



КИЇВСЬКА ШКОЛА ЕКОНОМІКИ
МАГІСТЕРСЬКА ПРОГРАМА З ПУБЛІЧНОЇ ПОЛІТИКИ ТА ВРЯДУВАННЯ

ДИПЛОМНА РОБОТА
«Невидимі зв'язки: характеристики мереж, які обходять міжнародні санкції»

Студент: Стеблівський Р.Є.

Науковий керівник: кандидат політичних наук, Гомза І.А.

Для здобуття освітнього ступеня: Магістр
за спеціальністю: 281 Публічне управління та адміністрування

Київ 2024

ЗМІСТ

АНОТАЦІЯ.....	2
ВСТУП.....	3-5
ОГЛЯД ЛІТЕРАТУРИ.....	6-9
АНАЛІТИЧНА РАМКА ДОСЛІДЖЕННЯ.....	10-13
МЕТОДОЛОГІЧНИЙ ДИЗАЙН.....	14-15
ДОСЛІДЖЕННЯ І РЕЗУЛЬТАТИ.....	16-25
ДИСКУСІЯ ТА ІНТЕРПРЕТАЦІЇ.....	26-28
РЕКОМЕНДАЦІЇ.....	29
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ.....	30-32
ДОДАТКИ.....	33-203
<i>Додаток 1. Вузли та зв'язки мереж 1-6.....</i>	<i>33-42</i>
<i>Додаток 2. Матеріали кримінальних справ кейсів 1-6.....</i>	<i>42-203</i>

АНОТАЦІЯ

Дослідження міжнародних санкцій часто ставлять перед собою питання ефективності санкцій проти країни-цілі. Одним із основних факторів ефективності міжнародних санкцій є протидія схемам обходу цих санкцій, основою яких є мережі людей та компаній у різних країнах світу. Науковці використовують мережевий аналіз для дослідження мереж терористів, наркаторговців та транснаціональних злочинців, але досі майже не застосовували цей метод для аналізу мереж, що обходять міжнародні санкції. У цій роботі ми проаналізували окремі мережі злочинців, які експортували підсанкційні товари для російського військово-промислового комплексу з США, з метою визначити характеристики цих мереж. Та встановили, що ці мережі мають відносно високий рівень централізації, а кожна із мереж має один або декілька вузлів з набагато вищим рівнем центральності за інші вузли мережі.

Ключові слова: мережевий аналіз, міжнародні санкції, Росія, центральність.

Кількість слів: 6718

ВСТУП

Після початку повномасштабного вторгнення Росії в Україну та запровадження міжнародних санкцій проти Росії основною проблемою у сфері санкцій став обхід санкцій. Про це свідчать дані журналістів розслідувачів («EU goods worth», 2023), аналітичних центрів (Vilousova et al., 2024) і органів контролю країн санкційної коаліції. Наукова дискусія у сфері санкцій намагається дати відповідь на питання, чи ефективні санкції взагалі, при цьому дослідження саме способів обходу санкцій лише набуває популярності (Allison et al., 2023).

Схеми обходу санкцій відрізняються між собою в залежності від типів санкцій, які вони обходять. У 2016 році більше половини всіх міжнародних санкцій мали «смайт» формат, який забороняє конкретні операції конкретним особам (Felbermaur et al., 2021). У контексті санкцій проти Росії після 2022 року, зазвичай, йдеться про заборону експорту до Росії конкретних товарів або заборону на проведення будь-яких фінансових чи торгівельних операцій з визначеними підсанкційними особами. Саме таким підходом країни санкційної коаліції проти Росії намагаються послабити доступ Росії до товарів подвійного та військового призначення.

Європейський Союз разом із міжнародними партнерами (США, Великобританія, Японія) створили список товарів (List of Common High Priority Items), пріоритетних для російського військово - промислового комплексу, який регулярно оновлюється: *«Ці елементи включають електронні компоненти, такі як інтегральні схеми та трансиверні модулі, а також предмети, необхідні для виробництва та тестування електронних компонентів друкованих плат і виготовлення високоточних складних металевих компонентів, отриманих на полі бою»* («List of common high priority items», 2024, р. 1). Експорт цієї продукції заборонений до Росії регламентом 833/2014.

У США є схожий інструмент заборони на експорт критичних для Росії товарів. Йдеться про Регламент адміністрування експорту (Export Administration Regulation), в межах якого визначено 9 категорій особливо важливих товарів (Bureau of Industry and Security).

І саме ці санкції Росія намагається обходити, використовуючи різноманітні схеми. При цьому станом на 2024 рік Росія продовжує використовувати ці схеми та закуповувати критичні товари з «третіх країн» (Vilousova et al., 2024).

Позицію третіх країн та обходи санкційних режимів різні дослідники пояснюють економічними (Early, 2009), геополітичними (G. Hufbauer et al., 2008; Hellquist, 2016), бізнесовими (Early, 2009; Allison et al., 2023) факторами, проте однозначної відповіді на питання про те, якими ж характеристиками володіють ці мережі, що обходять міжнародні санкції, немає.

При цьому основні актори, які обходять санкції, є навіть не держави, а компанії та фізичні особи. Держави є гравцями на міжнародній арені, адже держави приймають

рішення про зміну політик, початок чи завершення збройних конфліктів, приєднання чи ігнорування міжнародних санкційних режимів. Проте саме приватні компанії та люди є акторами, які будують мережі, налагоджують міжнародну взаємодію для обходу обмежень.

Основою схем обходу цих санкцій є мережі людей та компаній у третіх країнах: *«Основний висновок нашого аналізу полягає в тому, що прями продажі та поставки з країн коаліції, що контролюють експорт, в основному були замінені транзакціями, які включають посередників із третіх країн»* (Bilousova et al., 2024, p.10).

Обхід санкцій прийнято вважати певним ланцюжком, який складається із багатьох компаній та осіб, розташованих у різних країнах для світу (Burne, et al., 2023). Проте чи справді у цих ланцюжках всі ланки незалежні одна від одною? Чи все такий у мережі може бути присутній основний організатор або група організаторів всієї схеми, а сам «ланцюжок» може бути радше мережею, ніж ланцюгом? В межах цієї роботи на основі кейсів я прагну показати, що поняття «ланцюжок» є не зовсім коректним по відношенню до мереж, які обходять міжнародні санкції, адже кожна така мережа має основних організаторів цих схем.

Мережевий аналіз для розслідувань міжнародних мереж злочинців використовується не вперше. У 2002 році мережевий аналіз був використаний для дослідження мережі терористів, які здійснили атаку в США у вересні 2001 року (Krebs, 2002). Julei (2014) вивчав мережу терористичних організацій у Східному Туркестані. У 2013 році Bright та Delaney (2013) використали мережевий аналіз для аналізу еволюції мереж торгівлі наркотиками у 1991-1998 роках в Австралії.

Проте досі науковці не застосовували цей метод для аналізу іншого типу злочину – обходу міжнародних санкцій. Таким чином, це є **прогалиною** у дослідженні міжнародних санкцій та мереж, які намагаються їх обходити. Саме тому я ставлю **аналітичне питання таким чином**: «Якими характеристиками володіють мережі, що обходять міжнародні санкції?».

Методологічний індивідуалізм є основною рамкою цієї роботи, адже у цих мережах роль основних організаторів мереж відіграють саме окремі індивіди та компанії, поведінка яких формує структури та характеристики цих мереж. Досліджувати санкційні режими можна і з точки зору структурного функціоналізму, фокусуючись безпосередньо на органах влади, які запроваджують санкції, та їхній взаємодії між собою. Цей підхід може допомогти пояснити структуру міжнародних санкційних режимів загалом. Проте дослідження окремих мереж людей та компаній повинно фокусуватись саме на діях людей, а не інституцій, та їхньому впливі на функціонування мереж. Саме тому методологічний індивідуалізм був обраний для цієї роботи.

