

22. **The largest quantities of illicit drug imports will continue through three main streams (sea and air cargo, mail), but regular small-scale imports in mail and fast freight will also likely continue providing high seizure numbers and major volumes for the next 1-2 years.** Occasional use of large bulk consignments of drugs in maritime vessels will persist (e.g. container cargo concealments, hull attachments, container refrigeration units), and air couriers will resume.

[24] 'Misrepresented' signifies a drug advertised or sold (knowingly or not) as a different substance.

RELEASED UNDER THE OFFICIAL INFORMATION ACT 1982

23. **The recent increase in methamphetamine precursors (mostly PSE/EPH) possibly indicates increased domestic methamphetamine manufacture, or that precursors are exported or stockpiled.** It is possible domestic methamphetamine manufacture will increase if OCGs decide to use NZ as a methamphetamine export country (like Netherlands, South Africa). There is no indication this is about to occur. However, the continued import of small quantities of unregulated novel precursor chemicals is likely.

6(c) [redacted]

RELEASED UNDER THE OFFICIAL INFORMATION ACT 1982

Firearms/Parts and Other Weapons

Threat Rating

6(c) [redacted]

Deliberately non-compliant importers, OCGs and other threat actors will almost certainly continue to import firearms and parts into New Zealand, mainly through mail and fast parcel streams.

Intent

- Deliberately non-compliant importers have high intent to illicitly import prohibited parts (especially) and some firearms since recent legislation now prohibits a range of firearms previously legal. Threat actors are motivated to upgrade existing weapons or to service weapons held illegally, and some desire to possess firearms now restricted.
- OCGs are highly motivated to import parts to service illicitly held firearms, and also to import some illicit firearms where illicit domestic supply cannot meet their requirements.

Capability

- Threat actors can exploit the collaboration of overseas suppliers, cooperative brokers, and complicit importers, as well as knowledge of the mail and fast freight systems, to bypass border checks on firearms and parts imports.
- OCGs can leverage the knowledge of firearms and border evasion tactics of returning gang members and newly arriving OCG/OMCG personnel.
- The knowledge required to build/convert firearms is no longer held only by experts. It is now available for free, often on the internet, and can be accessed worldwide. There are many online forums, chat rooms and outlets (both open web and dark web) where individuals can share material related to weapons manufacture and techniques. Illicit threat actors can utilise this type of information for the purposes of manufacturing parts/converting firearms for use in NZ.

OUTLOOK AND OPPORTUNITIES SUMMARY

24. The immediate future of illicit importing will largely depend on whether domestic sources meet illicit firearms demand and how firearm grey and black markets develop. The full impact of recent firearms legislation on illicit activity will be better understood after several years of adjustment. But the legislation and focused police attention on domestic firearms supply to gangs and organised crime entities (Operation TAUWHIRO) will likely provoke some threat actors to attempt to secure firearms and parts from alternative sources, including importing.

25. Continued cooperation and information sharing with US LEAs, particularly Customs and Border Patrol (CBP) and the Bureau of Alcohol, Tobacco and Firearms (ATF), to understand the changing firearms and parts environment in the US (NZ's major import supplier of firearm and parts) will assist in understanding how trends there impact on importing trends in NZ in the next few years. Similar arrangements with overseas NZ LOs and agencies in other countries (e.g. Canada Border Services Agency (CBSA)) will assist in understanding key trends in other regions also.

26. Developing an understanding of how and where firearms parts importing may shift will be helpful in targeting firearms and parts imports in fast freight and mail streams. More parts may be imported from Asia, and specific engagement with NZ Customs LOs in Asia on firearms/parts trafficking and supply trends may give NZ an early warning regarding any changing supply trends.

ANALYSIS

27. **The broad impact of the new firearms legislation on the border has been minimal, mainly showing in lower import quantities of major firearm types, but little change in illicit importing.** COVID-19 impacts on supply likely also contributed to a decrease in seizures of firearms and parts imports from 2020 onwards, but the full impact of new firearms legislation on illicit activity is likely to evolve and will be better understood after several years.

28. **The aftermath of the 2019 firearms legislation changes, and COVID-19 impacts on supply and demand, likely contributed to both lower firearms import quantities across 2020 to 2022 and low firearms and parts seizure rates.** The new firearms legislation has had little adverse impact on illicit importing. Most former users and importers of semi-automatic firearms and parts are now prevented under the new legislation, and permit numbers for such weapons is greatly reduced and tightly controlled. Very few firearms were seized during 2021 (30 firearms seized – mostly air or BB guns) and 2022 (28 firearms seized - mostly air guns), significantly fewer compared to 2019 (469). Low volumes likely also reflect lower import volumes in general. This is likely derived in part from the dampening effect of COVID-19 on firearms supply and use (rifle and shotgun quantities decreased compared to 2019), but also from importers and firearms users still adjusting to new legislation, exercising caution, and not permitted now to import certain firearms. Significantly fewer firearms parts were seized across 2020 to 2022 (214, 306, 225 respectively) compared to 2019, likely for the same reasons as for lower firearm import seizures.

29. **Disruption to traditional domestic sources of firearms or parts will likely drive serious firearms threat actors (e.g. OCGs, recidivist illicit importers/retailers, criminal entities, hard-core firearm offenders) to find any alternative means to secure the firearms or parts they require.** Serious threat actors will react strongly to constraints placed on NZ illicit firearms supply. Some firearms users and criminal actors will not comply with new legislation and regulations, and will seek alternative supply sources, including illicit parts importing and some forms of domestic manufacture, if not immediately, then almost certainly in the future.[25]

30. **Firearms or parts smuggling is relatively uncommon relative to other Border Five (M5/B5) countries, with only isolated cases in recent years, and most illicit imports are**

[25] INT-22-1941: Imports of Firearms Parts into New Zealand

RELEASED UNDER THE OFFICIAL INFORMATION ACT 1982

attempts to evade permit regulations or to import without permits. Offenders mostly use mis-declaration (e.g. mis-description, misclassification) on air mail and fast freight packages, almost none by sea. 6(c) [redacted]. Illicit prohibited firearms/parts importing decreased, but it is unlikely that all illicit importing stopped in 2022, especially parts. NZ Post's 'blue ban' on handling firearms and parts in the mail (imposed in the wake of new firearms legislation) did not prevent imports in fast freight streams. Brokers and declarants are coming to understand the law changes, but exploiting the new legislation, especially regarding goods descriptions, will likely continue, even increase. Illicit importers and declarants almost certainly take more care to conceal illicit and facilitating activity at the border now.

[redacted]

32. **Many imported parts arrive from the US, but recent US supply shortages could impact on both licit and illicit parts supply in the near future.** Firearms parts supply shortages have been reported in the US for several years.[26] If this continues, it is likely other overseas sources will replace US parts suppliers, or 3D-printed parts will be substituted in.

33. **An increase in equipment imports such as firearms tooling kits and manufacturing equipment may indicate a rise in illicit firearms assembly.** Firearms assembly and manufacture requires machinery and tooling (e.g. lathes, stamp machines, presses). Understanding the types of machinery, tools and materials (e.g. stamped metal blanks, tubes) used in illicit firearms manufacture will likely be as important as identifying parts imports themselves, although machinery and tools imports are likely to be less common.

34. **The lack of statistical quantity for firearm parts in the Tariff continues to ensure that the scale of parts importing, both legitimate and illicit, remains unknown.** Any increase in illicit firearms parts importing could be an opportunity to request introducing 'statistical quantity' on firearms parts in the Tariff to better monitor quantities and flows.

OUTLOOK

35. **The full impact of the 2019 firearms legislation on illicit activity will almost certainly continue to influence importing.** The impact of legislation changes on the illicit firearms market in NZ and ongoing law enforcement focus on, and disruption to, the illicit firearms market will lead to greater efforts to source firearms from alternative sources. This will likely include firearms conversion, and increased imports of firearm parts for maintenance and domestic firearms assembly. Overseas examples indicate that where access to firearms is constrained, illicit firearms users will resort to alternative methods to obtain firearms, including sourcing parts for conversions, reactivations, and illicit firearms assembly and manufacture. In some cases (e.g. US, UK), such parts are imported.

36. **The mid- to long-term future of importing will largely depend on whether domestic sources sufficiently meet illicit firearms demand and how the grey and black markets develop.** No major change is expected in non-compliant or general illicit importing in the next three years, but it is possible organised crime entities and associates will attempt illicit imports. The police are 'concerned' about the recent upsurge in gang-related firearms violence, likely

[26] Privately Made Firearms (Update), Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF) briefing to the International Firearms Trafficking Working Group (IFTWG) 27 August 2021. Firearms, parts and ammunition supply shortages have occurred in the US in recent years, exacerbated by high recent US firearms sales and weapons supply to the Ukraine conflict. https://apnews.com/article/sports-business-health-coronavirus-pandemic-gun-politics-86e61939eb4ae1230e110ed6d7576b70

RELEASED UNDER THE OFFICIAL INFORMATION ACT 1982

resulting in part from tensions caused by foreign gangs arriving.[27] Any continuation of this trend will possibly impact on gang firearms requirements, with threat actors motivated to procure firearms for self-defence or for intimidation. It is not known if this will also impact significantly short- to medium-term on illicit imports.

37. **Firearms parts importing, both licit and illicit, for the purpose of assembling or manufacturing illicit weapons will possibly increase in the medium term (1-3 years).** Serious firearm threat actors have primarily sourced illicit firearms domestically, and this almost certainly continues. 6(c) [redacted]

38. **B5 partners and European LEAs report trends of increasing diversion, conversion, and the popularity of various 'alternative' firearm types.** The European Union and United States report increases in blank-firing, replica, flobert calibre, and air (gas) firearm conversions to live-firing weapons (often using parts ex China), and domestic firearms assembly, especially personally-made firearms (PMFs), and manufacturing from illicitly imported parts (including pre-stamped and pre-tooled parts). They, with Australia, also report illicit parts importing, such as barrel blanks and solvent traps (used as suppressors). It is possible NZ will also see increases in such firearms acquiring, including imports, as well as illicit parts imports for firearms upgrading, personal manufacturing, or domestic assembly.

39. **Police attention on firearms supply to gangs and organised crime entities (Operation TAUWHERO) will likely provoke some reaction, which may result in firearms/parts acquired from alternative sources.** This will possibly include attempts to source firearms offshore or to assemble their own from domestically-sourced or imported parts. NZ police focus includes a review of border alerts for firearms and parts. Alert changes could impact on seizures and NZ Customs' visibility on illicit importing patterns over the next 1-3 years until the effectiveness of adjustments are fully ascertained. The new Firearms Registry intends to make firearms diversion to criminal actors more difficult, which could also result in threat actors sourcing more firearms overseas or assembling their own.

40. **It is possible 3D-printed parts imports will occur to evade import permit regulations and to assist in firearms assembly.** Many of these parts are printed with fake, or no, serial numbers, manufactured by both individuals and businesses, and are used as substitutes for genuine parts. Overseas, they are often used to build 'ghost guns' (firearms made using parts without serial numbers) or wholly 3D-printed firearms. Some importers will likely import on behalf of criminal entities who do not possess import permits or firearms licences. 3D-printed parts are subject to the same permit requirements as any other firearms parts.

41. **Dark web purchases will possibly increase over the next 1-3 years, but there is little evidence Dark web ordering is presently attractive for most illicit importers.** 6(c) [redacted] The most likely commodities are prohibited parts and a small amount of hand guns. Dark web imports are likely isolated cases rather than a widespread trend and are not expected to pose a significant border threat in the next 1-3 years, although ongoing instances are likely.[29]

[27] https://www.nzherald.co.nz/nz/auckland-gang-shootings-police-very-concerned-about-their-access-to-firearms/E4VOE7VTHEPDCQ4IDKGWDJNI6A/; https://www.police.govt.nz/news/release/police-operation-prevent-firearms-related-violence

[28] 6(c) [redacted]

[29] NZ Police report that domestic demand for illicit firearms could drive online sales, but it is unlikely that Dark web sourcing is currently a significant platform of choice for importers. COLT-IR-21-07-14 Online Firearms Trafficking In New Zealand - for PLO.

RELEASED UNDER THE OFFICIAL INFORMATION ACT 1982

6(c)

[redacted]

Objectionable Material

Threat Rating

6(c)

[redacted]

Threat actors, mostly opportunistic but determined individuals, with a variety of motivations and target markets will almost certainly continue to import objectionable material into New Zealand.

Intent

- Individual threat actors remain highly motivated to source, and sometimes create objectionable material in foreign jurisdictions and to import predominantly digital material, despite having access to internet material.
- Individuals adhering to extremist ideologies import digital material that aligns with their beliefs and informs their agendas since much of this material is produced overseas.
- NZ-based threat actors are motivated to travel to access, and sometimes create child sexual exploitation material (CSEM) and import it back to NZ since such material is likely easier to access and make offshore.

Capability

- Only small amounts of objectionable material are seized, with most seizures occurring at residential premises, likely indicating both the ease with which material can avoid border controls and the levels of knowledge many importers have to evade regulations.
- Threat actors are able to hide objectionable material on many digital devices, often encrypted, in order to evade border controls, and import it through mail/fast freight streams and/or passenger streams.
- Printed objectionable material is hard to identify and easy to misdescribe, and individuals will continue importing print publications via mail and fast freight streams, often with limited or no concealment.
- Some individuals will highly likely continue carrying objectionable material on personal devices when travelling internationally, possibly believing discovery is unlikely.

OUTLOOK AND OPPORTUNITIES SUMMARY

42. Objectionable material imports will almost certainly increase as full travel returns. Imports by travellers, and seizures, will likely rise again in the next few years, especially since travel provides a significant opportunity for tangible objectionable material imports. Few imports are noted in mail and cargo, but this will likely increase as more interdiction success occurs in the passenger stream. It is possible travellers arriving from PIC with child sex exploitation material (CSEM) on digital devices will increase following a reported rise in child exploitation material (CEM) activity in PIC in recent years.

43. Ongoing cooperation with domestic and international partner agencies will continue to prove valuable in disrupting threat actor networks and child sex exploitation (CSE) syndicates. NZ Customs' Child Exploitation Operations Team's (CEOT) work with other domestic and

RELEASED UNDER THE OFFICIAL INFORMATION ACT 1982

international partner agencies will almost certainly assist in informing NZ Customs of ongoing and emerging border threats and threat actors.

ANALYSIS

44. **Despite borders reopening, objectionable material seizures have not yet returned to pre-pandemic levels.** Threat actors, most often air travellers, continue to carry material across the border on personal electronic and digital devices (e.g. phones, data storage devices, laptops). Objectionable material seizures have steadily declined in recent years (29 in 2019; 2020, 13; 2021, 8, 2022, 9). It is almost certain that the COVID-19-related reduction in air travel and disruptions to mail and cargo streams led to less objectionable material seizures during 2020 to early 2022.