Я обираю **пошуковий дизайн дослідження**, адже хочу дослідити характеристики мереж, що обходять міжнародні санкції на прикладі окремих кейсів

мереж. Наукова дискусія досі не дала відповідей на питання, яким чином влаштовані мережі, що обходять міжнародні санкції, і не запропонувала чітких гіпотез, які можна було б перевірити. Саме тому ми можемо формулювати лише теоретичні очікування в рамках саме пошукового дизайну.

ОГЛЯД ЛІТЕРАТУРИ

Поняття «санкції» може мати різні визначення. Наприклад, санкції можуть означати покарання за порушення певних правил, коли монополія держави на насилля та покарання переноситься у логіку міжнародних відносин, де держава може покарати за порушення правил іншу державу (Ruys, 2017). У цьому випадку «санкції» виступають синонімом до слова «покарання» або «реакція». У дискусії про ефективність санкцій таке визначення можна віднести до підходу санкцій як сигналу. Коли уряди одних країн вводять не дуже ефективні обмеження з метою не покарати реальними обмеженням, а дати сигнал про свою позицію. Санкції також можна сприймати як перелік дій міжнародних організацій, які вони можуть вчинити по відношенню до своїх членів за порушення правил організацій (Ruys, 2017). Таке визначення також підходить до визначення санкцій як реакції на певні дії.

Проте у нашому випадку йдеться про *«підхід, відомий у теорії міжнародних відносин, який визначає санкції за типом вжитих заходів і тлумачить їх як посилення на економічні санкції, такі як імпорتنі та експортні обмеження щодо певних країн або заморожування активів, спрямованих проти конкретних осіб чи організацій»* (Ruys, 2017, с. 1). Саме цей тип санкцій використовують ЄС та США, коли формують списки товарів, заборонених на експорт до Росії, а також списки осіб та компаній, з якими західному бізнесу заборонено мати торгівельні та фінансові операції.

У літературі такий підхід ще називають «смайт» санкціями або «таргетованими» санкціями (Tostensen & Bull, 2002). Він полягає тому, що санкційні обмеження повинні стосуватися безпосередньо тих, хто відповідальний за певну політику держави-цілі, яку санкції прагнуть змінити, а не всього населення певної країни. Часто йдеться про фінансові санкції проти компаній та заборони на пересування фізичним особам (Felbermaug et al., 2021). Felbermaug та інші зауважують, що у 1950 «смайт санкції» стосувались однієї третини усіх міжнародних санкцій, тоді як у 2016 – більше половини всіх санкцій (2021, р.8.)

Саме цим «смайт» підходом до санкцій після 2022 року користується, наприклад, Європейський Союз, забороняючи торгівлі або з окремими особами, або товарами «високої пріоритетності» для російського військово - промислового комплексу.

Наукових публікацій, присвячених обходам Росією міжнародних санкцій, не так багато. Проти серед тих робіт, які намагаються розкрити цю тему, однією із основних характеристики мереж, які обходять санкцій, є реєстрація компаній чи використання компаній з так званих «третіх країн». Треті країни – це країни, які не є ані організаторами, ані «цілями» санкцій (Allison, 2023, с.5). До країн санкційної коаліції Національне агентство із запобігання корупції України, які веде профільний сайт «Війна та санкції», вносить країни-члени ЄС, США, Канаду, Японію, Великобританію, Австралію та Нову Зеландію («База даних санкцій, застосованих після нападу Росії на Україну»). Проте навіть санкції цих країн-партнерів не співпадають у багатьох

аспектах, тому неможливо дати більш точне визначення поняттю «треті країн», оскільки у кожному конкретному кейсі обходу санкцій «третьою» може бути будь-яка країна, яка не застосувала конкретну санкційну норму («Санкції щодо ВПК Росії – непослідовні», 2023).

Натомість дослідники виділяють конкретні країни, які найбільш активно використовуються для обходу західних санкцій. Так, у звіті Київської школи економіки особливу увагу приділяють Китаю, Туреччині та ОАЕ (Bilousova et al., 2024).

«Посередники» – це ще одна ключова характеристика процесу обходу міжнародних санкцій. Саме посередники формують мережу обходу санкцій і дозволяють говорити про ці процеси саме як про мережі. У соціальних науках дослідження мереж виокремлюється у цілий метод та використовується для досліджень різних напрямків. Мережевий аналіз у політичних науках зокрема використовується для дослідження тероризму та політичного насилля (Perliger & Pedahzur, 2011). Стимулом для розвитку цього напрямку став терористичний акт 11 вересня 2001 року, коли терористична організація «Аль-Каїда» здійснила атаку на Всесвітній торговельний центр в Нью-Йорку. Наприклад, Krebs (2002), використовуючи публічні дані газет, визначив мережу терористів, які здійснили атаку 11 вересня.

Окрім цього дослідники приділяють увагу російському громадянству як фактору, на який звертають увагу під час дослідження обходу санкцій (Allison, 2023). Йдеться про бізнеси, власниками яких є росіяни, а, особливо, про компанії, які були створені у третіх країнах після початку повномасштабного вторгнення Росії в Україну. Так, у 2022 році суттєво збільшилась кількість компаній, яка була зареєстрована росіянами у Туреччині, Казахстані, Грузії, ОАЕ, Сербії (Allison, 2023, р.19). Безумовно, наявність російського громадянства не може бути єдиним ризик-фактором для визначення компанії, яка обходить санкції, проте це може бути однією із характеристик таких мереж.

Компанії, які можуть обходити санкції, є *“анонімними та номінальними корпоративними структурами”* (Allison, 2023, р.25). Про це також йдеться у застозозі для фінансових інституцій світу про можливі спроби обходу компаніями експортного контролю, спрямованого на послаблення військових потужностей Росії та Білорусі, опублікованого у 2022 році Агентством боротьби з фінансовими злочинами (FinCEN) та Бюро промисловості та безпеки (BIS) Міністерства фінансів США («FinCEN and the U.S. Department of Commerce’s Bureau...», 2022). Зокрема, у документі зазначено, що ознаками фіктивності компаній можуть бути відсутність інформації про компанію онлайн або відсутність фізичної адреси.

У цій же застозозі перелічені й інші характеристики, якими можуть володіти мережі, що обходять санкції. Для прикладу, такі компанії можуть мати зв'язки з підсанкційними особами, російськими державними компаніями, військовими

кінцевими користувачами та ФСБ. Про такі самі характеристики йдеться й в застозі Управління з питань виконання фінансових санкцій Великобританії («Red Alert. Exporting High Risk Goods», 2023).

Дослідження використання мережевого аналізу у розслідуваннях міжнародних злочинних мереж не нове, хоча цей метод не став популярним для дослідження мереж, які обходять міжнародні санкції. У 2002 році аналіз мереж застосовувався для аналізу мережі терористів, що стояла за терактами у США у вересні 2001 року (Krebs, 2002). Вчені скористалися інформацією з газет та прес-релізів, щоб надати візуалізацію мережі терористів, відображаючи те, як ця мережа була представлена в засобах масової інформації. У дослідженні вони визначили ступінь централізації мережі, щільність мережі та ступінь центральності кожного із терористів. Ці кроки допомогли показати, що мережа терористів була розгалужена і не мала якскраво виражених центрів.

У свою чергу Julei (2014) вивчав мережу терористичних організацій у Східному Туркестані. На основі даних з відкритих джерел про мережі терористів, а також терористичні атаки у 1949-2012 роках, дослідники побудували графіки мереж терористів, визначили ступінь центральності вузлів мереж.

Bright (2013) досліджував динаміку розвитку мереж, які займалися торгівлею наркотиками. Зокрема він на основі даних з поліції протягом 8 років визначив ролі людей, які були залучені до процесів торгівлі зокрема за допомогою підрахунку центральності цих вузлів.

Також мережевий аналіз застосовувався для виявлення транснаціональних кримінальних мереж. У 2016 році дослідження від американського аналітичного центру Centre for Advanced Defence Studies розглядало вплив глобалізації на розвиток транснаціональної злочинності, а також використання відкритих даних та сучасних програм для аналізу даних для пошуку злочинних мереж (Vira et al., 2016).

Оскільки тема санкцій та експортного контролю пов'язана з торгівлею, мережевий аналіз також використовується для дослідження торговельних зв'язків. У дослідженні мереж постачальників автор використовує характеристики центральності для визначення найсильніших мереж, які торгують певними типами продукції (Nuss et al., 2016).

У дослідженнях ефективності санкційної політики, як вже було зазначено вище, описують проблему обходу санкцій, роль третіх країн та посередників, визначаються деякі характеристики мереж, які обходять міжнародні санкції, проте вони не є вичерпними. Зокрема, під час аналізу не використовуються такі поняття як центральність мережі, хоча саме це поняття може бути ключовим для аналізу мереж, як показують приклади досліджень мереж терористів, торговців наркотиками та транснаціональних злочинців. Тож якими характеристиками володіють мережі людей та компаній, що обходять міжнародні антиросійські санкції? Наскільки мережі людей

та компаній, що обходять міжнародні антиросійські санкції, об'єднані довкола однієї людини або компанії?

Відповіді на ці питання допоможуть сформувати структури глобальних мереж, які обходять міжнародні санкції і несуть загрозу для національної безпеки країн санкційної коаліції, зокрема, США. Адже саме Федеральне бюро розслідувань США є одним із найуспішніших органів із розслідування порушень експортного контролю та санкційних режимів США.

Окрім того, під час повномасштабного вторгнення Росії в Україну розслідування порушень міжнародних санкційних режимів стало одним із сфер протидії російської агресії проти цивілізованого світу, а виявлення злочинців – пріоритетом у сфері міжнародних санкцій. Злочинці можуть відкрити сотні підставних компаній, саме тому фокус санкційної політики лежить у визначенні самих злочинців та притягнення їх до відповідальності.

АНАЛІТИЧНА РАМКА ДОСЛІДЖЕННЯ

Основним поняттям цього дослідження є мережа, а сам підхід роботи можна віднести до досліджень, які ідентифікують фактори, що впливають на ефективність санкцій. Allison et al (2023) виокремлюють цей підхід від інших двох типів дослідження санкцій: перші дослідження санкцій у 1970-тих роках на основі обмежених переліків кейсів санкцій та виключно кількісного аналізу ефективності санкцій. Обхід санкцій є одним із факторів, які впливають на ефективність санкційної політики, а мережі – система, яка є основою обходу санкцій.

Адже обхід санкцій полягає у тому, щоб створити мережу компаній та людей, які, фактично, створюють видимість поставок певних товарів до підставних кінцевих користувачів. Таким чином мережа компаній обманює навіть тих виробників чи дистриб'юторів, які не хочуть порушувати санкційні режими.

Мережі, які обходять антиросійські санкції, як і будь-які інші мережі складаються із акторів та відносин між цими акторами. У термінах аналізу соціальних мереж (social network analysis) акторами є вузли (nodes), а зв'язки між вузлами (edges) означають певну комунікацію. У контексті мереж, які беруть участь в обході санкцій, йдеться про комунікацію між компаніями та фізичними особами. При цьому ця комунікація може бути відображена у сумах торговельних операцій, зв'язках у соціальних мережах, спілкування телефоном чи через онлайн-месенджери тощо.

З метою визначити характеристик мереж, які беруть участь в обході антиросійських санкцій, необхідно визначити перш за все самі мережі.

Мережі, які беруть участь в обході антиросійських санкцій, – це групи компаній та осіб, які були задокументовані органами правопорядку або журналістами-розслідувачами в обході антиросійських санкцій у 2022-2024 роках. Міжнародні санкції проти Росії є ключовим фокусом країн санкційної коаліції під час вторгнення Росії в Україну, саме тому ці санкції є найбільш актуальним прикладом міжнародних санкційних режимів та способів їх обходу.

У свою чергу міжнародний санкційний режим проти Росії – санкції країн санкційної коаліції у 2022-2024 роках. В межах цього дослідження йдеться перш за все про експортний контроль США стосовно заборони експорту товарів подвійного та військового призначення з США до Росії, а також реекспорту цих товарів з третіх країн до Росії.

Важливим моментом дослідження ланцюгів постачання є визначення найважливішого організатора схеми. Адже попри десятки анонімних та номінальних компаній завжди є основна людина або компанія, яка стоїть за організацією всіх процесів. У мережевому аналізі за визначення такої людини (вузла) відповідають параметри ступінь центральності (degree centrality) та ступінь централізації (degree centralization).

Центральність (centrality) мереж *“фіксує потенційний доступ особи до ресурсів”* (according to Wasserman and Faust (1994), as cited in Ten Kate et al., 2010, с.23). Іншими словами, центральність мереж – це *«координаційний центр спілкування»* мережі (Freeman, 1979, с. 220). Дослідники використовують параметр центральності для визначення основних вузлів мереж. Для прикладу, Krebs (2002) використовує цей параметр для аналізу мережи терористів, Bright та Delaney (2013) для аналізу мережи наркоторговців, а Nuss (2016) для аналізу торгівельних мереж. В аналізі соціальних мереж існують найбільш поширені характеристики центральності – ступінь центральності вузла (degree centrality), ступінь централізації мережі (degree centralization), центральність посередника (betweenness centrality) та центральність близькості (closeness centrality):

- ступінь центральності (degree centrality) визначається кількістю зв'язків вузла в мережі, показує, наскільки центральним є вузол у мережі за кількістю зв'язків з іншими вузлами;
- ступінь централізації мережі (degree centralization) вказує на те, наскільки рівномірно розподілені зв'язки між усіма вузлами у мережі, оцінює, наскільки один вузол (або декілька вузлів) є центральними порівняно з усіма іншими вузлами;
- центральність посередника (betweenness centrality) визначає, наскільки вузол важливий для сполучення інших вузлів у мережі, вимірює кількість найкоротших шляхів між усіма вузлами, які проходять через вузол;
- центральність близькості (closeness centrality) визначає, наскільки швидко вузол може досягти інших вузлів у мережі, вимірює середню відстань від вузла до всіх інших вузлів у мережі.

Загалом, всі вони визначають те, наскільки багато зв'язків зосереджується в одному вузлі мережі.

Мережі розрізняють на декілька типів: зірка, коло тощо (Goyal, 2007). Чим вища централізація мережі, тим більше мережа схожа на тип «зірку», коли всі вузли з'єднані лише з одним центральним вузлом. На противагу «зірці» існують мережі типу «коло», коли кожен вузол з'єднаний лише з двома іншими вузлами, а центрального вузла взагалі не існує. Чим більше мережа схожа на «зірку», тим вищий ступінь централізації (degree centralization). Мережа-зірка має ступінь централізації «1», тоді як будь-яка звичайна мережа – «0» (Goyal, 2007, p.16).

Попри популярність використання та свої переваги, параметри центральності та централізації мають низку обмежень та ризиків. Одним із недоліків є брак даних про діяльність мереж. Адже у жодному джерелі даних, окрім основних організаторів схем, немає інформації про всі можливі вузли мереж, їхні зв'язки та всі епізоди обходу санкцій. Проблема полягає у тому, що *«виявлення нового змовника разом із новими зв'язками або виявлення зв'язку між існуючими вузлами може змінити розташування*

топових вузлів» (Krebs, 2002, с.47). Тобто використання неповних даних може спотворити реальну схему взаємодій у мережі.

Свою специфіку вносить також популярне джерело даних у цій сфері – матеріали кримінальних справ, судові документи. Адже ці дані вже опрацьовані органами правопорядку, викладені у тій формі, яка необхідна правоохоронцям для доведення вини злочинців. Тоді як незалежний дослідник, який отримує доступ до цих документів, наприклад, із відкритих джерел, не знає, яка інформація була пропущена в цих матеріалах, недостатньо задокументовано. Можливо, органи правопорядку арештували одного злочинця, щоб швидше закрити справу, замість того, щоб належно задокументувати роботу цілої мережі.