45. **The overwhelming majority of objectionable material seizures are sexual in nature, mostly CSEM, mostly in digital form, and most commonly at residential premises.** Between 2019 and 2022 there were 59 seizures of objectionable material, with most occurring at a CCA (15 seizures) or residential premise (24 seizures). The remaining 20 seizures occurred at airports, the mail centre or a seaport. Of the 59 seizures, 40 were either a digital device or a digital storage device. From 2019 to 2022, most of seizures were of electronic devices containing sexual material, with minimal seizures of violent extremist material.

46. **The Pacific Islands is possibly an emerging threat for CSA material to NZ.** CSEM watchdog agencies have reported that online CSEM offending (material creating, accessing and sharing) increased in the Pacific during the pandemic years, likely assisted by increasing internet connectivity in PIC. It is likely that offending is still occurring, possibly increasing.[30]

6(a) [redacted]

47. **CSE threat actors mostly operate alone and share material across closed platforms and secretive networks that are often difficult to penetrate and disrupt.** CEOT investigations indicate that the majority of CSE threat actors are individuals who conduct their offending in isolation and largely unconnected directly with other groups. Consequently, threat actors are elusive and difficult to identify, and investigations often require high levels of technical capability and patience. NZ Customs recently contributed to an international operation (Operation H) which led to the disruption of a CSEM network and 46 arrests in New Zealand, as well as resulting in 836 international investigations.[32]

48. **NZ's market for child sex dolls is small but is an emerging and possibly growing border threat.** Child sex dolls are an illicit commodity in NZ and are increasingly being seized at the borders of other B5 countries. Five border seizures of child sex dolls have occurred since 2017, all addressed to individuals, all sent from China. One commercial sex doll retailer made enquiries with NZ Customs seeking to avoid accidental imports of child-like dolls, but other

[30] National Center for Missing & Exploited Children (NCMEC) 2020 and 2021 Cyber Tipline Reports by Electronic Service Providers; Pacific Transnational Crime Network (PTCN), *Transnational Crime Assessment 2021-22*, 2022; PTCN *Transnational Crime Assessment 2020-21*, 2021

6(a) [redacted]

[32] https://www.dia.govt.nz/press.nsf/d77da9b523f12931cc256ac5000d19b6/23d4c3f76035199dcc2587f80075cf5c!OpenDocument. Operation H was initiated in 2019 and is ongoing.

RELEASED UNDER THE OFFICIAL INFORMATION ACT 1982

retailers may not be as concerned about compliance. It is likely that motivated individuals will continue to source child-like sex dolls and attempt importing by mis-declaring goods.

- NZ's first conviction for importing a child sex doll occurred in 2018. The person was convicted for both the import and for possessing videos and images on devices.

49. **Child-sex fetish sprays are an emerging threat, adding to the CSEM threat at NZ's border.** In 2022, a NZ Customs' operation aiming to detect child sex doll imports led to the seizure of two consignments containing child-sex fetish sprays from Japan. Consignments each contained several sprays and scents, some of which were deemed to be indecent and obscene due to the use of the words 'highschooler' and 'schoolgirl' in the description.

50. **NZ Customs' seizures of violent-extremist objectionable material remains low due to the dominant online nature of sharing and accessing such material.** Four seizures of 'The Anarchists Cookbook'[33] occurred across 2020 and 2021. Only a very small amount of objectionable material seizures has been physical media categorised as extremist material, notably identity-motivated and neo-Nazi material, and multiple copies of The Anarchist Cookbook. Much of this material is typically shared via closed groups in mainstream social media or on 'alt tech'[34] platforms. Alt tech will continue to be used to share objectionable material in NZ and overseas.

OUTLOOK

51. **Re-opening the border and the ongoing rise in inbound travel will likely increase the amount of objectionable material entering NZ, as well as seizures.** Inbound passenger streams from countries considered high risk for child exploitation, particularly passenger travel from locations in Asia and the Pacific known for high rates of CSE offending (e.g. Philippines), are an ongoing threat. Some visiting travellers will continue acquiring CSEM and attempting to enter NZ with material stored on digital devices or in software products.

52. **It is likely there will be a resumption, possibly even an increase in outbound travel from NZ to high-risk locations for CSE offending as international travel continues to recover.** It is likely this travel will contribute to the proliferation of CSE material and increase the amount of objectionable material returning travellers attempt to bring back across the NZ border.

53. **LEA success in disrupting objectionable material use and possession in online forums may drive some threat actors to seek alternative methods of storage and distribution.** In particular, if LEAs and watchdog groups manage to disrupt child exploitation networks a shift towards conventional means of imports via passenger and mail streams is possible.

54. **Interdicting illicit violent-extremism material will likely remain low since this material, especially faith-base and identity motivated extremism[35], is primarily shared online.** Identity-based violent-extremism and single issue-motivated extremism is increasing globally,[36] possibly resulting in a future increase in violent-extremist objectionable material entering via passenger and mail streams. 6(c) [redacted].

[33] The Anarchist Cookbook contains instructions relating to the manufacture of explosives, creating improvised weapons and manufacturing drugs (e.g. LSD).
[34] Social media platforms and internet service providers with less moderation than mainstream platforms.
[35] Radical ideologies and beliefs focused on real or perceived threats to concepts of ethnic culture and identity.
[36] Issues-based extremism includes eco-terrorism, conspiracy theory motivations or social order risks due to misinformation.

RELEASED UNDER THE OFFICIAL INFORMATION ACT 1982

55. **It is possible a thematic shift in violent-extremist objectionable material seen and seized within NZ and at the border will occur.** Recent years have seen a global increase in Identity Motivated Violent Extremism (IMVE) and single-issue public order concerns in NZ, such as the Christchurch Mosque terrorist attack and 2022 anti-vaccine mandate protests. More politically sensitive issues will likely become prevalent in NZ, possibly resulting in a wide range of related material crossing the border. An increased appearance of this material and further protests or violent extremism will possibly result in legislative changes targeting more kinds of material, including misinformation possibly defined as objectionable material.

56. **Effective disruption and mitigation will require sustained application of technology solutions and advanced levels of expertise.** The increasingly digital nature (e.g. electronic devices) of objectionable material crossing the border via passenger streams will require continuous training within NZ Customs and use of specialist tools to effectively detect, identify, and decrypt objectionable material. Ongoing resourcing and training for frontline staff will be required to interdict and deter threat actors offending at the border using digital devices.

6(c) [redacted]

Intellectual Property Rights

Threat Rating	6(c) [redacted]

Small scale commercial IPR-infringing consignments will likely continue to be imported by New Zealand-based entities for financial gain. The ability to locate suppliers and source these illicit goods will continue to be enabled by the growth of online and social media marketplaces.

Intent

- Small scale commercial importers of IPR goods are highly motivated to source and ship counterfeit and fake consumer goods[37] for profit, understanding the ease with which such goods can be concealed in high other import volumes and the low prospect of discovery.

Capability

- Threat actors can readily access wide and increasing ranges of IPR-infringing goods from many sources and can hide these in high volumes of other like goods across most import streams.
- Both small-scale commercial importers and individual consumers are easily able to exploit the proliferation of online marketplaces and social media sites offering IPR-infringing goods.

OUTLOOK AND OPPORTUNITIES SUMMARY

57. Seizures of small-scale commercial IPR-infringing import consignments are expected to remain consistent over the next three years, barring any significant impact to manufacturing and supply chains internationally in general. Continued growth of online marketplaces will likely increase access to IPR-infringing goods as well as provide competition to a wide range of

[37] Counterfeit goods are genuine goods trafficked or sold by unlicensed vendors. Fake goods are goods, often of inferior quality, manufactured or sold by unlicensed makers/vendors attempting to pass them as genuine.

RELEASED UNDER THE OFFICIAL INFORMATION ACT 1982

legitimate products. In the near future, it is possible that ongoing economic hardship will influence an increase in consumer preference for cheaper goods, which could drive consumers more towards IPR-infringing goods as affordable alternatives.

58. The application of NZ Customs' sophisticated targeting and analytical tools to enhance intelligence development and targeting of IPR-infringing threat actors has the potential to significantly increase seizures. In addition, a developed intelligence and targeting picture could facilitate collaborative work with the Intellectual Property Office of New Zealand (IPONZ) and licence holders and result in further disruption of IPR-infringing trade at the border.

ANALYSIS

59. **Relatively small numbers of IPR-infringing seizures occur, averaging 33 IPR seizures annually over the last three years.** Despite a reported increase in online shopping in recent years, the annual seizure numbers for IPR-infringing consignments have remained consistently low. In 2020 44 seizures occurred, with 42 in 2021 and 12 in 2022. The reluctance of major rights-holders to pursue action against many infringers, and NZ Customs' resource priorities and focusing searches on other prioritised goods during the pandemic has likely contributed to recent low seizure numbers.

60. **The air cargo stream accounts for most IPR-infringing goods seizures.** While the air cargo stream accounted for 77% of IPR seizures between 2019 and 2021, it accounted for only 58% of IPR seizures in 2022. The remaining seizures were predominantly distributed across mail and small loose container load (LCL) sea cargo consignments. The overwhelming use of air cargo is likely due to high use of small-volume goods consignments and the common sourcing of goods via online sites and IPR-infringing goods promoted on social media.

61. **Clothing accessories, clothing items, electronic goods and footwear are the most common IPR-infringing goods seized at the border.** Clothing accessories and clothing items were the two most encountered consignment types from 2019 to 2022, accounting for 59% of yearly IPR-infringing seizures (on average). Small electronic goods/accessories were also commonly seized, mostly parts and accessories for Apple and Samsung cell phones.

62. **Export and origin countries for IPR-infringing consignments are consistent with regular source countries for low value goods to New Zealand.** Goods origin is often difficult to establish, but country of export is routinely noted in seizure data. China was the most frequent export country for IPR-infringing consignments between 2019 and 2021, followed by Philippines. An average of approximately 60% of seizures made in 2019-2022 were shipped via air cargo, with the remaining split between sea cargo, mail and passenger baggage.

63. **Most identified importers of IPR-infringing goods continue to be small-scale commercial individuals and businesses.** Individuals or family groups reselling goods via small businesses (e.g. $2 shops) and markets are typical importers. Profit-making is the most likely motivation rather than organised efforts to undermine rights holders' profits or cause reputational damage by selling substandard counterfeit or fake goods. Some illicit importers are likely aware NZ Customs does not seize or take enforcement action on all IPR-infringing goods imported for 'private and domestic' use. With most commercially imported goods resold in small volumes through small retail outlets, threat actors likely understand that the difference between 'personal' and 'commercial' consignments can be negligible (e.g. two t-shirts vs ten) and keep consignment volumes low. Small goods such as cell phone covers or chargers are often imported in larger volumes making them easier to identify as commercial imports.

RELEASED UNDER THE OFFICIAL INFORMATION ACT 1982

64. **The COVID-19 pandemic and restrictions had little impact on IPR-infringing seizures at the border.** IPR-infringing seizures remained consistent over the pandemic, and no significant shift in IPR-infringing pandemic-related goods seizures occurred. A significant increase in seizures occurred of personal protective equipment (PPE) deemed to be 'unsafe goods', a small amount of which was IPR-infringing, although seizures did not occur for that reason. As the need for COVID-19-related PPE and medical supplies declined, incentives to import IPR-infringing PPE and other pandemic related goods also reduced.

OUTLOOK

65. **NZ's IPR-infringing goods market in NZ is likely to persist, and there is unlikely to be any significant change to IPR-infringing goods importing as a result.** IPR-infringing goods imports for commercial gain will continue, mostly small scale. IPR-infringing goods threat actors will continue to be aware of, and closely watch for, any opportunities to increase profitability. Asia, and China in particular, is likely to remain a major goods supply source, and luxury goods are almost certain to remain popular and profitable.

66. **Ongoing growth of internet shopping and social media market places will continue to both positively and negatively impact IPR-infringing imports.** Increasing use of online marketplaces, exacerbated by supply issues on some preferred goods, positively and negatively influences IPR-infringing goods purchasing. It will become progressively easier for people to locate and purchase both IPR-infringing goods and more competitively priced genuine products which, in turn, may further fuel IPR-infringing goods supply.

67. **The rising costs of consumer goods and economic hardship will likely drive some consumers to import cheaper IPR-infringing goods.** Cost of living hardship, inflation and recession issues could make importing low value IPR-infringing products more attractive, and low-cost goods manufacturers overseas and small-scale commercial importers will exploit this.

68. **Domestic and international legislation changes will potentially impact both the import and border enforcement of IPR-infringing goods.** Domestically, potential changes to geographical indicators (goods origin) or a new version of the Designs Act (1953) could impact IPR goods at the border. Internationally, progressing Free Trade Agreements (FTA) with other nations will likely include discussions around IPR trade enforcement.

69. **NZ Customs has advanced analytical and targeting tools that assist in interdicting IPR-infringing imports.** NZ Customs has developed and implemented sophisticated and nuanced targeting and analytical tools, which are applied to high priority goods and risks at the border. Using these tools, ongoing trend analysis of IPR seizures could help develop key criteria into clusters of profiling indicators that majorly increase seizures. A developed intelligence picture allied with flexible targeting tools such as Risk and Intelligence (R&I) to proactively target recidivist consignees and consignors could generate a more complete border offending picture for NZ Customs. This will also likely result in more seizures, almost certainly impacting on NZ Customs resources. However, a more complete border picture would help develop a collaborative approach with other agencies engaged with trademark infringements, such as the IPONZ, and with rights-holders.

6(c) [redacted]

RELEASED UNDER THE OFFICIAL INFORMATION ACT 1982

Hazardous Goods

Threat Rating

6(c) [redacted]

Non-compliant and illicit imports and exports of hazardous goods are likely to continue, but volumes will likely be low. In the next 1-3 years, climate change legislation will likely impact on hazardous goods imports and exports and will likely require adjustments in border oversight.

Intent

- Most threat actors attempt to illicitly import or export hazardous goods to avoid declaration and permit requirements. Threat actors have little intent to illicitly import hazardous substances that could be used to manufacture harmful goods such as explosives, radiation weapons, or dirty bombs.
- Waste exporting threat actors, often using or disguised as legitimate businesses, will likely continue deliberate and persistent illicit hazardous waste exports to countries offering high prices for waste and scrap materials, particularly in South Asia and the Middle East. Threat actors will exploit opportunities to export increasingly obsolete technology, some of which contains hazardous materials.

Capability

- Many non-compliant threat actors have little knowledge of border requirements, but some threat actors are highly knowledgeable about border regulations and how to exploit vulnerabilities, and they are experienced at evading detection.
- Threat actors can use simple methods such as false declarations and not obtaining permits. However, in addition to low-level methods, some export threat actors use more sophisticated techniques and technology to conceal illicit goods or to make inspections difficult.

OUTLOOK AND OPPORTUNITIES SUMMARY

70. Threat actors will continue to intend to illicitly import or export hazardous goods, and highly likely have, or could acquire the capability to do so. Deliberately non-compliant import and export threat actors are moderately motivated to avoid declaring goods correctly, obtaining permits, adhering to health/safety requirements, or incurring additional costs (e.g. insurance, handling fees, carrier charges, duties). False declarations (often goods misdescriptions) and failure to obtain permits are the main and simplest methods to evade border regulations. Occasionally threat actors attempt more sophisticated methods, especially for exports. Little serious intent to illicitly import hazardous substances for weaponizing or making explosives, explosive devices or irradiated/radiation weapons is noted. Although illicit hazardous goods imports and exports are not common, continual monitoring is required to ensure compliance and to mitigate the threat to NZ's border.