Деякі дослідники також вважають, що підрахунок центральності вузлів фокусується лише на основних вузлах, тоді як в мережах важливо моніторити кожен із вузлів: *«ми стверджуємо, що всі актори в мережі є «ключовими», тобто всі вони мають бути однаково промоніторені» (Basu, 2021, с.45).*

Тим не менш, дослідники мереж терористів чи наркоторговців також перебувають у схожій ситуації із проблемним доступом до даних, проте це не заважає досліджувати ці мережі на основі наявної інформації. Саме тому важливо використовувати дані з відкритих джерел для дослідження діяльності мереж, які обходять міжнародні санкції.

На відміну від мереж терористів та наркоторговців, мережі, щоб обходять міжнародні санкції, можуть мати один вузол, який зосереджує на собі більшість координації мережі, володіє повною інформацією про схему. Адже у цих мережах певні вузли свідомо використовують підставні компанії для проведення схем: реєструють або купують такі компанії в офшорних юрисдикціях, відкривають банківські рахунки на підставних осіб, підроблюють документи про вартість, кінцевого користувача та країну призначення продукції. Ці кроки складно впроваджувати, коли окремі вузли мережі не знають про роботу інших вузлів.

У певних випадках компанії за межами Росії можуть бути пов'язані родинними або професійними зв'язками з компаніями в Росії, які замовляють певну продукцію (Голішевська et al., 2023). Це так само означає, що закордонні постачальники розуміють, коли вони йдуть на порушення тих чи інших санкційних обмежень.

Ба більше, роботу таких мереж у випадку Росії можуть навіть координувати російські спецслужби, які зацікавлені у налагодженні поставок в Росію підсанкційної західної продукції для нарощування виробництва військово - промислового комплексу. Засоби масової інформації та органи правопорядку неодноразово повідомляли, що Служба зовнішньої розвідки Росії, Головне розвідувальне управління та Федеральна служба безпеки Росії залучені до організації схем обходу санкцій («Lithuanian firms involved...», 2024). Міністерство юстиції США навіть публікувало фото агента у формі ФСБ, який був залучений до однієї із схем обходу санкцій (Додаток 2). У цьому

випадку вся схема поставок може координуватися з одного центру і зав'язана на одному чи декількох вузлах мережі.

Таким чином, враховуючи специфіку роботи цих мереж, можна зробити теоретичні очікування про те, що мережі, які беруть участь в обході міжнародних санкцій, мають одного основного організатора або невелику групу організаторів, які відповідальні за налагодження більшості зв'язків у мережі, таких як створення підставних компаній, отримання замовлення від кінцевих користувачів підсанкційної продукції, оплату підсанкційної продукції, логістику підсанкційної продукції тощо.

Теоретичне очікування 1: мережі, які беруть участь в обході міжнародних санкцій, мають високий ступінь централізації (degree centralization).

Теоретичне очікування 2: декілька вузлів мережі мають суттєво вищий ступінь центральності (degree centrality) за інші вузли мережі.

МЕТОДОЛОГІЧНИЙ ДИЗАЙН

Основним поняттям цього дослідження є мережа. Саме тому у цій роботі я пропоную застосувати підходи **мережевого аналізу** для пошуку центральних вузлів різних мереж людей та компаній, які обходять міжнародні санкції. Мережевий аналіз дає можливість охарактеризувати структури пов'язаних між собою вузлів та порівняти різні мережі між собою.

Мережевий аналіз компаній та осіб, які обходять санкції, має схожі проблеми із мережевим аналізом, який використовується для аналізу кримінальних груп. Зокрема, йдеться про неповноту даних – адже дослідник ніколи не володіє всією інформацією про мережу; нерозуміння, кого варто включати до мережі, а хто не відіграє важливої ролі; динаміку змін мереж – дослідник завжди володіє історичними даними про мережу, а тим часом вона продовжує змінюватися (Sparrow, 1991).

Я не ставлю за мету цього дослідження створити узагальнені висновки про всі мережі, які обходять санкції. Натомість я ставлю перед собою завдання описати певні процеси всередині конкретних мереж, а роль центральних вузлів у таких мережах, їхні завдання та зв'язки з іншими, менш важливим вузлами. Для виконання цієї задачі я обираю **дослідження кейсів**. Цей метод допоможе заглибитися у механізми взаємодії в межах конкретних мереж.

Дослідження окремих мереж не можна назвати репрезентативним. Проте метод кейс стаді і не ставить за мету репрезентативність. Навпаки, дослідження конкретних випадків дає змогу пропрацювати деталі, механізми та зрозуміти процеси окремих мереж. У ситуації, коли мережевий аналіз не засовується активно для аналізу цих типів мереж, така розвідка може бути першим кроком до дослідження.

Як випадки для аналізу я обрав низку мереж, які обходять антиросійські санкції, та описані в низці кримінальних справ у США про незаконні поставки компонентів для російських військових кінцевих користувачів у 2022-2024 роках. Для формування вибірки я здійснив пошук за ключовими словами «Росія», «санкції», «експортний контроль» на сайті Міністерства юстиції США, на якому публікують прес-релізи про обвинувачення осіб у порушення експортного контролю.

Таким чином у вибірку потрапили справи 2022-2024 року, які вдалось знайти таким способом на цьому ресурсі, а саме:

- Ордер на арешт Ніколая Гольцева, Салімджона Насріддінова та Крістіни Пузирьової (Додаток 2).
- Обвинувальний акт Кирилу Буяновському та Дугласу Робертсону (Додаток 2).
- Позов проти Максима Марченка (Додаток 2).

- Обвинувальний акт Євгену Гриніну, Олексію Іпполітову, Борису Лівшицу, Світлані Скворцовій, Вадиму Конощенку, Олексію Брайману, Вадиму Єрмоленку (Додаток 2).
- Ордер на арешт Іллі Кана (Додаток 2).
- Позов проти Артура Петрова (Додаток 2).

Хоча деякі країни-члени ЄС також розслідують схожі справи, для аналізу в межах цієї роботи я обрав справи у США через низку причин:

- США більш активно розслідують справи обходи санкцій, а порушники несуть кримінальну відповідальність за порушення експортного контролю;
- США публікують матеріали справи, у яких можна встановити зв'язки між особами та компаніями.

Із кожної справи я визначив вузли та зв'язки між вузлами на основі даних, описаних в кримінальній справі. Вузли можуть бути як компанії, так і люди. А за основу зв'язків між вузлами я беру наступні дані:

- поставки товарів від компанії до компанії;
- пересилання коштів від компанії до компанії;
- організацію поставок конкретними особами;
- переписки між людьми про організацію поставок;
- спільні адреси компаній та людей;
- спільні номери телефонів компаній та людей.

Зв'язки між вузлами не є спрямованими та не мають кількісних характеристик сили зв'язків (value), адже це потребує розробки окремої методології та не є завданням дослідження.

Для визначення характеристик мереж я використовую мережевий аналіз, а саме параметри ступінь центральності вузлів (degree centrality) та ступінь централізації мережі (degree centralization).

На основі сформованих таблиць зв'язків у мережах я розрахував ступінь центральності вузлів (degree centrality), ступінь централізації мереж (degree centralization) в програмному середовищі для статистичних обчислень "R". За допомогою підрахунку стандартного відхилення я визначив вузли у кожній мережі, які мають найбільший ступінь центральності в мережах.

Окрім цього я побудував графі кожної із мереж за допомогою програми «Flourish.Studio». На основі даних про ступінь центральності вузлів я визначив силу кожного із вузлів, що дає можливість показати роль окремих вузлів на графі – вузли із найбільшою кількістю зв'язків мають більший розмір за вузли з меншою кількістю зв'язків.