71. In the next 1-3 years threat actors will intentionally attempt to import or export hazardous goods, although most activity will likely be erroneous or uninformed non-compliance attempts. Ongoing supply shortages, including building materials, will likely result in attempts to import substitute and substandard goods that contain hazardous materials and fail NZ safety or health standards. Some hazardous waste, e-waste and scrap waste export destination countries no longer accept some waste material forcing threat actors to export illicitly or to find other markets. Threat actors will also likely find ways to exploit an expanding range of new climate-change and environment-friendly technologies and goods.

ANALYSIS

72. **Hazardous goods cover a wide range of products offering many opportunities for threat actors, some of whom do not understand regulations or the dangers goods pose.** Hazardous goods include waste materials (liquids, gases, or solids) that are explosive, flammable, corrosive, toxic, radioactive, or infectious, arriving from many sources. Threat actors are often unaware that hazardous waste poses a major risk when not stored, transported, treated, or disposed of properly. Some hazardous goods (e.g. asbestos products)

73.

RELEASED UNDER THE OFFICIAL INFORMATION ACT 1982

are imported from developing countries. Some importers will be unaware of the harm, but others deliberately fail to comply with regulatory requirements in full knowledge of the hazard.

74. **Illicit hazardous goods imports are infrequent, and threat actors mostly use low-level regulation avoidance methods.** Common methods are misdeclarations and misdescription and/or failing to apply for permits. Deliberately non-compliant import/export threat actors are highly motivated to avoid shipment checks and/or incurring additional costs (e.g. insurance, handling fees, carrier charges, duties) by declaring goods incorrectly, not obtaining import or export permits, and failing to disclose health and safety implications. Goods are often shipped in unsafe ways. For example, automotive parts exporters will often fail to drain engines, gearboxes and other reservoirs of dangerous, toxic or flammable liquids.

75. **Some threat actors also use more sophisticated methods, exploiting various ways hazardous waste goods can be classified or categorised to evade border regulations.** Threat actors exploit complexities in describing hazardous goods and e-waste and the 'exceptions' that are found in different Tariff classifications. For example, e-waste exports can avoid being deemed 'hazardous' if they are described as having offending materials removed beforehand; lead acid (from batteries) has a tariff code, but other acid-containing products may not; some computers and circuit boards do not need to be labelled as e-waste; an electronic product is not e-waste if it is declared as 'intended for re-use' or as 'second-hand'.[38]

76. **Illicit export threat actors are often intentional, routinely and deliberately ignoring regulations.** Threat actors are motivated by high prices overseas for scrap or waste products (e.g. plastics, metals, electronics, vehicle parts, batteries), many containing hazardous goods. They want to avoid levies, permits and safety requirements associated with legitimate exports. As with imports, low-level evasion methods (e.g. misdescription, permit evasion) are commonly used. But more sophisticated methods are also used, the likelihood rising if threat actors were previously prevented from exporting. For example, illicit scrap exporters often use container-filling methods (e.g., container-tipping machinery), making border inspections difficult and dangerous. They often also pose as legitimate exporting businesses or use legitimate businesses or exporters that have permits or can obtain them.

77. **Threat actors exploit NZ Customs' lack of direct regulatory oversight over hazardous goods at the border, even though it intercepts and inspects them.** Import and export permits for hazardous goods are issued by the Environmental Protection Authority (EPA).[39] NZ Customs does not licence hazardous goods exports and imports, only checking that required import/export permits are attached and inspecting goods if non-compliance is suspected. Some export threat actors understand this and use misdescriptions and permit application avoidance to reduce the likelihood of goods inspections. Although the Customs and Excise Act 2018 gives NZ Customs control over the movement of hazardous waste across the border it does not have priority regulatory oversight over goods. NZ Customs enforces compliance, but relies on importers and exporters obtaining permits, often only intervening if provided information about potential non-compliance.

OUTLOOK

78. **Threat actors will continue to intentionally attempt to import or export hazardous goods in the next 1-3 years, but most attempts will likely be unintentional or uninformed non-compliance attempts.** NZ is not a known destination for deliberate imports of waste or hazardous goods. However, lucrative overseas markets, profit motivation, and permit avoidance, which increases the range of countries goods can be exported to, will likely ensure

[38] Under the Basel Convention on the Control of Transboundary Movements of Hazardous Wastes and Their Disposal 'second-hand' refers to 'Electrical and electronic assemblies (including printed circuit boards, electronic components and wires) destined for direct reuse, and not for recycling or final disposal.' https://www.basel.int/Portals/4/Basel%20Convention/docs/text/BaselConventionText-e.pdf
[39] https://epa1.cwp.govt.nz/industry-areas/hazardous-substances/

RELEASED UNDER THE OFFICIAL INFORMATION ACT 1982

domestic threat actors continue attempts to export hazardous goods illicitly.

79. **It is almost certain e-commerce will provide more opportunities for some hazardous goods importing.** Goods not complying with group standards issued by the EPA can be readily purchased online and imported without permits. This includes paints, crayons/pastels, battery-operated electronic goods, some cosmetics, and a range of chemicals. Consumers' lack of awareness of hazardous goods regulations will result in more non-compliance. More goods will go undetected because of inaccurate or incomplete import (or export) descriptions.

80. **Ongoing supply shortages, especially with building materials, will likely lead to attempts to import substitute materials and goods failing NZ safety or health standards in the next 1-2 years.** Offshore suppliers will possibly use unlicensed or unscrupulous sources who offer substandard, harmful, unsafe or illegal goods when previous or preferred suppliers cannot meet demand. Some goods possibly will be hazardous or contain hazardous elements.

81. **Some destination countries for hazardous waste, e-waste and scrap waste exports no longer accept waste, forcing threat actors to export illicitly or to find other markets.** For instance, some scrap plastic-recycling countries now limit or ban imports, resulting in NZ stockpiling such waste and exporters without permits switching to other destinations. Quantifying exporters violating permits and compliance requirements is difficult. In an increasingly environment- and climate-issue concerned world, violations of waste export permits will result in ongoing, perhaps escalating, disposal, recycling and reputational issues. NZ-based threat actors and companies illegally exporting hazardous and unpermitted goods, especially to developing countries, will become a substantial border and reputational threat.

82. **Threat actors will likely find ways to exploit an expanding range of new climate-change and environment-friendly technologies, goods and border-related regulations.** The numbers and varieties of goods defined as 'hazardous', or banned outright, will possibly increase, as will attempts to import or export them. Imports or exports of counterfeit or fake goods purporting to be 'green' or environmentally friendly, and/or not meeting safety or health standards, will also possibly rise. Threat actors will almost certainly illicitly move increasing volumes of goods deemed environmentally harmful (e.g. batteries, fuels, goods containing heavy metals) and deemed 'hazardous'. Threat actors could easily send such goods to any country (e.g. PIC) prepared to accept old or less-compliant technology, opening NZ up to accusations of goods 'dumping'. They will also try to avoid paying costs and levies for exporting goods for disposal (e.g. end-of-life e-vehicle batteries) which will likely increase as more goods and technologies become obsolete and require recycling or disposing of.

83. **Illicit imports of hazardous substances for weaponizing or making explosives, explosive devices or irradiated/radiation weapons are unlikely.** No attempts have been recently noted to import such goods, but the harm implications are such that ongoing high vigilance is required. Changes to the Radiation Safety Act 2016 and the Radiation Safety Regulations 2016 legislation[40] could impact how radioactive goods are inspected in the future.

84. **It is both beneficial and necessary for NZ Customs to work closely with other regulatory agencies, such as Ministry for the Environment (MfE), EPA and Ministry for Foreign Affairs and Trade (MFAT), to reduce the threat of hazardous materials exports.** [41] Since NZ Customs does not issue hazardous goods permits, disrupting deliberate regulation evasion attempts relies on detecting non-compliant permits and receiving information from other agencies where noncompliance is intended or suspected. Without such information it is also difficult to accurately determine the extent of successful illicit exports.

[40] The Ministry of Health's Office of Radiation Safety (ORS) administers the Radiation Safety Act 2016 and the Radiation Safety Regulations 2016 on behalf of the NZ government.
[41] The Imports and Exports (Restrictions) Act 1988 is administered by Ministry for the Environment (MfE). The Environmental Protection Agency (EPA) regulates a range of goods under various international conventions.

RELEASED UNDER THE OFFICIAL INFORMATION ACT 1982



CITES (Convention on International Trade in Endangered Species)

Threat Rating	6(c)

Wildlife traffickers, other wildlife enthusiasts, and non-compliant travellers are likely to continue to attempt to import CITES goods and/or make unpermitted live exports of fauna and flora, mostly by air travel and cargo.

Intent

- Visiting or returning travellers continue to import CITES items for personal use, and some commercial imports of CITES-prohibited goods are likely to be deliberately misdeclared and non-compliant.
- The global wildlife trade is worth upwards of an estimated $23 billion USD, and the huge profits available to wildlife traffickers are a strong ongoing incentive for a diverse array of threat actors supplying existing markets and also seeking new markets to sell to, including those who look to target New Zealand.

Capability

- Threat actors have well established trafficking networks for the movement of illicit wildlife and CITES products. There is substantial crossover internationally between wildlife and drug trafficking networks and routes. Some threat actor individuals can travel to and from NZ without notice and can use domestic assistants to aid them.
- TNOC groups who specialise in the illicit wildlife trade are well resourced and connected.

OUTLOOK AND OPPORTUNITIES SUMMARY

85. There has been very little change in the type of CITES products seized at the New Zealand border in recent years, with most imports being for personal use. It is likely that the trade in CITES species will increase and return to pre-COVID-19 levels in the next 1-2 years. Although NZ's CITES product market is not large and CITES exports are relatively few it is possible both could increase slightly in the near future.

86. Good opportunities exist for NZ Customs to further understand wildlife trafficking and illicit actors attempting to import CITES-containing goods. A proposed legislation change, and increased training and information sharing with other government agencies, particularly Department of Conservation (DOC), will assist officers to identify and regulate restricted goods.

ANALYSIS

87. **Traditional medicines make up the bulk of NZ Customs' CITES seizures.** They mostly arrive in small quantities in mail and fast freight, and with air travellers. In 2022, many traditional Asian medicines (TAM) seized contain Saussurea costus (also known as Radix aucklandiae/Aucklandia lappa), a CITES-listed plant. Other CITES products seized in 2022 were items containing ivory (bookends/knives/chess sets), hippo tusks, giraffe leg bones, turtle

RELEASED UNDER THE OFFICIAL INFORMATION ACT 1982

shells, elephant hair, and high-end luxury goods (e.g. animal skin handbags, cosmetics containing caviar). As in previous years, most seizures are imported largely for personal use.

88. **Non-compliant imports of CITES goods are often due to system/user errors and badly informed importers, although some are almost certainly deliberate evasion attempts.** DOC has seen increasing numbers of transactions where incorrect CITES declarations to NZ Customs are made. The prohibited goods field in Trade Single Window (TSW) is often not correctly completed leading to goods cleared with no Customs intervention, often due to incorrect advice given to an importer (i.e. no CITES permit required) or failing to present CITES permits correctly (no originals, or not at the time of import). In some cases, non-compliance results from import agents' actions. It is suspected that some 'errors' are deliberate attempts to bypass border controls.

89. **During COVID-19, NZ's travel restrictions limited CITES threat actor activity, especially exports.** Despite pandemic travel restrictions, wildlife traffickers overseas continued operating. DOC noted arrests of known wildlife traffickers occurred overseas During COVID-19, some wildlife traffickers were able to adapt activities to meet market demand during restrictions. However, air travel restrictions limited CITES threat actors operating at NZ's border.

90. **NZ Customs collaborating with DOC at the border continues to be an effective method for mitigating identified threats.** CITES-containing products develop and change (e.g. recently Barshasha and Pygeum were identified), and new concealment methods are used. Awareness of new products and concealments is necessary to identify non-compliant imports. DOC have recently provided four new CITES training modules for use by both NZ Customs' Service Delivery staff and Frontline officers to identify imports. Ongoing cooperation with DOC assists in dealing with incorrectly declared CITES goods (particularly through TSW).

OUTLOOK

91. **Trade in CITES species will likely increase and return to pre-COVID-19 levels in the next 1-2 years. It** is likely that mail/fast freight seizures will continue since demand for CITES goods is ongoing. It is also likely that travellers visiting NZ to export wildlife will return as opportunity allows and market demand drives collecting.

92. **New Zealand's market for CITES products is not large, but this could possibly change.** Wildlife trafficking is highly lucrative, with overseas reporting outlining that profits continue to rise post-pandemic. Wildlife traffickers will seek to diversify areas of operation, particularly those with links to drug trafficking networks and supply pathways, and will likely attempt to find markets in NZ, possibly exploiting foreign travellers and immigrants as a new or expanding consumer base. Additionally, NZ has some high demand rare and valuable native species that command high prices, especially if they are endangered. As the endangered species list grows demand will likely also grow and export attempts will increase.

93. **Online shopping and CITES-containing goods purchases (e.g. TAM) via overseas websites will remain high, with consumers relying on such channels to buy products**. Some imports will likely be deliberately non-compliant since some importers will be aware of border restrictions on CITES goods. However, many will not know full content details of their purchases and/or will not know they are restricted items.

94. **It is possible that CITES-containing goods with expired documents will continue to arrive.** During the pandemic, supply chain disruption and shipping delays resulted in delayed shipments of goods with expiry dates**.** While this threat has largely passed, goods arriving with expired documentation for other reasons may still occur.

95. **Changes in legislation will result in further controls on imports of CITES goods.** Changes to the Trade in Endangered Species (TIES) Act 1989 were agreed by Cabinet in August 2020, including a ban on domestic sales of any items made with ivory from elephants killed after 1975. Additionally, imports and exports of elephant ivory will be prohibited, with narrow exemptions to ensure elephant ivory items can still be traded by museums, for DNA testing and testing to determine age, and that antique musical instruments with permits can still enter/exit. Other planned changes to the TIES Act focus on improving the Act's implementation

RELEASED UNDER THE OFFICIAL INFORMATION ACT 1982

to ensure border regulations efficiently and effectively manage international wildlife trade and stops illegal trade. Despite NZ's small ivory market, changes seek to deter any further ivory importing to NZ. It is possible increased ivory product restrictions could lead to concealed illicit import attempts and importers attempting to falsify import documents, as reported overseas.

96. **Several opportunities exist for NZ Customs to work with DOC to mitigate identified threats**. DOC and NZ Customs could collaborate further on commercial imports of CITES goods. Manufactured commodities such as furniture (e.g. bulk rosewood furniture (Dalbergia spp.)), small items like picture frames and pool cues made from Ramin, and cosmetics containing CITES species are often seen for sale, with DOC having no record of permits lodged for such imports. These are likely mis-declared at import. Increased information sharing will likely reduce the number of instances and products evading border inspection.

6(c) [redacted]

Revenue & Illicit Value Movement

Revenue/Economic Threats

Threat Rating	6(c) [redacted]

OCGs, other criminal actors, and opportunistic businesses and individuals continue to display high levels of intent and capability to evade border revenue collection and import/export commodities non-compliantly or illicitly.

Intent

- Deliberately non-compliant traders are highly motivated to avoid paying revenue (duty, excise and GST) and to increase profits by exploiting the use of misdeclared valuations and amounts, misclassifications and misdescribed goods.
- Many threat actors likely consider the interdiction risk is low and any penalties incurred are an insufficient deterrent. Previously successful imports/exports also continue to motivate some non-compliant traders.

Capability

- OCGs and non-compliant traders have high levels of knowledge of all supply chain streams and border processes, reporting requirements and vulnerabilities, and they especially exploit high volume freight streams.
- Both OCG and deliberately non-compliant commercial threat actors can employ sophisticated revenue avoidance methods but make most use of less complex methods common to most non-compliant actors.
- Some threat actors use professional facilitators, or exploit professional services and systems, sometimes without the knowledge of those exploited or leveraged.

OUTLOOK AND OPPORTUNITIES SUMMARY

97. Revenue evasion on imported goods by non-compliant traders and other threat actors is a significant threat at NZ's border, even more so currently as the government focuses on post-pandemic economic recovery. Critical to economic recovery success is hardening and protecting supply chains and ensuring border facilities and systems are not disrupted so that

RELEASED UNDER THE OFFICIAL INFORMATION ACT 1982

border revenue collection occurs optimally. Excise, import duty, and Goods and Services Tax (GST) evasion are high threat as both deliberate and opportunistic threat actors seek to reduce costs and maximise profits wherever they can. While commercial revenue evasion will account for large scale systemic evasion amounts, regular opportunistic and non-compliant importing of lower value consignments will result in many small-scale revenue evasion events. Illicit tobacco and alcohol imports, trade concessions/preference exploitation, and online shopping are the most common forms of revenue evasion.

98. Continued cooperation and information sharing with domestic and international law-enforcement partners, and developments in targeting and detection technologies, will help NZ Customs identify and disrupt revenue evasion threats. NZ Customs will continue to utilise and develop risk-based targeting, outliers' analysis, and auditing to mitigate threats to revenue and the economy. Improving trade data quality, including partnering with key industry actors to enhance information flows, and developing new compliance methodologies will also assist in identifying both new and ongoing evasion threat.

ANALYSIS

99. **Revenue evasion on cross-border goods is significant, ranging from a few high-volume excisable goods types to a wide variety of goods in lower volumes where other duty and GST evasion occurs.** COVID-19-related disruptions impacted both trade across the border as well as revenue collection in 2021 and 2022. In a volatile economic climate importers attempted to economise as much as possible, including attempts to evade border duties and levies. Collecting as much due revenue as possible is important to the government's pursuit of post-pandemic economic recovery.

100. **Tobacco and alcohol continue to be high risk commodities for revenue evasion attempts due to the excise rates applied to them.** Tobacco is the most smuggled excisable good, with attempts at revenue evasion on alcohol also noted. Tobacco is smuggled both by OCGs and by opportunist and entrepreneurial threat actors. Increasingly high prices for NZ's retail tobacco helps to incentivize smuggling threat actors. As NZ moves towards Smokefree Aotearoa 2025, tobacco smuggling becomes more profitable for threat actors who show increasing levels of sophistication and organisation. They are almost certainly increasing illicit imports attempts and concealment efforts. Cartons of cigarettes are increasingly smuggled, but raw tobacco leaf and shisha tobacco also increased in 2022. OCGs operating from several countries arrange illicit imports using a range of shipping routes to hide origins. Despite a decreasing consumer market, tobacco smuggling is still attractive for traffickers because of its profitability and a perception of lower penalties compared with illicit drug smuggling.

101. **The revenue evasion threat for shisha tobacco is evolving, likely forced by NZ Customs' recent success in changing shisha tobacco import legislation.** Water-pipe tobacco includes flavoured, hookah, shisha, molasses and fruit tobacco.[42] In 2022 NZ Customs began to tax shisha fairly and equitably to protect legitimate importers, like other B5 countries. From May 2022, water-pipe tobacco was a prohibited import requiring a permit. It was treated the same as tobacco products, tobacco leaf and tobacco refuse that became prohibited imports from 1 July 2020. The duty-charging method and the duty rate for water-pipe tobacco changed, effective from May 2022.[43] Any un-permitted tobacco imports (including water-pipe tobacco, leaf or refuse) are seized and destroyed. Increased duty rates and requiring import permits will likely drive actors to attempt circumventing such measures if the demand for shisha remains.

[42] https://www.customs.govt.nz/business/import/tobacco/
[43] The previous duty charging method based on the declared kilogram of tobacco content (KTC) was replaced by charging based on total weight. https://www.customs.govt.nz/business/import/tobacco/

RELEASED UNDER THE OFFICIAL INFORMATION ACT 1982

The legislation change is likely forcing importers to drive illicit supply through black market avenues.

102. **Almost all deliberate threat actors utilise some low complexity evasion methods.** Common methods are misdeclarations (especially misdescriptions, false valuations and origins) and document falsifying. For example, some tobacco imports have false origin declarations. Other common evasion methods include using overseas suppliers not applying GST at the point of sale and/or providing free or reduced-cost shipping. Non-deliberate declarant errors are common in commercial imports resulting in revenue evasion. Both deliberate and unintentional declaration errors result in major lost revenue across all imports.

103. **Some threat actors have developed more sophisticated revenue evasion techniques.** Commercial actors exploiting duty/tax legislation, FTA provisions (e.g. deliberately claiming preference incorrectly), and varied valuation methods (e.g. misdeclaring origin, exploiting Free Trade Zone (FTZ) information limits not requiring details of previous goods journeys) all threaten revenue collection. Threat actors also increasingly use professional facilitators to circumvent regulations and evade payments. Commercial actors, often working with professionals (e.g. lawyers, tax consultants, financial advisors), exploit legislation to reduce duty/tax payments. This includes shifting the duty tax point to more favourable places in the supply chain (e.g. deferring duty payment as late as possible post-importation; withholding import valuation declarations until value can be determined at its lowest point). Although some methods challenged by NZ Customs were found to be legal,[44] some other methods used are almost certainly illicit. Continued use shows a willingness by commercial entities to seek ways to evade due payments.

104. **Increasing use of online shopping, almost certainly heightened during the pandemic, likely both increased GST revenue and revenue evasion opportunities, whilst also exacerbating trademark-infringing activity.** NZ now requires overseas online trading sites to be GST-registered, however, more online activity almost certainly increases the range of overseas traders that importers use that are not GST-registered. Deliberately misdeclaring import values below the de minimis threshold (raised in 2019) has also affected duty and GST collection. The data quality on many low value imports hinders enforcement action, including targeting of specific imports and importers. Data provisions for Inward Cargo Reports (ICR) are minimal, and exploitation especially occurs in the air cargo stream where goods are commonly valued below the $1,000 NZD threshold. Goods below the threshold do not require a full declaration, and importers often misdeclare goods to defeat risk assessment mechanisms. Threat actors also take advantage of these high import volume streams to conceal their revenue evasion attempts.

105. **While pandemic-related supply chain issues have now eased, NZ continues to be vulnerable to supply chain blocks that could impact NZ's economic recovery due to our distance from markets.** Ongoing disrupted supply chains for NZ imports and exports likely contributed to some stifling of economic activity during 2020 through 2022. Auckland Port congestion and delays in 2021 highlighted the impact of slowed goods supply and potential for exploitation by revenue fraud threat actors.

OUTLOOK

106. **Tobacco smuggling will almost certainly increase in profitability, continuing to drive illicit imports.** An annual ten percent tax indexation increase across all tobacco products will

[44] In 2020, the Customs Appeal Authority (CAA) ruled in favour of an importer allowing it to import with an almost zero value for duty by deducting larger portions of expenses than was previously considered appropriate.

RELEASED UNDER THE OFFICIAL INFORMATION ACT 1982

make cheap illicit tobacco imports more profitable and easier to sell. To make a profit, illicit suppliers only need to sell products below retail prices, increasing profit margins. This will almost certainly increase the intent, appeal and amount of tobacco smuggling into NZ.

107. **Re-opening the border will almost certainly see tobacco smuggling resume in passenger streams.** Passenger stream seizures of cigarette sticks and loose tobacco fell in 2020 and 2021, almost certainly due to COVID-19 border restrictions. However, the resumption of travel, especially from countries in Asia, and the onset of Smokefree Aotearoa 2025 measures will likely prompt more illicit tobacco smuggling attempts.

108. **Changes to shisha duty rates in the May 2022 budget will almost certainly drive illicit activity and smuggling**. Despite the government's success in taxing shisha tobacco, the measure also almost certainly resulted in incentivising black-market imports and growers to increase production and distribution efforts, and will likely continue to do so.

109. **As e-commerce grows, associated revenue evasion will almost certainly continue, possibly even increase.** More users, both private and corporate, will identify opportunities to exploit the de minimis threshold and to undervalue goods, using sites or mail options that avoid applying GST. Businesses will almost certainly increase e-commerce use as cost-cutting and supply-managing measures, likely increasing revenue evasion opportunities.

110. **Over the next two years, supply chain disruption will likely continue, from multiple causes including goods sanctions/embargos, port operation issues, and shipping re-routing and re-scheduling.** Goods embargos on conflict zone participants (e.g. Ukraine, Syria) and other sanctioned countries (e.g. Iraq, North Korea) will continue to impact goods movement in some supply chains. New trade agreements will likely raise new supply and logistics factors and issues, including revenue evasion potential. Supply chain vulnerabilities such as trusted insider threat activity and targeted cyber-related penetrations of border-related systems also have the potential for revenue fraud and exploitation to evade revenue collection. Threat actors will continue to target vulnerabilities in the supply chain that assist in revenue fraud, and are highly likely to adapt to changes, such as the growing use of automated ports and tracking mechanisms. Economic recovery is a priority government focus, and critical to success is hardening and protecting supply chains and ensuring border facilities and systems are not disrupted so that border revenue collection occurs optimally.

111. **Some commercial actors found legislative loopholes and creative alternative solutions to reduce or evade duty owed, and other importers will likely seek similar ways to replicate those successes.** It is possible some commercial actors, encouraged to seek out and initiate similar sorts of outcomes, will go further and adopt solutions that contravene border regulations and legislation. This will place pressure on NZ Customs' resources detecting revenue evasion and litigating against threat actors. Additionally, increasing amounts of goods intentionally routed through FTZs to disguise origin will increase the revenue evasion threat.

6(c) [redacted]

RELEASED UNDER THE OFFICIAL INFORMATION ACT 1982

Illicit Money and Value Instruments Movement

Threat Rating

6(c) [redacted]

OCGs and deliberately non-compliant threat actors are highly motivated to continue moving illicit cash and value across the border, most often via bulk cash smuggling or with other value transfer mechanisms.

Intent

- Threat actors are highly motivated to make profits from illicit activity in NZ and to move their proceeds offshore. NZ drug prices are among the world's highest, and offshore actors target NZ for this reason. Criminal actors will need to continue laundering and moving funds as long as illicit activity occurs in NZ.
- OCGs rely on concealment and undetected movement of illicit funds in order to maintain control of profits gained through illicit activity, including seeking to transfer illicit funds (e.g. drug trafficking profits) across the NZ border using an array of transfer and laundering methods.

Capability

- Threat actors transferring illicit funds across the NZ border are likely well-resourced from OCG networks offshore. Professional money laundering syndicates are used by OCGs who seek to outsource financial operations. OCGs often have established connections with professional enablers/facilitators (e.g. accountants/real-estate agents/lawyers) to help launder funds.
- Many cash smuggling attempts at the NZ border are not complex. OCGs likely use both basic and complex money transfer methods. Some OCGs can diversify their operations to evade LEAs.
- OCGs use current and emerging technologies to illicitly transfer funds across borders. Encrypted communications are used to prevent detection by LEAs. Cryptocurrency and other emerging technologies are also used by criminal actors to efficiently and quickly launder and transfer money.

OUTLOOK AND OPPORTUNITIES SUMMARY

112. OCGs and other criminal threat actors based domestically and offshore will continue to require the proceeds of illicit activity to be concealed and moved across borders, and then subsequently re-integrated into the financial system in another jurisdiction in to fund further illicit activity. Illicit threat actors will continue to employ bulk cash smuggling methods currently used, but will possibly also seek out and adopt other mechanisms, some of which are more sophisticated, to move cash or make illicit value transfers.

113. Identifying illicit funds and the threat actors using more sophisticated systems will continue to be challenging and require a range of advanced financial crime-combatting skills, methods and technologies. Many of these methods are used by other LEAs and helpful products are commercially available. Maintaining up-to-date legislation governing cryptocurrency use will continue as a key challenge as well as opportunity to combat illicit cryptocurrency activity.

ANALYSIS

114. **Border cash seizures reduced from early 2020 during travel restrictions, but both a return of travel and increased border focus recently has seen more seizure incidents.** Border cash seizures in 2020 amounted to $76,351.92, and increased in 2021 to $187,675.21. Both are much lower than the total value of seizures in 2019 ($1,111,860.95), a decrease largely attributed to COVID-19 border travel restrictions. The impact is also demonstrated by the frequency of seizures across 2019-2021, from 24 in 2019 to just seven in 2021. Criminal actors were likely forced to find other ways to move illicit funds in 2021. Late in 2022, border cash report (BCR) incidents increased, largely due to NZ's border re-opening mid-2022, better training of NZ Customs frontline officers as well as increased screening by detector dogs and frontline officers, and improved intelligence on bulk cash smuggling. Since the border re-

115.

RELEASED UNDER THE OFFICIAL INFORMATION ACT 1982

opened in 2022, there were six instances of seized undeclared cash totalling $343,284.91, an increase from 2020 and 2021. The 2023 seizure figure will likely be far greater.

116. **Asia nationalities and New Zealanders are the most frequently noted undeclared cash offenders.** The most common nationalities involved in undeclared cash seizures between 2019 and 2022 were NZ and Cambodia (KH) passport holders. Other nationalities involved in cash seizures in the last three years were People's Republic of China, Hong Kong, Australia, Fiji, Cambodia, Thailand and Indonesia. Most NZ passport holders with undeclared cash were naturalised NZ citizens. Australian passport holders were only noted more prominently in 2021 undeclared cash incidents. This is likely due to the travel bubble between New Zealand and Australia during the COVID-19 pandemic. During this period, instances of undeclared cash were noted on persons travelling for the purpose of gambling at NZ casinos.

117. **The top two most trafficked currencies are NZD, followed by USD.** Less trafficked but notable currencies are AUD, EUR, CNY and HKD. Several other currencies are also trafficked in smaller amounts and are usually located with higher amounts of the above currencies. Chinese and New Zealand passport holders predominantly traffic NZD and some USD, with a small amount of the other currencies mentioned above. Hong Kong, South Korea, Cambodia, and Indonesia passport holders traffic a mixture of NZD and/or USD, again with small amounts of other currencies.