ДОСЛІДЖЕННЯ І РЕЗУЛЬТАТИ

Під час дослідження мені вдалось проаналізувати 6 кейсів мереж, які обходили міжнародні антиросійські санкції і були звинувачені у порушення законодавства США у галузі експортного контролю.

Всі мережі закупували електроніку з США після початку повномасштабного вторгнення Росії в Україну, хоча деякі з особи та компанії постачали електроніку до Росії і раніше. У цих кейсах осіб звинувачують в організації таємних схем поставок електроніки, яка підпадає під експортний контроль у США. Бюро промисловості та безпеки США в інтересах національної безпеки країни забороняє експортувати продукцію, яка може бути використана у військових цілях. Обмеження Бюро прописані в Правилах експортного контролю (EAR) та залежать від технічних характеристик, пункту призначення, кінцевого користувача та призначення продукції. Найбільш важлива продукція визначена у Торговому контрольному списку (Commerce Control List). Експорт такої продукції заборонений до Росії.

Розслідуванням цих злочинів займається Міністерство національної безпеки США, Федеральне бюро розслідувань.

Кейс 1.

Мережа кейсу складається із 18 вузлів, які діяли на території США, Китаю, Росії, Гонконгу та Туреччини. Ступінь централізації мережі становить 0.52, а вузли «Ніколай Гольцев»(18) та SH Brothers Group(15) відрізняються від середнього значення ступеня центральності вузлів мережі (3.7) більш ніж на два стандартних відхилення. Це свідчить про високу роль цих вузлів в організації мережі та взаємодії з іншими вузлами.

Вузол	Ступінь центральності вузла
Ніколай Гольцев	18
SH Brothers Group	15
Салімджон Насріддінов	11
Testkomplekt	6
Співзмовник 2	5
Кристина Пузирьова	4
Співзмовник 1	4
Співзмовник 3	4
Співзмовник 4	4
Robotronix Semiconductors LTD	4
Suntronic F.Z.E.	3
Гонконгська компанія 1	3
Турецька компанія 1	3
SN Electronics	3
Ресторан Насріддінова	3
Komtech	3

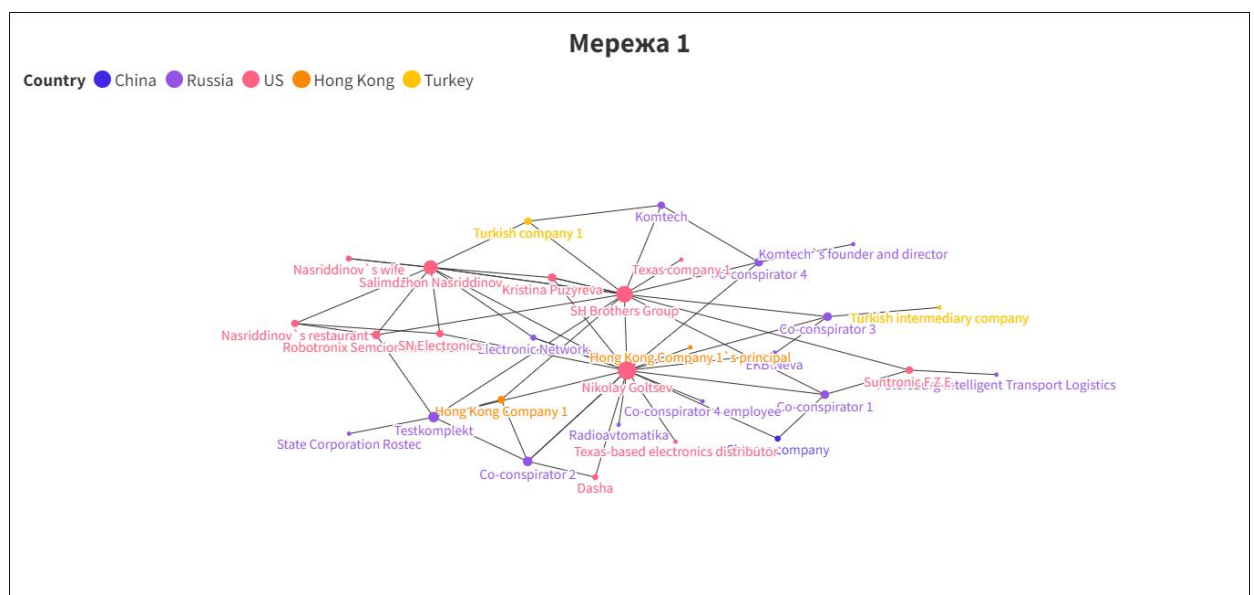
Дружина Насриддінова	2
Китайська компанія	2
Даша	2
Electronic Network	2
ЕКВ-Neva	2
Співзмовник 4 співробітник	1
Техаський дистриб'ютор електроніки	1
Турецька компанія-посередник	1
Директор Гонконгської компанії 1	1
Засновник і директор Komtech	1
Техаська компанія 1	1
State Corporation Rostec	1
Radioavtomatika	1
Petersburg Intelligent Transport Logistics	1

Примітка: власні розрахунки та основі даних кримінальної справи (Додаток 2)

Саме Ніколай Гольцев є основним обвинуваченим у цій справі, а компанія SH Brothers Group виступала основною компанією, через яку злочинці закуповували електроніку, переказували кошти тощо. Ніколай Гольцев закуповував в американських дистриб'юторів електроніку та експортував її до Росії через компанії в Туреччині, Китаї та Гонконгу. Деякі типи електронних компонентів, які також експортував Ніколай Гольцев, були знайдені у захоплених російських вертольотах, танках, БПЛА на території України.

Ніколай Гольцев мав тривалі зв'язки з російськими компаніями, які закуповували електроніку. Зокрема, він співпрацював з Радіоавтоматикою, Тесткомплектом та іншими підприємствами протягом 12 років. Що підтверджує важливість Ніколая Гольцева у мережі закупівель в інтересах російських компаній в обхід американських санкцій.

Схема 1. Мережа 1.



Примітка: дані кримінальної справи (Додаток 2)

Кейс 2.

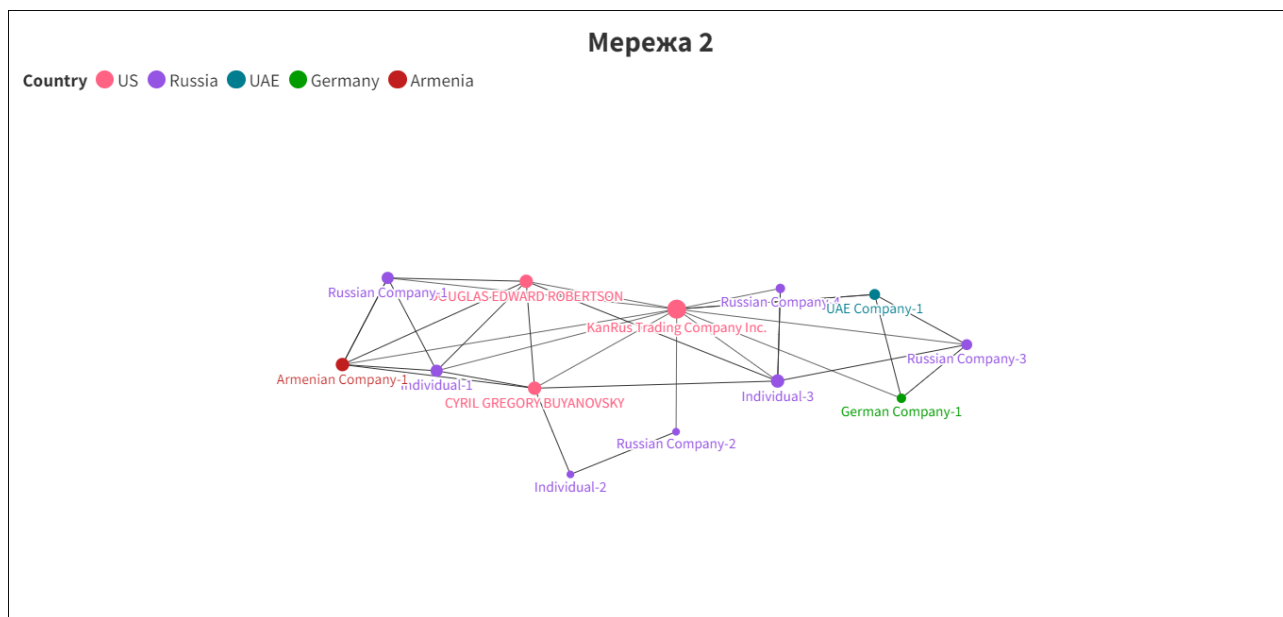
Мережа кейсу складається із 13 вузлів, які діяли на території США, Росії, ОАЕ, Німеччини та Вірменії. Ступінь централізації мережі становить 0.58, а вузол KanRus Trading Company Inc. (12) відрізняються від середнього значення ступеня центральності мережі (4.9) більш ніж на два стандартних відхилення. Це свідчить про високу роль цього вузла в організації мережі та взаємодії з іншими вузлами.