118. **All instances of undeclared cash between 2019 and 2022 were in the air passenger stream.** Air travel is a common and relatively easy method for transferring cash and value instruments across borders, both by organised threat actors and by casual or opportunistic threat actors. Customs detection methods are currently primarily focused on the air passenger stream, with the sea passenger stream being a known vulnerability. However, there are also some tools and resources deployed to detect money movements in the mail or cargo streams (primarily detector dogs, x-ray screening, intelligence, and manual profiling). Although cash smuggled via mail and cargo import streams is hard to detect, some seizures occurred in 2023.

119. **Most cash seizures have not been obviously organised crime-related or terror/extremism funding attempts but are associated with miscellaneous travellers attempting to evade border controls for many other reasons.** Determining whether undeclared cash movement is OCG-related or money laundering, or deliberate or unintentional non-compliance for other reasons, is difficult.

120. **Some undeclared cash was linked to OCGs, money laundering activity, or suspected terrorism-related actors**. It is difficult to determine the extent of OCG/OMCG involvement in cash movement but a few incidents across several years indicate OCG activity is ongoing.

6(c) [redacted]

121. **Most cash smuggling attempts adopt non-complex methods, such as false declarations, and are predominately undertaken by individual actors on an ad hoc basis.** Non-declaration and misdeclaration of funds being moved is used to bypass border controls. Often threat actors do not even bother to conceal the cash or value instruments, likely believing that the likelihood of discovery is low.

RELEASED UNDER THE OFFICIAL INFORMATION ACT 1982

122. **More sophisticated methods have been noted, often used by casual threat actors and by OCG engaging in money laundering and illicit transfer activity.** Casino tour groups (known as 'international referrals') are noted structuring funds between travel companions to avoid Anti-Money Laundering and Countering Financing of Terrorism (AML/CFT) Act 2009 border cash reporting obligations (e.g. carrying under the NZ$10,000 reporting threshold). They have also been identified carrying Bearer Negotiable Instruments (BNI) instead of cash, which are harder for Customs officers to detect. An OMCG was linked to an intentional concealment of vacuum-sealed cash carried on a person, most likely trying to evade cash detector dogs or body scanning. It is also often difficult to confirm the motivation for the criminal activity, whether it is just cash declaration evasion or part of money laundering activity.

123. **During the pandemic some stockpiling of illicit cash occurred in other countries, and it is possible this occurred in NZ also.** The desire to move undeclared and illicit funds almost certainly continued during the pandemic, but NZ's COVID-19 travel restrictions and freight disruptions likely reduced, possibly even prevented, illicit cash exports and imports in passenger, cargo, and mail streams. However, it is likely some attempts were made, likely mostly in freight streams. Re-opening the border in October 2022 has prompted attempts to move undeclared and illicit cash and value instruments again via previously used methods.

124. **OMCG and OCG will almost certainly continue moving undeclared currency to and from PIC and likely stockpile illicit cash in PIC before moving it elsewhere.** OCG operating in NZ, PIC and outside the Pacific likely use various methods to launder illicit funds made in NZ in and through PIC.

- PIC-registered companies have been used by criminal syndicates to launder money in PIC before moving funds to China, sometimes using NZ as a transit point.[45]

125. **It is possible that OCGs use trusted insiders to move illicit funds across the border.** Trusted insiders have previously been used in the movement of illicit drugs, so OCGs may employ the same methodology for cash. In the supply chain and border facilities OCGs utilise people that have no obvious indicators of criminal association. It is likely that OCGs use people with no Customs (or other LEA) notings ('cleanskins'), or that are unlikely to attract attention, to bypass operational targeting. Customs uses known profile indicators and operational risk targeting to identify threat actors. But OCGs are adept at using all types of people to assist them, and they can help conceal and move cash as easily as other goods.

126. **Alternative value transfer instruments (AVTI), including high value goods, have been used to transfer illicit value across NZ's border.** Value transfer instruments and goods include precious stones or metals, vehicles or parts[46], and high value consumer goods (watches[47], mobile phones[48] and cameras). Eight instances of individuals travelling with gold bars were noted in recent years. Although these instances were deemed to be genuine movements across the border, they illustrate that such instruments are used and that some movement may occur undetected.

- A fast freight export of gold bullion to the US was intercepted in August 2022. The gold was concealed in tin foil inside books, with a false declaration on the packaging.

6(c) [redacted]

RELEASED UNDER THE OFFICIAL INFORMATION ACT 1982

127. **Use of non-fungible tokens (NFTs) for illicit value transfers is rare, but this could change in the future.** NFTs are cryptographic assets or digital commodities (e.g. art, videos) stored on a blockchain. Each has a unique identification code distinguishing them, which prevents copying, substitution or dividing, and so are a highly secure method of transferring value. Ownership is recorded on the blockchain, and ownership is transferred without the need to physically exchange goods. Under NZ law, NFTs are not considered a unit of value and reporting of NFTs over NZ$10,000 is not required. Although this is a gap in current regulations, there is no confirmation that NFTs have been used in laundering or value movement activities in NZ. Additionally, NFTs are considered an unattractive asset for trade-based laundering (TBML), as this trade still requires an exchange of material goods, each with its own border transfer record, thus negating the benefit of anonymity and undisclosed transfer that NFTs provide. However, NFTs can be used as an illicit value transfer method, and popularity may increase. Several instances of criminal usage of cryptocurrency involving NZ-related OCGs and threat actors have occurred in recent years.

- In 2021, Operation OTP GREENLIGHT/TROJAN SHIELD resulted in criminal assets seized across the globe, including cryptocurrencies. The operation noted the alleged involvement of NZ criminal threat actors in drug importing and money laundering.[49]

- In 2022, a Ministry for Primary Industries (MPI) investigation into alleged black market sea food sales noted an offshore individual engaged to convert fiat currency into cryptocurrencies in an effort to conceal a portion of the proceeds of crime.[50]

OUTLOOK

128. **Illicit actors will continue to employ border cash smuggling methods currently used, but will possibly also seek out and adopt other mechanisms to move cash or make illicit value transfers.** It is likely that an increase in money laundering through cryptocurrency and TBML will occur as regulations related to the storing and movement of illicit cash become more restrictive. It is also possible that greater use of NFTs, AVTI (e.g. daigou, hawala, stored value cards (SVC)) and non-monetary instruments will occur as illicit actors seek to move large illicit funds amounts more easily and anonymously.

129. **Improvements in SVCs may see a reduction in physical cash moved by OCGs and other organised criminal actors.** SVCs are capable of carrying multiple credit card numbers on one card, and are able to be loaded remotely (e.g. a physical card in Australia can be used to place credits on a card in New Zealand). This enables the transfer of funds onto a card in one jurisdiction further displaced to a card in another jurisdiction. SVCs are hard to detect at the border, difficult to prosecute as it is not easy to establish a card's value or the original source of funds and are easy to use for value transfers while concealing beneficial ownership. International partners have seen an increase in the movement of illicit funds stored on SVCs, therefore threat actors transferring across the NZ border could also use them.

130. **Value transfer instruments and high value goods will likely be used more in air travel streams now NZ's border has re-opened.** Value transfer instruments and goods imports and exports via sea and air cargo streams were likely used during the pandemic period. But air passenger transfers will likely increase as international travel to most countries returns and

[49] https://www.europol.europa.eu/media-press/newsroom/news/800-criminals-arrested-in-biggest-ever-law-enforcement-operation-against-encrypted-communication; https://www.nzherald.co.nz/nz/operation-trojan-shield-fresh-drug-money-laundering-charges-laid-against-alleged-organised-crime-criminals/NPL7ZRYGEASC4473IDCX6TG57I/
[50] Transnational Organised Crime – Looking Forward, Prepared For The Transnational Organised Crime Leadership Group, August 2022

RELEASED UNDER THE OFFICIAL INFORMATION ACT 1982

increases. Anticipated changes to AML/CFT regulations will enable Customs to report to the police Financial Crime Unit on Bearer Negotiable Instruments (BNI), including casino chips.

131. **As cryptocurrency develops it will likely be used more for illicit value transfers, although noted illicit use in NZ has been rare.** Future use of cryptocurrency is expected to increase as more actors leverage the anonymous/pseudonymous nature of cryptocurrency exchanges.[51] This is likely to be assisted further by rapid changes and developments in the cryptocurrency and digital currency industry. Emerging trends in NFTs, decentralised finance (DeFi), 'tornado cash' and smart contracts are expected to add capability to cryptocurrency use that makes it harder to identify, view and monitor activity. Rapid advancement in cryptocurrency and decentralised finance space is a challenge to effective enforcement.

132. **Border cash intercepts are increasing, and assist in detecting illicit money flows, but identifying illicit funds and threat actors using other more sophisticated systems will be necessary, although challenging.** Cash smuggling is not the main mechanism for large illicit value transfers. It is likely criminal actors physically move small amounts of cash via low-level operators, while larger amounts are moved in more complex ways, most of it not directly traceable to OCGs or threat actors. NZ Customs likely detects low-level actors aiding professional money launderers (PML) or OCGs to move illicit funds across the border, but not high-level organised crime or facilitating actors. It is suspected that PMLs and OCGs use low level actors to carry money across the border to reduce their own exposure risk. Organised crime actors and assisting PMLs leverage legitimate informal value transfer systems (IVTS) since the high cash/value transfer volumes and the informal nature of such systems make it difficult to identify and interdict illicit transfers. Criminal actors can move cash easily while also obscuring their activity. Money service businesses (MSB), casinos, virtual asset service providers (VASP), and hawaladars are also noted preferred illicit funds transfer methods. However, not all funds movements through such mechanisms is illicit and it is often difficult to identify and separate legitimate users from illicit users.

133. **Maintaining up-to-date legislation governing cryptocurrency use will continue to be a key challenge, and opportunity, in combatting illicit cryptocurrency activity.** Current cryptocurrency legislation is often unable to update quick enough to adapt to the rapid changes in cryptocurrency usage. Under NZ law cryptocurrency exchanges require compliance with AML/CFT regulations as key cryptocurrency activities are considered to be financial services. However, there is no requirement to report the movement of cryptocurrency across the border. It is expected that both domestic and international legislation will continue to change to establish laws and guidelines that make cryptocurrency safer for investors and less accessible by cyber criminals and money launderers. To ensure compliance and enforce legislation new cryptocurrency tracking products from companies like Chainalysis assist in tracing crypto transactions back to the source, wallet or exchange.

6(c)

[redacted]

[51] Anonymising features hide user identities, while pseudonymous features allow users to adopt a fictitious identity.

RELEASED UNDER THE OFFICIAL INFORMATION ACT 1982

6(c)

[redacted]

National Security

Terrorism & Extremism

Threat Rating

6(c)

[redacted]

Motivated Violent Extremist (MVE) entities are almost certain to continue utilising both travel and goods imports across the New Zealand border to further their specific goals in the next few years. Extremist entities at the New Zealand border continue to maintain a low-medium level of intent matched with a comparable level of capability.

Intent

- After restrictions on travel in recent years both Faith Motivated Violent Extremists (FMVE) and Identity Motivated Violent Extremists (IMVE) are strongly motivated to travel to re-connect with overseas groups and re-establish associations. Consequently, MVE travel is expected to return to pre-pandemic levels. In order to travel, it is likely threat actors will be willing to risk interaction with border officials on departure and/or arrival.

- FMVE will likely be motivated to travel to conflict areas and assist in establishing locations for FMVE groups to facilitate networking and training. Similarly, IMVE will likely desire to travel to ideologically associated events and locations (e.g. key anniversaries, festivals, social events).

Capability

- Extremist entities are now able to undertake international travel and have had several years to plan travel and their border LEA evasion tactics and methods. Consequently. Some travellers will likely prove challenging for NZ Customs to identify and assess.

- Extremist entities will exploit the recovering and increasing legitimate import volumes and continue using well known and previously successful concealment and border regulation evasion techniques to obtain materials to promote and facilitate MVE acts and to further their ideological goals.

OUTLOOK AND OPPORTUNITIES SUMMARY

134. Reduced Motivated Violent Extremist (MVE) travel in recent years is expected to return to pre-pandemic levels as restrictions ease and flight availability increases. No extra increase in travel is expected beyond a return to prior levels, however ideologically linked events, anniversaries, and conflict zones are still likely to be reasons for travel by violent extremist threat actors. It is possible destabilised regions, such as Afghanistan, will attract travellers if terrorist groups re-emerge there, and conflict zones will be a similar drawcard for prospective combatants. MVE threat actors waiting to return to NZ in the next few years are likely to be negligible, while the Christchurch Mosque terrorist attack anniversaries may attract some MVE travel in the future.

RELEASED UNDER THE OFFICIAL INFORMATION ACT 1982

135. Increasing access to new border technologies is providing Customs intelligence with agile and targeted methods to identify risk entities, and the impact of international events and conflicts in real time. Threat actors resuming travel will be exposed to border LEA scrutiny and movement tracking, with the potential for further intelligence gathering and threat assessment. Both resumed travel and increasing connectivity and collaboration with international partners will also provide opportunities for NZ Customs to benefit from information-sharing on identified targets and potential threat actors. 6(c) [redacted] The increasingly borderless aspect of extremist ideology and the proven ability of global terror groups to provide technical support to otherwise remote individuals will continue to influence the NZ terrorist border risk. As extremist threat actors develop greater interconnectivity and exploit advances in communication technology, an opportunity exists for LEAs with advanced tracking capability to monitor and gather intelligence on threat actors.

ANALYSIS

136. **Faith-Motivated Violent Extremists (FMVE) and Identity-Motivated Violent Extremists (IMVE) are the predominant extremist ideology threat actors encountered at the border**. FMVE is more frequently encountered in the passenger stream as threat actors travel outbound to associate with others (e.g. multinational extremist groups) or to enter conflict regions (e.g. Ukraine, Afghanistan, possibly Syria). IMVE is mostly encountered in the import streams, most notably goods associated with current and historical symbolism, literature and memorabilia.

137. **Air travel is the main method of MVE movement across the NZ border.** 6(c) [redacted] Threat actors can also travel alone, or as part of family or other groups to diminish the chance of scrutiny. Border screening of such indicators is often able to identify potential threat actors. 6(c) [redacted]

138. **The pandemic did not majorly influence returning Foreign Terrorist Fighter (FTF) travel across NZ's border.** Continuing lack of FTF return travel across NZ's border is attributed to threat entities' ongoing residence within foreign detention camps. While a significant decrease occurred in travellers assessed for terrorism threat over this period, this is largely due to a reduction in overall pandemic air travel rather than the targeting of terrorist threat entities.

139. **Goods imports linked to both FMVE and IMVE ideologies continue to be identified at the NZ border, but seizure numbers and volumes in recent years have been small.** Recently, IMVE-associated goods represented the largest percentage of MVE ideology-linked items encountered by volume. Although most of the items encountered recently were not considered 'objectionable'[52], they indicate a growing interest in MVE material and a desire to import it, and they can be used to identify potential threat actors. While changes in IMVE ideology could account for some increase, a shift in border resources from passenger targeting to goods targeting likely also accounts for some 'increase'.

140. **Imports of weapons explosives, Improvised Explosive Device (IED) materials and relevant precursors/parts continue to be a border threat.** Previous examples, such as the

[52] Films, Videos and Publications Classification Act 1993

RELEASED UNDER THE OFFICIAL INFORMATION ACT 1982

2017 Sydney Etihad bomb plot, demonstrate the potential for harm and damage, but no attempted imports have been noted in the last five years. Project 'Global Shield' targeting profiles screen import streams for dual use items that have a potential for manufacturing IEDs.

6(a) [redacted]

142. **Ongoing conflict in the Ukraine also poses a credible MVE threat to NZ's border, with extremist IMVE groups active in the region.** Known militant groups, such as the Azov Assault Brigade (Azov), are engaged in the Ukraine conflict. The confluence of geopolitics and ideology in these groups often resonates with IMVE entities and legitimises their activity. This often drives ideologically compatible and sympathetic foreign fighters to align with and travel to support such groups. Conflict arenas also attract other individuals who actively seek out high risk and combat environments. Legitimacy via ideology and the perceived fight against a large aggressor are strong motivators for influenced or radicalised individuals to join a variety of groups, such as Azov, Yekineyen Parastina Gel (People's Defence Units) (YPG) or Islamic State of Iraq and the Levant (ISIL). NZ Customs is watchful for activity (e.g. finance and materials exports) that may constitute support of a designated terror organisation or a sanctioned country.

OUTLOOK

143. **Increased global online connectivity between MVE, supporters and sympathisers will likely increase the travel and goods threats across the NZ border over the next 1-3 years.** Online communication, education and radicalization between individuals and organised groups has been seen globally across MVE ideology streams. This has likely enhanced links between IMVE adherents, and possibly fuelled a desire to travel and to share publications and support materials.

144. **With NZ's border now re-opened for travel, travel by offshore actors associated with extremist ideologies will likely increase.** With the unrestricted return of international travel, ideologically focused events will more regularly feature prominent offshore figures who are invited by or deferred to by domestic persons and groups of interest. Recent events in NZ, such as the 2022 parliamentary protest, exemplify a heightened interest in protest and resistance activity that could attract international sympathisers, advocates, and speakers.

145. **FMVE travel between NZ and risk locations will likely increase as border restrictions ease and the viability of international travel returns.** Increased travel access to active conflict areas is expected to lead to more attempted FMVE travel. It is possible that any re-establishment of an al Qaeda haven and terrorist training camps in a Taliban-led Afghanistan will incite FMVE travel.

146. **IMVE travel by NZ nationals is likely to return to pre-COVID-19 levels over the next 1-3 years, but no significant increase in the short term is expected.** Very little intended travel to the Ukraine conflict has been noted, but the conflict region remains a potential drawcard for IMVE travel, either to fight and/or support or to participate in training. Previous IMVE travel that centred on associated events (e.g. festivals, music/concerts, exhibitions, symposiums) and anniversaries is expected to resume as restrictions on travel and associating ease. In

RELEASED UNDER THE OFFICIAL INFORMATION ACT 1982

most cases actors are likely to attempt travelling inconspicuously and to avoid wearing distinctive clothing or badging to avoid border LEA scrutiny.

147. **Increases to MVE travel and resulting border screening requirements will be primarily driven by conflicts, anniversaries and aligned events.** While the potential establishing of an area of control for terrorist organisations, such as al Qaeda or ISIL, is the most obvious driver, the emergence of a conflict area aligned with extremist ideologies will possibly increase cross-border extremist travel. Although not as major, anniversary dates for past events or attacks with ideological significance will possibly also influence travel and require increased border screening. This includes potential travel to NZ by extremist entities for the Christchurch Mosque terrorist attack anniversaries. Travel for a repeat or similar attack is assessed as a low probability occurrence.

148. **While FTF return travel across the NZ border is expected to be minimal at this time, increased legitimate passenger volumes provides some cover for extremists.** Few FTF are expected to return imminently, and no visitors to conflict arenas or threat countries are known to be waiting for repatriation. However increased travel from New Zealand to Afghanistan and Somalia, both currently risk regions, could provide opportunities for risk entities to cross the border among a currently increasing passenger flow.

149. **FMVE imports are few, while IMVE-associated imports, mainly publications, increased in recent years, although volumes identified are expected to stabilize rather than grow over the next 1-3 years.** Any increase in IMVE goods (e.g. publications, clothing, signifiers/badges, promotional material) in the next 1-3 years will more likely be driven by continued improvements and refinements to border detection methods than by any notable actual IMVE import increases. Other MVE-related goods imports (e.g. firearms, explosive materials) are not expected to increase. Risk imports associated with FMVE are minimal and also considered unlikely to increase in volume in the near future.

150. **Funding and material support exports for MVE groups and conflict contexts will likely continue, possibly even increase.** As occurred previously, MVE group supporters and sympathizers likely provide funding from NZ, some of which will be illicit cash and monetary instrument transfers. Support goods and funding exports for Ukraine conflict participants has occurred in 2022, and while many such exports are legitimate it is possible illicit exports will also occur, both to the Ukraine conflict region and to others.

151. **Pandemic-driven changes to the border environment provided opportunities to shift resources and identify new areas of threat, and will continue to provide new opportunities for threat assessment in the next few years.** Ongoing investment of analytical resources into the goods environment will likely continue to expand current beneficial outcomes. 6(c) [redacted]

152. **New and developing technology available to NZ Customs Intelligence will help provide new avenues and opportunities for identifying MVE entities at the border.** As passenger volumes return to pre-pandemic levels there will be increased pressure on current resources to maintain goods-related discovery activity. 6(c) [redacted]

RELEASED UNDER THE OFFICIAL INFORMATION ACT 1982

153. **Increased operational collaboration with international partners and B5 working groups will provide new and ongoing opportunities for interdiction and intelligence gathering.** Partner agencies overseas hold key information that will assist in identifying both MVE goods and travel threats before they arrive, particularly holding information on activity indicators that could be leveraged.

6(c) [redacted]

Strategic & Proliferation-related Goods

Threat Rating	6(c) [redacted]

State-linked and other organised threat actors, facilitated by visiting business, education and research actors, continue to attempt export transfers of dual use, restricted and sensitive goods and knowledge from New Zealand.

Intent

- Threat actors are highly motivated to illicitly export strategic goods and knowledge, as well as dual-use technology. Intent is also assisted by confidence in successfully evading border regulations.
- Furthering commercial, technological or militaristic goals strongly drives both state and non-state actors to gain access to strategic goods. Seeking competitive advantage, leveraging opportunities to secure new technology or exploit NZ businesses offloading dual-use technology, economising on their own research and development requirements, or profiting from obtaining restricted goods for third parties continues to motivate threat actors.

Capability

- Threat actors are well resourced and supported to engage in illicit transfers of strategic goods. They have substantial knowledge and training to be able to undertake illicit activity, are able to exploit the covert nature of transfers (e.g. digital/electronic devices), and have ready procurers for goods.
- Threat actors use extensive means to avoid detection by border agencies, with considerable levels of planning and resources dedicated to transfer concealments and avoiding LEA attention and identification.
- NZ's economic, education and research and development relationships with many countries, including some high threat sanctioned nations, also provides proliferation opportunities for threat actors.

OUTLOOK AND OPPORTUNITIES SUMMARY

154. State-linked and other organised threat actors and their agents will continue to attempt to secure and export NZ's goods and knowledge, especially information, data and research. The most likely removal methods are digital or electronic devices or carried by air visitors. Several sanctioned countries will periodically attempt to exfiltrate desired dual-use goods, but most exporting will be commercially sensitive knowledge and innovative technology.

155. NZ's increased protections against exporting will likely drive threat actors to adopt more sophisticated and covert methods. A key response to this will be raising greater threat awareness across academia, research institutions and industry to counter the targeting of the most sought-after goods.

ANALYSIS

6(a) [redacted]

RELEASED UNDER THE OFFICIAL INFORMATION ACT 1982

6(a) [redacted]

6(a) [redacted]

6(a) [redacted]

159. **Transfers of information often occur digitally and electronically, making it hard to detect and intercept exfiltrations.** It is likely that information exports (e.g. scientific and technology information, research, plans, and data) are the most exported 'good', mainly by electronic means. The nature of such transfers and the methods used are very difficult to identify, monitor and control. It is likely threat actors exploit this vulnerability, deliberately arriving to target industry and research facilities (e.g. students, business people, researchers) to access sensitive knowledge and digital goods forms, specifically for the purpose of removal.

160. **New Zealand has enacted legislation tightening overseas investment related to controlled and sensitive technology**. However, closing off investment opportunities, combined with greater reluctance to attract 6(a) [redacted] investment specifically, due to the reputational risk, has possibly incited the use of more covert vectors to acquire research and technology and to exfiltrate them illicitly.

161. **A significant challenge is regulating exports of dual-use technology which has yet to be controlled or may not be feasible to control, but which has military utility.** NZ recently expanded 'catch-all' controls, bringing within scope all goods and technology with a potential military use or for use by the military, paramilitary, militia or police (i.e. not just goods and technology related to weapons of mass destruction (WMD)). It is now easier to control such exports, although ongoing challenges remain with intangible and electronic transfers related to dual-use goods and technologies.

162. **Ongoing conflicts in several regions increased the requirement to monitor sanctioned goods, including ensuring dual-use goods are not exported.** Goods to/from the Russia-Ukraine conflict region are now monitored and restricted to reduce the threat of sanction-busting goods movement. Supporters of conflict participants continually seek ways to provide material support, often in innovative ways (e.g. crowd-funding) and in defiance of sanctions.

OUTLOOK

6(a) [redacted]

RELEASED UNDER THE OFFICIAL INFORMATION ACT 1982

6(a) [redacted]

6(a) [redacted]

165. **Domestic measures undertaken to protect New Zealand against foreign interference will impact the behaviour and methods of proliferation threat actors.** New Zealand is taking further measures to protect against foreign interference, including increasing the awareness of risk within academia and industry, screening NZ government-funded research, and expanding the scope of visa vetting to include sensitive technology (not just WMD as previously). 6(a) [redacted] Threat actors may devote greater resources to managing and facilitating the development of links in a more regulated environment hostile to their aims. 6(c) [redacted]

166. **Threat actors will continue to look for and exploit regulatory gaps in legislation, and to find innovative ways to leverage start-up companies to procure targeted goods and knowledge.** Regulatory gaps relating to research and intangible transfers are exploited in NZ, as is investment in emerging technology start-up companies which can result in acquisitions and the subsequent exfiltration of technology.

167. **A key mitigation strategy and opportunity is to raise threat awareness within academia, research institutions and industry, especially those already targeted or potentially vulnerable.** This helps to reduce inadvertent exports due to a lack of awareness, lowers the risk of passing technology to threat actors and their agents, and increases security awareness around technology access and research holdings, and the security of facilities, systems, information technology and key personnel.

168. **Ongoing cooperation with B5/M5 partners and intelligence sharing with B5/M5 and domestic agencies will assist NZ to be aware of persistent as well as changing threat vectors, as well as enabling targeted operations.** New Zealand has collection capabilities for monitoring this risk domestically, and partners share significant insights on international threats. However, domestic risk visibility is constrained by the nature of covert transfers (especially electronic), resource limitations, and some legislative constraints on the ability to share information across agencies and industry.

6(c) [redacted]

RELEASED UNDER THE OFFICIAL INFORMATION ACT 1982

SPECIAL / SUPPLEMENTARY TOPIC

Cyber-enabled Threats

Threat Rating	6(c) [redacted]

Border threat actors using cybercrime techniques and technologies will increasingly pose significant threats to border-related systems, both within the supply chain, and related to border agencies and NZ Customs

Intent

- Threat actors will increasingly use cybercrime techniques in a variety of cross-border contexts to enable their illicit activities since they are easy to implement, yield good results for effort applied, provide access to protected systems, and largely anonymise the user.
- Threat actors are usually profit-motivated, and cybercrime techniques used to bypass security measures grant system access to hackers and enable actors to facilitate illicit goods movement or concealment are likely to facilitate successful goods trafficking ventures. Additionally, scams, ransomware and phishing attacks supporting fraud activity are also likely to be lucrative. Threat actors are increasingly motivated to exploit the limits of cybercrime legislation and law enforcement ability to track, trace and stop illicit activity.

Capability

- State threat actors and cybercrime-specialising threat groups have the highest capability to penetrate border systems and facilitate crime. They also employ operational security awareness and tradecraft to evade LEA attention and hinder their effectiveness. Due to the asymmetric nature of cybercrime, many different actors are also capable of conducting effective activities and attacks.
- Cybercrime threat actors overseas successfully circumvent cybersecurity systems and are able to undertake attacks in NZ or train NZ-focused threat actors how to operate. Cyber (and cyber-related) criminals are largely based offshore, operating either as individuals or as diverse groups, with well-developed internet competency and connectivity, and high rates of internet accessibility. But domestic threat actors are also able to infiltrate supply chains and use cybercrime techniques to enable illicit activity.

OUTLOOK AND OPPORTUNITIES SUMMARY

169. Borders are increasingly exposed to cybercrime threats as traditional criminals, who may already operate in border areas, look to use cybercrime techniques in support of their illicit activities. Such techniques, both simple and sophisticated, are an especially viable and immediate threat in border-related supply chain contexts. Simultaneously, enhanced border-related digital data collection and storage and an increase in operating with digital technology is increasing the direct threat to border systems posed by cybercrime actors.

    Threat actors will continue to target vulnerabilities at the border and are highly likely to adapt to and exploit new developments, including growing use of automated ports and tracking mechanisms. Techniques and technology currently available will continue to enhance threat actor criminal capability and in most cases will be sufficient for most immediate purposes. Over the next 2-3 years, a plethora of emerging cyber technologies will provide new tools to target a range of border contexts and assist in illicit activities. Cybercrime activity in the border environment is not easy to identify or combat but opportunities exist for border agencies to develop a disruption and defence capability. Staff training, focused risk assessments, enhanced information exchange, and strengthened collaboration with the private sector and overseas partners, will assist in combating border-related cybercrime.

RELEASED UNDER THE OFFICIAL INFORMATION ACT 1982

ANALYSIS

170. **The use of cybercrime techniques and technologies is an increasing threat in the border environment.** Cyber-enabled crime involving border-related systems refers both to using cyber techniques and technology to access and exploit restricted facilities and systems, and to instances where equipment or people used to conduct such activity cross the border. This includes obtaining electronic access to CCA facilities and systems, hacking cargo management systems, using encrypted devices to enable or conceal activity, accessing databases for ransom or information removal, or using cyber techniques to defeat biometric scanning. Although cybercrime occurs across international boundaries, and much of it is 'borderless', some cyber-enabled activity occurs within and/or impacts directly on the border environment (i.e. border-related).