Таблиця 2. Ступінь центральності вузлів мережі 2.	
Вузол	Ступінь центральності вузла
KanRus Trading Company Inc.	12
Кирило Григорій Буяновський	6
Дуглас Едуард Робертсон	6
Особа-3	6
Вірменська Компанія-1	6
Російська Компанія-1	5
Особа-1	5
Російська Компанія-3	4
Компанія ОАЕ-1	4
Російська Компанія-4	3
Німецька Компанія-1	3
Російська Компанія-2	2
Особа-2	2

Примітка: власні розрахунки та основі даних кримінальної справи (Додаток 2)

Компанія KanRus Trading Company Inc. була основною компанією, через яку здійснювали закупівлі електроніки, змінювали кінцевих користувачів, ціну та місце призначення експортної продукції. Саме ця компанія є основною у створенні схеми у цій справі. Компанія була створена Буяновським та Робертсоном, які і є основними фігурантами справи по експорту складного авіонічного обладнання з США користувачами російських повітряних суден.

Малюнок 2. Мережа 2.



Примітка: дані кримінальної справи (Додаток 2)

Кейс 3.

Мережа кейсу складається із 12 вузлів, які діяли на території США, Росії, Гонконгу. Ступінь централізації мережі становить 0.50, а середнє значення центральності вузлів – 3.8, а вузол «Максим Марченко» (11) відрізняється від середнього значення ступеня центральності мережі (3.1) більш ніж на два стандартних відхилення. Це свідчить про високу роль Максима Марченка в організації мережі та взаємодії з іншими вузлами.

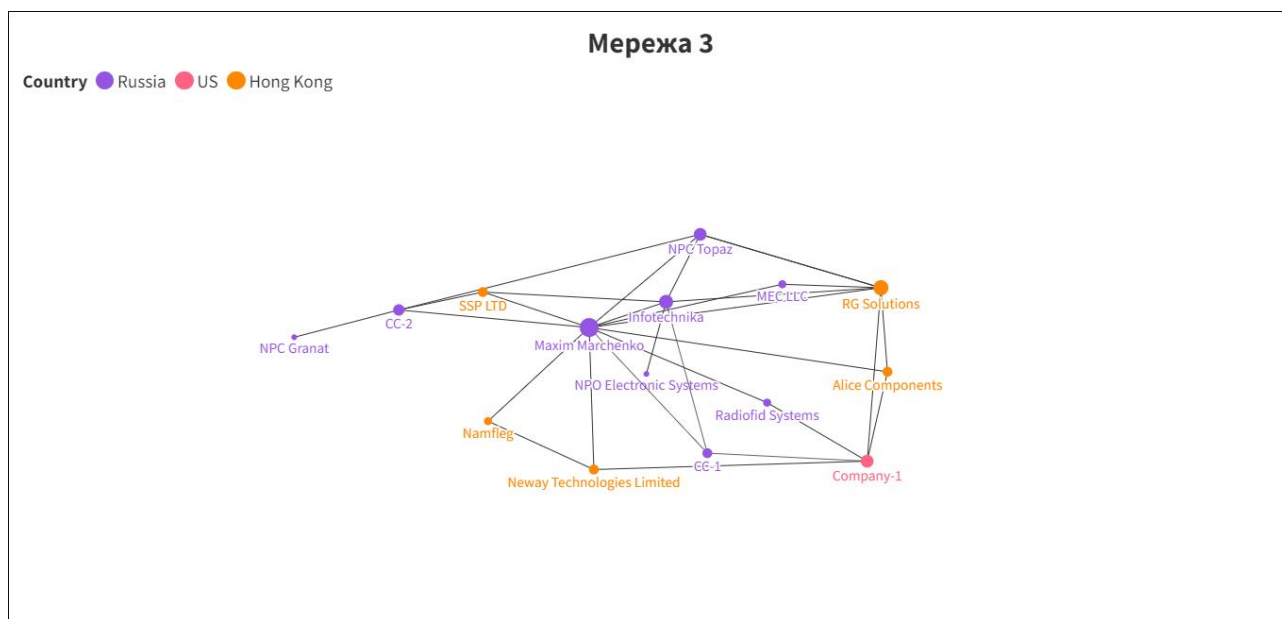
Таблиця 3. Ступінь центральності вузлів мережі 3.

Вузол	Ступінь центральності вузла
Максим Марченко	11
Alice Components	3
CC-1	3
RG Solutions	7
SSP LTD	3
Namfleg	2
CC-2	4
NPO Electronic Systems	1
NPC Topaz	5
Компанія-1	5
Radiofid Systems	2
MEC LLC	2
Neway Technologies Limited	3
Infotechnika	6
NPC Granat	1

Примітка: власні розрахунки та основи даних кримінальної справи (Додаток 2)

Саме Максим Марченко є основним обвинуваченими у цій справі. Він займався відмиванням коштів та контрабандою мікро-дисплеїв з США до Росії, які можуть мати військове призначення у приборах нічного бачення, оптичних прицілах. Роль Максима Марченка полягала у створенні підставних компаній в Гонконгу, які були транспортними хабами для подальшого експорту товару до Росії, адже сам Марченко проживає у Гонконгу. При цьому Марченко активно спілкувався із російськими замовниками для прийманні замовлень та оплати коштів за продукцію.

Малюнок 3. Мережа 3.



Примітка: дані кримінальної справи (Додаток 2)

Кейс 4.

Мережа кейсу складається із 25 вузлів, які діяли на території США, Росії, Великої Британії. Ступінь централізації мережі становить 0.5, а вузол «Борис Лівшиць» (16) відрізняються від середнього значення ступеня центральності мережі (3.1) більш ніж на два стандартних відхилення. Це свідчить про високу роль Бориса Лівшиця в організації мережі та взаємодії з іншими вузлами.

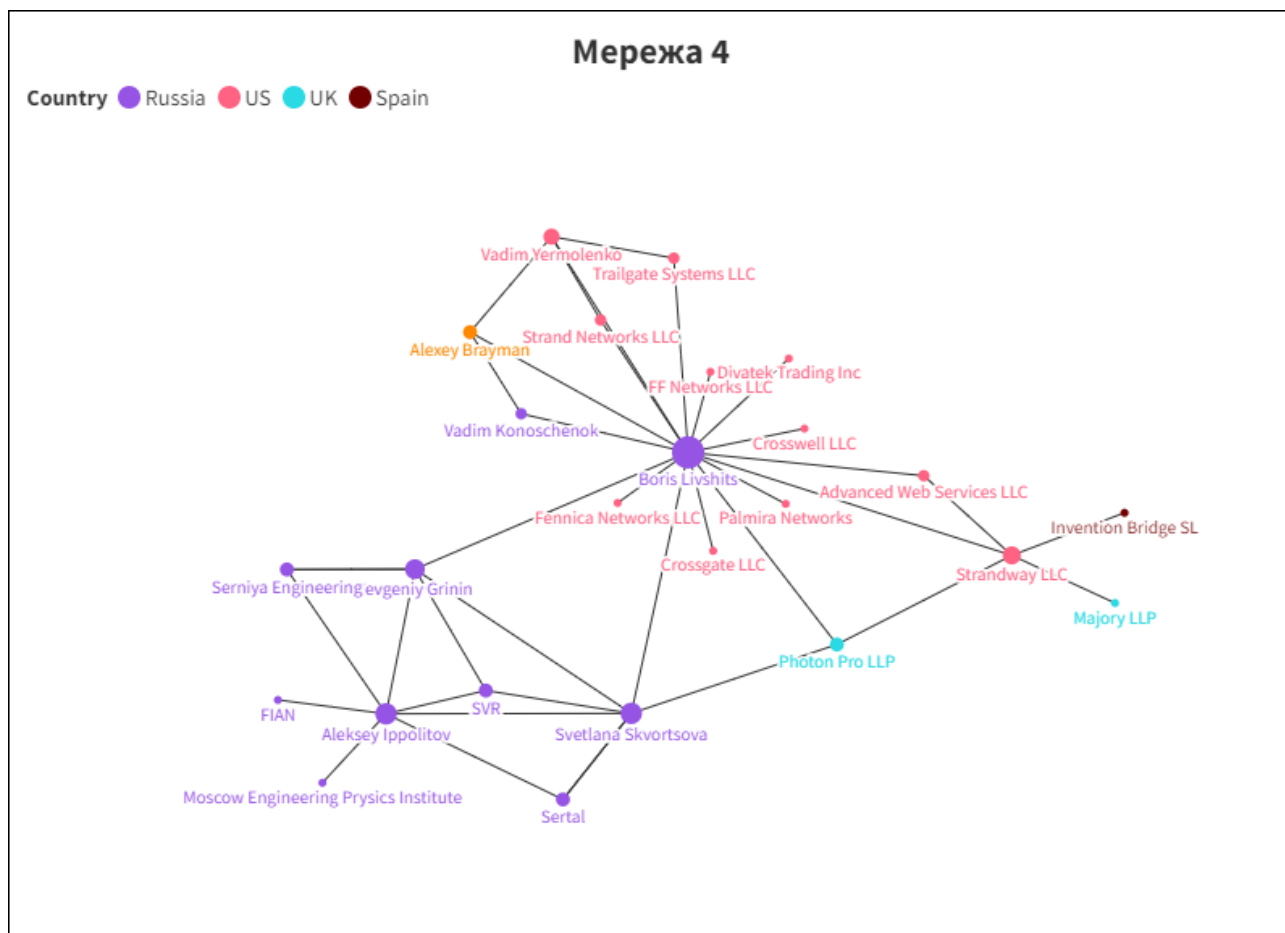
Таблиця 4. Ступінь центральності вузлів мережі 4.	
Вузол	Ступінь центральності вузла
Борис Лівшиць	16
Олексій Іпполітов	7
Світлана Скворцова	7
Євген Гринін	6
Strandway LLC	5
Вадим Єрмоленко	4
Олексій Брайман	3

Serniya Engineering	3
Sertal	3
Photon Pro LLP	3
SVR	3
Advanced Web Services LLC	2
Вадим Конощенко	2
Strand Networks LLC	2
Trailgate Systems LLC	2
Crossgate LLC	1
Crosswell LLC	1
Divatek Trading Inc	1
Fennica Networks LLC	1
FF Networks LLC	1
Palmira Networks	1
FIAN	1
Majory LLP	1
Invention Bridge SL	1
Moscow Engineering Physics Institute	1

Примітка: власні розрахунки та основи даних кримінальної справи (Додаток 2)

Борис Лівшиць є одним із основних обвинувачених у цій справі. Лівшиць заповував товари в американських компаніях, створив та контролював кілька фіктивних компаній і зв'язаних з ними банківських рахунків у Нью-Йорку. Ці структури використовувалися для організації поставок та складних фінансових операцій схеми.

Малюнок 4. Мережа 4.



Примітка: дані кримінальної справи (Додаток 2)

Кейс 5.

Мережа кейсу складається із 13 вузлів, які діяли на території США, Росії, Гонконгу, Тайвані. Ступінь централізації мережі становить 0.39, а вузол Ілля Кан (8) відрізняються від середнього значення ступеня центральності мережі (3.1) більш ніж на два стандартних відхилення. Це свідчить про високу роль Іллі Кана в організації мережі та взаємодії з іншими вузлами.

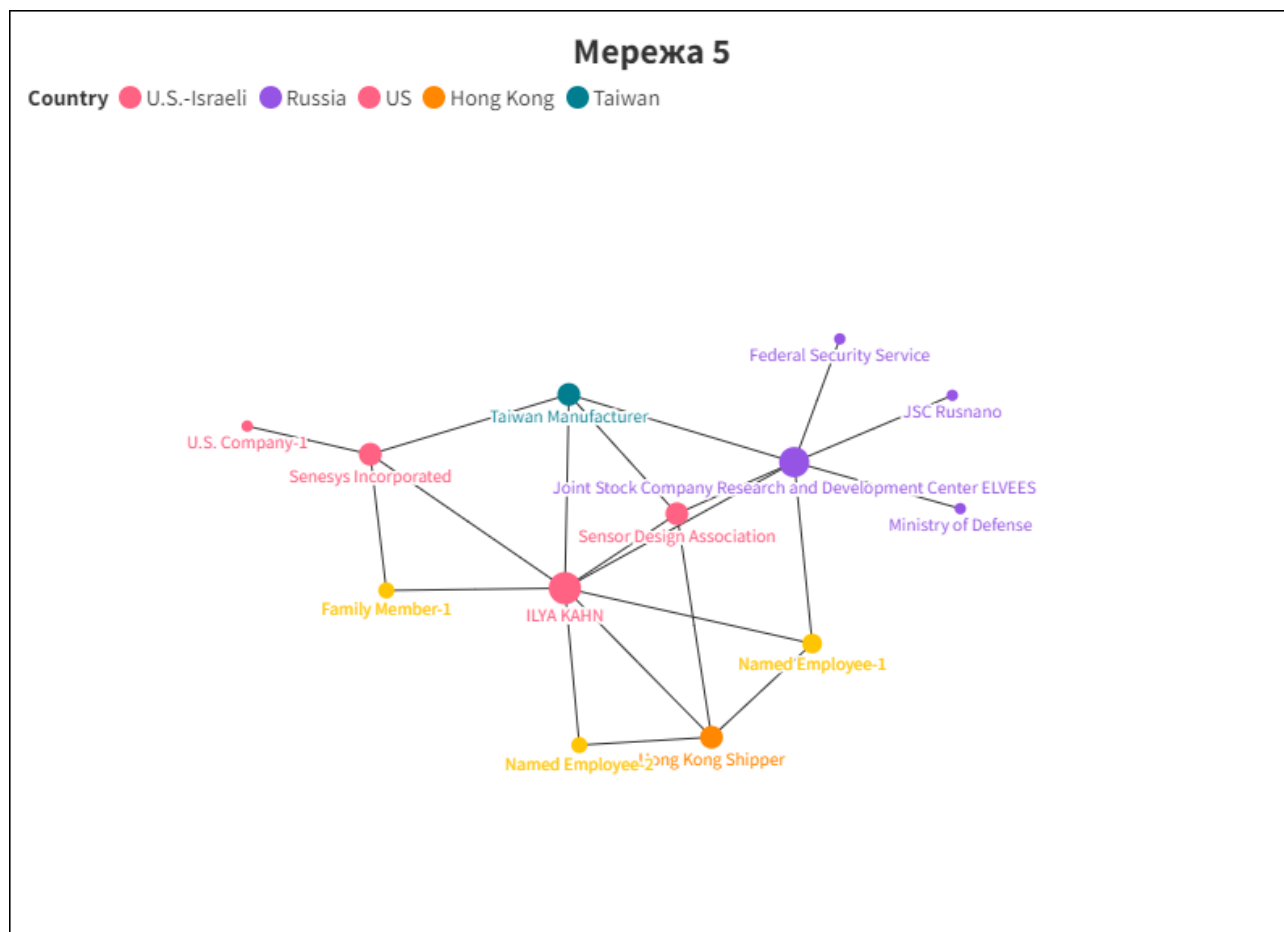
Таблиця 5. Ступінь центральності вузлів мережі 5.	
Вузол	Ступінь центральності вузла
Ілля Кан	8
Joint Stock Company Research and Development Center Elvees	7
Taiwan Manufacturer	4
Sensor Design Association	4
Senesys Incorporated	4
Hong Kong Shipper	4
Названий працівник-1	3
Названий працівник-2	2
Член сім'ї-1	2