171. **Cyber-enabled crime activity is 'asymmetric' and allows threat actors to inflict a disproportionately large amount of damage on a victim.** The cyber threat arena resembles 'asymmetric warfare' where combatants' relative forces or capabilities differ significantly, or where opposing adversaries use different methods and resources. In the border environment, threat actors can be individuals or crime groups using a few simple techniques and methods to conduct and conceal illicit activity causing significant amounts of system damage at the border, and within border agencies, and cause major harm in economy and the community.

172. **Cybercrime threat actors have high capability to target NZ border-related systems but, to date, have displayed relatively low intentionality.** Cybercrime threat actors (including email scammers, ransom hackers, denial of service (DoS) attackers) have shown high intent to penetrate NZ Customs' systems directly, but have been largely unsuccessful, likely demonstrating limited capability (as well as indicating the effectiveness of NZ Customs' cyber security systems). However, there have been fewer attacks on border-related systems (e.g. freight management and logistics systems, port systems) in NZ. Critical infrastructure is targeted in many countries, and border agencies have been prime targets for attacks. Although successful attacks on border systems in other countries indicate cyber threat actors have high capability and intent, NZ border systems have not been strongly targeted. Even so, multiple successful attacks on other NZ government agencies in recent years (e.g. ransomware attacks on the Waikato District Health Board (2021) and Mercury IT (2022); DDoS attack on Parliament website by NoName057(16) hacker group (2023)) demonstrate threat actors have high capability to engage in cybercrime activity here.[53]

173. **A variety of threat actors are capable of border-related cyber-enabled crime activity.** These include trusted insiders in the supply chain gaining access to border-related systems and facilities, insider threat actors within border LEAs abusing secure access privileges, cyber-criminals and other criminal groups undertaking attacks on border agency systems, and nation state threat actors accessing databases to siphon intelligence or ex-filtrating protected information across the border. Motivations include facilitating or concealing illicit goods movement, obtaining systems or database knowledge, systems disruption or infrastructure compromise, financial reward, or gaining an economic or industry advantage.

174. **Supply chain threat actors using cybercrime techniques are the most immediate and viable at-the-border cyber threat.** Trusted insiders with access to port and airport facilities, supply chain workers, logistics and distribution personnel, and customs brokers can utilise some form of cyber-type technique or activity, from simple abuse of access pass codes to sophisticated cyber penetration or exploitation of databases. Highly capable threat actors have targeted logistics and port systems to facilitate and conceal illicit goods movement. Threat actors not only penetrate port systems to move illicit cargo they also disrupt port operations to

[53] https://www.rnz.co.nz/news/ldr/455535/waikato-dhb-warned-a-cyberattack-catastrophic-for-patient-safety

RELEASED UNDER THE OFFICIAL INFORMATION ACT 1982

compromise supply chain integrity. Ports rely on synchronization and precision, so even small disruptions can cause major goods delays, from which threat actors can profit.[54]

- In early 2022, a cyber attack occurred on oil facility operating systems at several European ports, including Antwerp.[55] Airlines and air freight companies have also experienced an increase in cyber attacks in recent years.[56]

- In July 2021, four major ports in South Africa temporarily closed following a cyber attack on the port operating systems of Transnet National Port Authority, the country's main freight manager.[57] In August 2021, hackers exploited a software flaw in the password management system at the Port of Houston, allowing hackers to manipulate information systems to facilitate several activities including extracting sensitive data and installing malware.[58]

- In 2011, drug trafficking OCGs recruited hackers to breach IT systems controlling container movement and location at the Port of Antwerp over a two-year period, indicating OCGs with cyber-attack capability have undertaken targeted attacks for some time and that some attacks can occur over a sustained period.[59]

175. **The cybercrime capability of nation state threat actors is substantial, often possessing high levels of expertise and resource as well as ability to mount multiple coordinated attacks.** There is no evidence nation states have undertaken cybercrime activity at the NZ border beyond facilitating the exfiltration of digitised information (e.g. research data, commercially sensitive material) via visitors or web-based platforms.

176. **A variety of threat actors are increasingly utilising digital technology, which may include some capability to undertake a range of cybercrime-type activities.** Alongside upskilling with new technology and techniques that facilitate and conceal criminal activity, some crime groups leverage cyber services and products offered by cyber-criminal groups. Some services and products, many of which are available on Darkweb platforms, can help facilitate illicit behaviour across borders, For example, the Onion Router (TOR) browser, Invisible Internet Project (I2P) and other anonymising services provide layers of encryption that help conceal and anonymise Darkweb users. Both the cyber-crime and concealment-facilitating technology and techniques available from the Darkweb provide a significant increase in criminal capability for some OCGs and border threat actors.

177. **Threat actors are likely aware of NZ Customs' increasing use of digital systems and seek ways to exploit this.** Increased use of digital technology offers advantages by enhancing functionality and capability and reducing human error. However, as systems and processes steadily become more sophisticated, the vulnerabilities associated with an increasingly complex environment also increase and are exploited by attackers. Border agencies increasingly rely on third party software and service providers to provide or enhance border management systems. Although a necessity, using such providers expands the vectors threat actors can exploit. The proliferation of hardware and software (PCs, routers, operating systems, laptops, etc.) are all assets vulnerable to cyber attacks. Increased automation in border control requires databases and algorithms which may not function if they are modified illicitly. NZ Customs' databases contain personal data, documents, or files, providing an

[54] https://www.dhs.gov/news/2022/03/21/secretary-mayorkas-delivers-remarks-maritime-and-control-systems-cybersecurity
[55] https://www.securityweek.com/european-oil-port-terminals-hit-cyberattack
[56] https://www.shlegal.com/insights/aviation-is-facing-a-rising-wave-of-cyber-attacks-in-the-wake-of-covid
[57] https://www.reuters.com/article/us-transnet-cyber-idUSKBN2EZ0RQ; https://www.reuters.com/world/africa/exclusive-south-africas-transnet-hit-by-cyber-attack-sources-2021-07-22/
[58] https://www.stormshield.com/news/cybermaretique-a-short-history-of-cyberattacks-against-ports/
[59] https://www.bbc.com/news/world-europe-24539417

RELEASED UNDER THE OFFICIAL INFORMATION ACT 1982

attractive target for malicious actors. Network connectivity is upgraded to connect different systems, which also increases the access points for malicious actors. Wireless communications (e.g. satellite-based communications, Unmanned Aerial Vehicles (UAV)) are vulnerable to hacking, which threatens the effectiveness of surveillance.

OUTLOOK

178. **In the next 2-3 years, threat actors will likely use more cybercrime techniques to enable cross-border crime**. Use will most likely occur in NZ's supply chain environment, likely by trusted insiders, and possibly direct attacks on border systems (e.g. ports/airport systems, cargo tracking systems) will also occur. Direct attacks on NZ Customs' systems and databases will likely continue, but no successful penetration has been noted in recent years. It is also unlikely insider threat actors will undertake any damaging activity, but the possibility cannot be discounted.

179. **Techniques and technology currently available to threat actors will continue to enhance their criminal capability and, in most cases, will be sufficient for immediate purposes.** The multitude of threat actors, the increasing use of digitisation in border environments, the types of illicit actions occurring (e.g. security access bypassing, system penetration), and opportunities presented by successful cybercrime techniques, blockchain technology, cryptocurrencies and NFTs, will almost certainly enable threat actors to conduct illicit activity with a high degree of anonymity, including money laundering, illicit goods movement, system disruption and exploitation, data theft and even misinformation campaigns. The cybercrime techniques and technology already utilised will continue be used by those threat actors that have had some success and will likely also be adopted by others as they see the potential for success and upgrade their capability.

180. **New cyber technologies and techniques will provide new opportunities for criminal exploitation and will almost certainly further enhance border threat actor capabilities, especially the more that border agencies adopt digital technology.** A range of technology types will be exploited criminally, including 5G devices which have greater connection capabilities and data transfer volumes and speeds. Artificial intelligence and machine learning capability will allow cybercriminals to automate attacks and increase their sophistication. Edge computing, where data computation and retrieval does not occur across large networks but sits much closer to the device, will reduce disruption to criminal devices by LEAs and likely allow greater threat actor access to target devices and systems that are not well protected. The internet of things (IoT) will also be exploited more, since many smart devices with internet connection used by businesses and individuals are vulnerable to 'hacking' (i.e. unauthorized access to data in a system or computer) and redirected for criminal use. Quantum technology will allow hacking, system penetration and security bypassing at exponentially greater speeds and will reduce or remove the effectiveness of passwords and encryption.[60] Such technologies will likely be exploited progressively in the future, although it is unknown how quickly criminal uses will occur in the border environment.

181. **New technology uptake will be uneven and determined by threat actor intent and resources.** Although the capability and technology for significantly advanced forms of cybercrime activity exists now and will only increase, it is more likely that most border threat actors will persist with tried, tested and easier cybercrime methods in the immediate future.[61] Advanced technology uptake by most border threat actors will likely not be rapid since much of it is not well understood, is expensive or not readily available, and requires technical

[60] NAC(21)344 Top Technology Trends Impacting on SOC in 2026, National Crime Agency, July 2021; https://www.rand.org/pubs/research_reports/RRA137-1.html; https://www.rand.org/randeurope/research/projects/technological-developments-and-the-future-of-cybercrime.html; https://home.kpmg/ae/en/home/insights/2020/05/the-risk-of-cybercrime-and-emerging-technologies.html

[61] National Strategic Assessment (NSA) 2021, National Crime Agency (NCA); Cybercrime and Cryptocurrency Advisor, UNODC Regional Office for Southeast Asia and the Pacific, 8 December 2021; https://www.mas.co.nz/hub/cyber-crime-during-the-covid-19-pandemic/

RELEASED UNDER THE OFFICIAL INFORMATION ACT 1982

expertise to use and exploit.[62] There is still sufficient scope for success and expansion with existing methods and technology.

182. **Cybercrime activity in the border environment is not easy to identify or combat, but opportunities exist for border agencies to develop understanding and mitigation capability.** Cybercrime actors are hard to detect, disrupt and prosecute, operate with relative impunity and have an understanding that it is often difficult to trace their activities. A variety of operating and technology advantages available to cyber criminals, many cyber-environment user vulnerabilities to exploit, and limitations on LEA capabilities and resources assist cybercrime groups to avoid interdiction, remain hidden and continue operating.[63] However, increasing use of digital systems also necessitates a commensurate awareness of their vulnerabilities. Disruption is possible with dedicated use of cyber technology and expertise, increased awareness of cybercrime actor methods and vulnerabilities and commensurate NZ Customs training, fit-for-purpose legislation and regulations, coordinated cooperation and information exchange with other LEAs, and developing relationships across LEAs, academia, and private/business sectors to leverage all the available expertise.

6(c) [redacted]

RELEASED UNDER THE OFFICIAL INFORMATION ACT 1982

[62] Cybercrime and Cryptocurrency Advisor, UNODC Regional Office for Southeast Asia and the Pacific, 8 December 2021

[63] Transnational Criminal Organizations Almost Certainly Diversifying Use of Encrypted Platforms, Impeding Collection Capabilities, Strategic Perspective: Executive Analytical Report (SPEAR), 16 August 2021, Federal Bureau of Investigation (FBI); Crypters: enabling malware to evade detection, ACIC, 21/71214, 19 November 2021

Threat Rating Methodology Explanation

Threat ratings are based on the assessed Intent and Capability of threat actors undertaking a particular activity that occurs at the border or impacts on the border or border agency.

Intent - The culmination of an intentional threat actor's confidence and desire.

Capability - The culmination of an intentional threat actor's resources and knowledge.

The threat ratings in this assessment are based on the Intent and Capability scores derived from the NZ Customs Threat Survey responses.[64] The survey assesses threat ratings from a set of factors and elements pertinent to Intent and Capability using a scoring range of 1-5 (1 = Very Low, 5 = Very High). The separate survey scores for Intent and Capability are translated into the Intent and Capability ratings, and then combined using the table below to find the overall threat level for each topic assessed.

Threat Elements	INTENT				
CAPABILITY	**VERY HIGH**	**HIGH**	**MEDIUM**	**LOW**	**VERY LOW**
VERY HIGH	Very High	High	High	Medium	Medium
HIGH	High	High	Medium	Medium	Low
MEDIUM	High	Medium	Medium	Low	Low
LOW	Medium	Medium	Low	Low	Very Low
VERY LOW	Medium	Low	Low	Very Low	Very Low

Note: The Threat Matrix aligns with the B5/M5 Heads of Intelligence (HINT) Joint Strategic Threat Assessment (JSTA) threat matrix, in order to maintain consistency with international standards.

Threat Rating Descriptions

VERY HIGH: Current and future actor threat activity is Very High. Extensive threat activity will continue or commence within three years. Actors are driven, resilient, and readily able to exploit vulnerabilities and enablers to circumvent border controls and measures.
HIGH: Current and future actor threat activity is High. Threat activity will continue or is highly likely to commence within three years. With some effort, actors with intent can exploit vulnerabilities and enablers in response to changes in border controls and measures.
MEDIUM: Current and future actor threat activity is Medium. Some threat activity occurs or will likely commence within three years. With some difficulty, intentional actors may be able to exploit vulnerabilities and enablers in response to changes in border controls and measures.
LOW: Current and future actor threat activity is Low. Limited threat activity possibly occurs or may occur within three years. Actors have some capability to exploit vulnerabilities and enablers, but are unable to act or have little or no intent to seek alternate methods in response to changes in border controls and measures.
VERY LOW: Current and future actor threat activity is Very Low. Threat activity is unlikely to occur within the next three years. Threat actors, many of whom are individual or opportunistic actors, generally lack the intent or have limited capability to exploit vulnerabilities and enablers to circumvent border controls and measures.

[64] These ratings are pre-determined from and align with NZ Customs' response to the HINT B5/M5 Joint Strategic Threat Assessment (JSTA) each year.

RELEASED UNDER THE OFFICIAL INFORMATION ACT 1982

Threat Scoring Method

The threat ratings are determined from responses to a set of statements applied to each threat Intent and Capability category (four Intent, four Capability) (see below).

Each statement under the sections is scored from 1-5. Intent and Capability scores are collated, and the total scores are converted into overall threat ratings determined from the chart in Fig.1.

Fig.1 Intent & Capability Scoring

Intent and Capability	
17-20	VERY HIGH
13-16	HIGH
9-12	MEDIUM
5-8	LOW
1-4	VERY LOW

Intent and Capability Survey Statements

<u>Intent</u> (actor willingness and determination to pursue their aims)

- **Intensity: The level of diligence and determination actors display to bypass or exploit border controls**
  - e.g. The sophistication levels of threat actor concealment methods
  - e.g. The volumes of illicit goods smuggled, and the routes used

- **Stealth (actor): The extent to which actors attempt to avoid detection to bypass or exploit border controls**
  - e.g. The levels of willingness to use social media or encryption methods noted
  - e.g. The use made of false identities

- **Stealth (activity): The extent to which actors attempt to avoid the detection of goods/people moved or knowledge transfers to bypass or exploit border controls**
  - e.g. The use of technology, including encryption, to avoid detection
  - e.g. The use of false origin or concealment methods in actor supply chains

- **Time: The time actors dedicate to planning, developing, and deploying methods to bypass or exploit border controls**
  - e.g. The level of planning and preparation evident in expediting smuggling activity
  - e.g. The longevity of smuggling or illicit border-related activity

<u>Capability</u> (actor ability and resource availability in pursuit of their goals)

- **Personnel and networks: People, groups, associations, and specialists actors are able to utilise to bypass or exploit border controls**
  - e.g. Specialist skills, including third party or professional facilitators, actors utilise
  - e.g. Collaborations and associations with other groups or willing threat actors

- **Knowledge (technical): Theoretical and practical knowledge related to technical aspects of threats and activity that bypasses or exploits border controls**
  - e.g. Actor understanding and manipulation of border processes or procedures
  - e.g. Skill levels evident in manufacturing illicit goods

- **Knowledge (logistical): Theoretical and practical knowledge of goods and people movement and how to evade and/or exploit border controls**
  - e.g. The level of knowledge about supply chain logistics
  - e.g. The transport modes and streams that illicit goods are smuggled in

- **Access (to restricted systems): Actor's ability to access or exploit any border-related systems, facilities, and personnel before, at, and after the border**
  - e.g. Utilising insider threat actors in supply chains or border agencies
  - e.g. Ability to secure access passes or penetrate restricted access systems.

RELEASED UNDER THE OFFICIAL INFORMATION ACT 1982

Glossary & Abbreviations

Glossary

501 deportee	Deportees from Australia, named after the character section of the Australian Migration Act allowing cancellation of a visa. Pacific Island nation law enforcement agencies use the term 'returnee'.
Alt tech	Alt tech are social media platforms and internet service providers that moderate content less strictly than mainstream platforms/providers. Such platforms are popular with threat actors espousing extreme or fringe opinion.
Border cash report (BCR)	A declaration of cash moving or being received across NZ's border.
Bearer negotiable instruments (BNI)	Alternative form of cash that is not currency, and Includes bills of exchange, cheque, promissory notes.
Customs controlled area (CCA)	Customs controlled areas (CCA) are secure, controlled areas where NZ Customs maintains authority to monitor or conduct activities.
Child sex exploitation (CSE)	Child sex exploitation (CSE) and child sex exploitation material (CSEM) are terms used in NZ. Other/overseas agencies also use child sex abuse (CSA), child sex abuse material (CSAM), and child abuse material (CAM).
Corflute	Corflute is polypropylene co-polymer sheeting, often corrugated, often used as packaging, signage, and protective cladding.
Counterfeit and fake goods	Counterfeit goods are legitimately made (licensed) goods that are diverted, trafficked and used or sold by unauthorised agents. Fake goods are illegitimately manufactured or unlicensed goods imported/exported for use or sale. Both are covered under trademark-infringing goods (IPR).
Cryptocurrency (crypto)	A form of digital currency, an alternative form of payment created using encryption algorithms. Encryption technologies allow cryptocurrencies to function both as a currency and as a virtual accounting system.
Crypto wallet	A storage place for cryptocurrencies on a digital device. Cryptocurrency use requires a wallet.
Cybercrime	Cybercrime is criminal activity involving an internet-connected device (e.g. cell phone, computer, smart device) either used to commit crimes or as a target for crime activity. Also known as cyber-dependent crime.
Cyber-enabled crime	Cyber-enabled crime is criminal activity where technology (often digital) has been used to enhance another crime (e.g. fraud) but which does not require internet use.
Daigou	A form of exporting where individuals or syndicated groups outside China purchase goods for customers in China which are then sold for profit. Also known as surrogate shopping, daigou is used both legally and illicitly.
Denial of service attack (DoS & DDoS))	Denial of service (DoS) attacks aim to shut down a machine or network making it inaccessible for intended users. Distributed DoS (DDoS) attacks use multiple systems to flood the bandwidth or resources of a target system.
Digital currency	A currency that is only accessible using digital technology (e.g. computers, mobile phones), including cryptocurrencies.
Edge computing	Edge computing allows data processing on networks or devices closer to where it is being generated and to the user, enabling processing at greater speeds and volumes, leading to greater action-led results in real time.
Encrypted communication device	A mobile electronic device specifically designed or equipped with encryption capability. Known as dedicated encrypted communication devices (DECD).
Flobert firearms	Flobert firearms are gallery, parlour, or saloon firearms designed for recreational indoor target shooting.
Free Trade Zone (FTZ)	A special economic zone, a geographic area where goods are imported, stored, handled, manufactured, or reconfigured and re-exported under specific customs regulation and often not subject to customs duty.
Goods & services tax (GST)	NZ tax added to the price of most goods and services, including imports.
Green technology	Green technology (or green tech) is an umbrella term describing the use of technology and science (both research and actual technology) to reduce human impacts on the natural environment.
Grey/black market firearm	Grey market refers to the holding or transfer of firearms or parts legally owned but not declared, surrendered or registered when required, e.g. after a legislation change. Black market is any illicit sale, transfer or obtaining of firearms or parts.

RELEASED UNDER THE OFFICIAL INFORMATION ACT 1982

Hawala	Hawala (aka underground banking) is an honour-based form of informal money/value transmission (remittances) without any currency actually moving.
Hawaladars	People who act as money/value transmitters in the hawala system.
Informal Value Transfer System (IVTS)	Any system, mechanism, or network of people, often operating outside the conventional financial sector, that receives money or value instrument to make funds or an equivalent value payable to a third party in another geographic location.
Insider threat	Insider threat refers to employees/contractors working in LEAs who are, or could become, threat actors and facilitators. (see trusted insider)
Internet of things (IoT)	Internet of things is a network of interrelated internet-capable devices connecting and exchanging data with other IoT devices (often via the Cloud).
Motivated violent extremism (MVE)	MVE includes Politically-Motivated Violent Extremism (PMVE), Identity-Motivated Violent Extremism (IMVE), Faith-Motivated Violent Extremism (FMVE), and Single Issue-Motivated Violent Extremism (SMVE).
Money service business (MSB)	Money service businesses, including non-bank financial institutions, transmit or convert money.
New Zealand Adult Gang (NZAG)	NZ adult gangs are organised criminal groups other than domestic OMCGs, but which operate similarly. These have been identified and included in the NZ Police's National Gang List (NGL) of patched and prospect membership.
Personally-made firearms (PMF)	PMFs are firearms (including a frame or receiver) completed, assembled or otherwise produced by a person other than a licensed manufacturer. Also known as 'ghost guns', but this is a media term, not an official LEA term.
Professional money launderer (PML)	Individuals or groups who, for a fee, provide services to organised crime groups by laundering the proceeds of their criminal activity.
Quantum computing	A developing technology harnessing the laws and capability of quantum mechanics to solve problems beyond the capability of classical computers.
Risk & Intelligence (R&I)	NZ Customs' primary border risk identification and targeting system.
Smart contracts	Often used with cryptocurrencies, they are computer programs or transaction protocols that activate automatically when pre-set conditions are met. They execute, control or document events and actions according to agreed terms and are used to simplify and secure transactions between parties.
Synthetics	Synthetic drugs (aka designer drugs) and precursors are created using artificial or man-made chemicals rather than natural substances, often with the aim of mimicking natural or plant-based drugs.
Tariff	The Working Tariff Document of New Zealand
Te Kuaha (The Gateway)	NZ Customs' web-based query tool for Customs data.
Third party facilitator	Individuals or groups, often professionals and businesses, who provide expertise, services and assistance to threat actors, either directly and intentionally or indirectly and unknowingly. Many of these operate normally in legitimate capacities.
Tornado cash	An open source, non-custodial, decentralized cryptocurrency tumbler running on digital currency platforms. The service mixes potentially identifiable or 'tainted' crypto funds with others to obscure the fund's original source.
Trade Single Window	Trade Single Window is a facility in NZ Customs' Joint Border Management System (JBMS) providing a single portal for importers, exporters and their agents to submit required border information and to receive responses.
Transnational Organised Crime (TNOC)	TNOC is also known as Transnational Serious Organised Crime (TSOC) or Transnational Organised Crime (TOC) in overseas agency reporting.
Trusted insider	Trusted insiders are employees/contractors working in trusted positions inside supply chain businesses/facilities (e.g. marine ports, airports, customs brokers, freight forwarders, logistics companies). (see insider threat)
Vape device	Electronic nicotine delivery system or instrument.
Virtual asset service providers (VASP)	People or businesses engaged in types of activities and services related to virtual assets (VA). VAs are digital representations of value (e.g. cryptos) which can be digitally traded or transferred, and are used for payment or investment purposes.

RELEASED UNDER THE OFFICIAL INFORMATION ACT 1982

Abbreviations

AML/CFT	Anti-Money Laundering and Countering Financing of Terrorism Act 2009
AOC	Asian organised crime
ATF	Bureau of Alcohol, Tobacco and Firearms
AVTI	Alternative value transfer instrument
B5/M5	Border 5
BCR	Border cash report
BNI	Bearer negotiable instruments
CBP	Customs Border Protection (U.S.)
CBSA	Canada Border Services Agency
CCA	Customs Controlled Area
CEM	Chile exploitation material
CEOT	Child Exploitation Operations Team
CITES	Convention on International Trade in Endangered Species of Wild Fauna and Flora
CSE	Child sex exploitation
CSEM	Child sex exploitation material
DDoS	Distributed denial of service
DECD	Dedicated encrypted communication device
DOC	Department of Conservation
DoS	Denial of service
EPA	Environmental Protection Authority
EPH	Ephedrine
FCU	Financial Crime Unit
FMVE	Faith-motivated violent extremist
FTA	Free trade agreement
FTF	Foreign terrorist fighter
FTZ	Free trade zone
HINT	Border 5 Heads of Intelligence
ICR	Inwards cargo report
IED	Improvised explosive device
IMVE	Identity-motivated violent extremist
IoT	Internet of things
IPR	Free trade agreement
IPONZ	Intellectual Property Office of New Zealand
ISIL	Islamic State of Iraq and the Levant
IVTS	Informal value transfer system
LO	Liaison officer (NZ Customs)
MBIE	Ministry of Business, Innovation and Employment
MFAT	Ministry of Foreign Affairs and Trade
MfE	Ministry for the Environment
MPI	Ministry for Primary Industries
MSB	Money service business
MVE	Motivated violent extremist
NDIB	National Drugs Intelligence Bureau
NFT	Non-fungible token
NZAG	New Zealand adult gang
NOCG	National organised crime group
NPS	New psychoactive substance
NZ Police	New Zealand Police

RELEASED UNDER THE OFFICIAL INFORMATION ACT 1982

OCG	Organised crime group
OMCG	Outlaw motorcycle gang
PIC	Pacific Island country
PIED	Performance and image-enhancing drug
PML	Professional money launderer
PSE	Pseudoephedrine
PMF	Personally made firearm
R&I	Risk and Intelligence (NZ Customs)
RSE	Recognised seasonal employer
SVC	Stored value card
TAM	Traditional Asian medicines
TBML	Trade-based money laundering
TIES	Trade in Endangered Species Act 1989
TNOC	Transnational organised crime
TOR	The Onion Router
TSW	Trade Single Window
UNODC	United Nations Office on Drugs and Crime
VASP	Virtual service asset provider
WCO	World Customs Organisation
WMD	Weapons of mass destruction

RELEASED UNDER THE OFFICIAL INFORMATION ACT 1982

APPENDIX A

CLASSIFICATION

This document is the property of the New Zealand Customs Service (NZ Customs) and is classified as ~~**RESTRICTED**~~. No reclassification, duplication or dissemination of this document, or the intelligence it contains, can occur without express permission of the Manager, Intelligence, NZ Customs. This intelligence is to be deleted/destroyed once it has been used for the purpose for which it was produced.

CONDITIONS RELATING TO INFORMATION DISCLOSED WITHOUT A WRITTEN AGREEMENT IN PLACE

INTRODUCTION

1. This information is disclosed in accordance with section 318 of the Customs & Excise Act 2018.

2. The use of the information is disclosed subject to the conditions of use contained in this appendix.

PURPOSE

3. The New Zealand Customs Service is disclosing this information to you in order to assist in the prevention and detection of customs offences or offences punishable by imprisonment.

USE OF INFORMATION

4. In using, storing, or disclosing information in accordance with this appendix, you and your agency will act in accordance with any domestic information handlings laws and policies.

5. The information disclosed pursuant to this appendix will, regardless of form, be treated as being made or supplied in strict confidence and must only be used for the purposes identified in section 318.

6. The information is disclosed for intelligence purposes only and may not be otherwise used (including for evidential purposes) or further disclosed without obtaining the written approval of the New Zealand Customs Service.

SECURITY OF INFORMATION

7. You and your agency are to have security safeguards in place (including electronic safeguards) to protect the information against loss and unauthorised access, use, modification, disclosure or other misuse.

8. Access to the information is to be limited to only those personnel within your agency to whom access is necessary and such access does not conflict with this appendix.

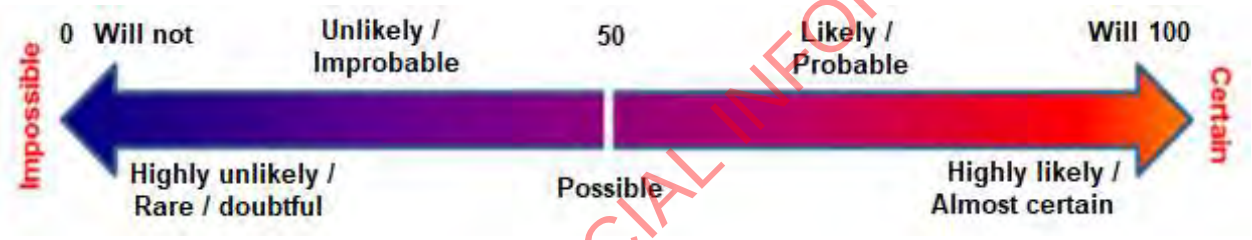
RELEASED UNDER THE OFFICIAL INFORMATION ACT 1982

ESTIMATIVE LANGUAGE

Certain words are used in this assessment to convey confidence and analytical judgement about the probability of a threat, development or event occurring. Judgements are often based on incomplete information and are not fact, proof or knowledge. The terms 'may', 'could', 'might', 'would', and such-like are indicative only but are not definitive probability terms and are not to be interpreted as an intention to formally assess probability. The phrases/words in the Probability Statements in the Guidance table below are the formal assessment terms.

Guidance: Probability table - the chance that an activity or threat will occur?

Probability Statement	Qualitative Statement	Probability %
Almost certain	The event will occur in nearly all circumstances	>95%
Likely / Probable	The event will occur in many/most circumstances	>65%
Possible	The event might/may/could occur some of the time	>35%
Unlikely / Improbable	The event could occur in only a few circumstances	<35%
Rare	The event has a remote chance of occurring	<5%



DOCUMENT PRODUCTION

Strategic Intelligence, New Zealand Customs Service

Product number: 6(c) [redacted]

Release Date: November 2023

DISSEMINATION LIST

New Zealand Customs Service

6(c) [redacted]

RELEASED UNDER THE OFFICIAL INFORMATION ACT 1982