Компанія США-1	1
Ministry of Defense	1
Federal Security Service	1
JSC Rusnano	1

Примітка: власні розрахунки та основи даних кримінальної справи (Додаток 2)

Саме Ілля Кан є основним обвинуваченим у цій справі. Він володіє американськими компаніями Senesys Incorporated та Sensor Design Association, управляє цими фірмами, які розробляють програмне забезпечення для безпеки та випробування кремнієвих пластин, що використовуються у військовій авіації та космічних технологіях. При цьому Кан як мінімум з 2012 року займався постачанням підсанкційних технологій з США до російського кінцевого користувача компанії «Elvees», яка є виробником напівпровідників, а серед клієнтів компанії – Федеральна служба безпеки Росії. При цьому сам Кан має подвійне громадянство США та Ізраїлю, що спрощувало спілкування Кана з американськими постачальниками.

Малюнок 5. Мережа 5.



Примітка: дані кримінальної справи (Додаток 2)

Кейс 6.

Мережа кейсу складається із 13 вузлів, які діяли на території США, Росії, Кіпру. Ступінь централізації мережі становить 0.4, а середнє значення центральності вузлів –

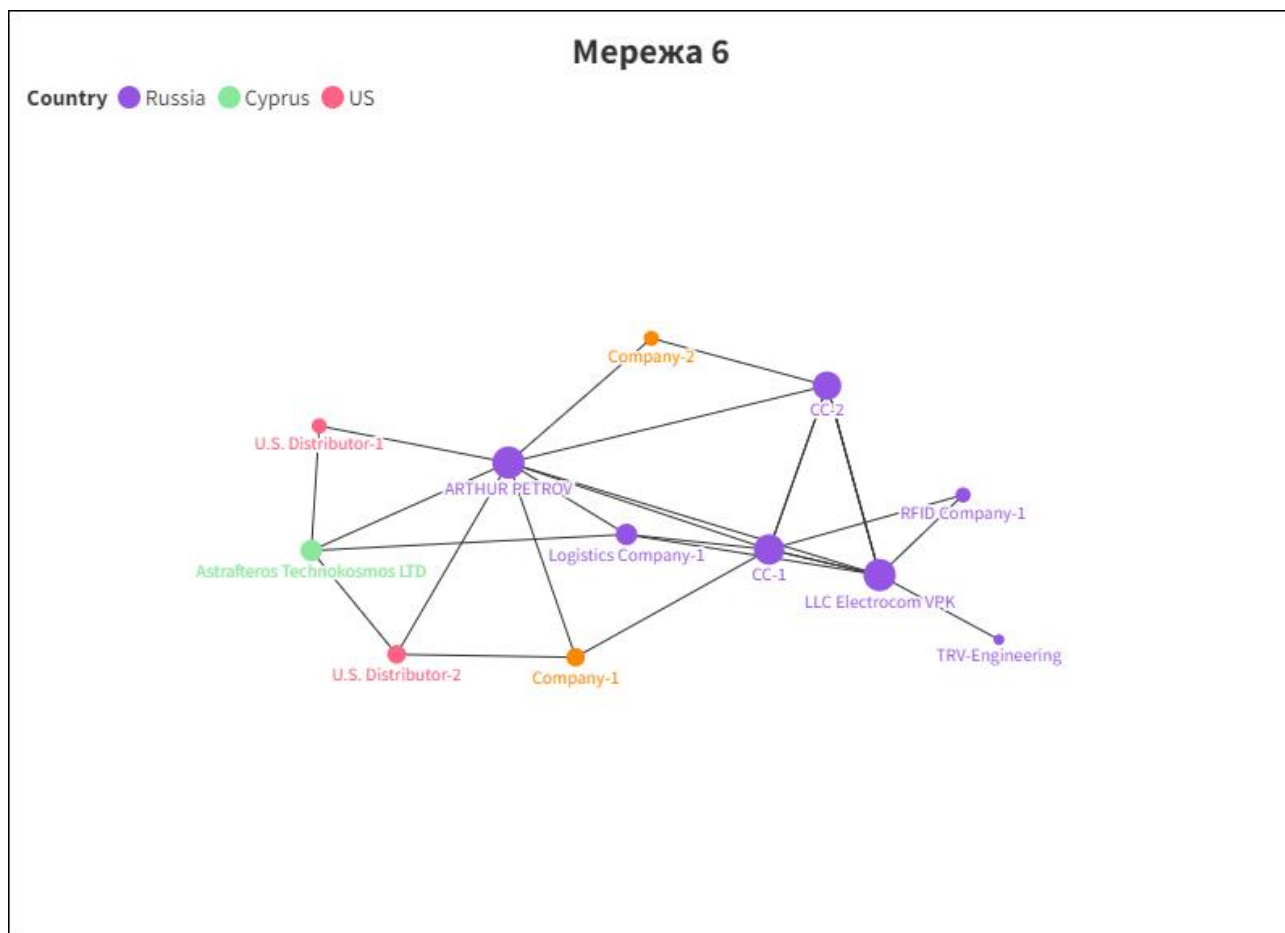
4.5. При цьому жоден вузол не відрізняється від середнього значення ступеня центральності мережі більш ніж на два стандартних відхилення, проте вузол Артур Петров та компанія «LLC Electrocom VPK» мають більше зв'язків за всі інші вузли. Саме ці вузли є основними організаторами схеми, через яку відбувались поставки електроніки.

Таблиця 6. Ступінь центральності вузлів мережі 6.	
Вузол	Ступінь центральності вузла
АРТУР ПЕТРОВ	9
LLC Electrocom VPK	9
СС-1	8
СС-2	7
Логістична компанія-1	4
Astrafteros Technokosmos LTD	4
Дистриб'ютор США-2	3
Компанія-1	3
Дистриб'ютор США-1	2
RFID Company-1	2
Компанія-2	2
TRV-Engineering	1

Примітка: власні розрахунки та основи даних кримінальної справи (Додаток 2)

Артур Петров є основним обвинуваченим у цій справі. Петров налагодив експорт підсанкційної мікроелектроніки до російського кінцевого користувача компанії «Electrocom», постачальника російської армії. Для цього Петров використовував кіпрські компанію «Astrafteros», яку учасники схеми зазначали кінцевим користувачем американської продукції, хоча насправді продукція далі потрапляла до Росії.

Малюнок 6. Мережа 6.



Примітка: дані кримінальної справи (Додаток 2)

ДИСКУСІЯ ТА ІНТЕРПРЕТАЦІЇ

Таким чином **теоретичне очікування 1** підтверджуються на прикладі 6 кейсів мереж, що обходили американські санкції, та експортували підсанкційну продукцію до Росії. На прикладах 6 кейсів у цій роботі можна побачити, яким чином функціонують ці мережі та яким чином центральні вузли мережі поєднані як, наприклад, з американськими постачальниками, так і з російськими замовниками. Ступінь централізації мереж коливається від 0.39 до 0.58, що свідчить про наближеність цих мереж до типу мереж «зірка», яка має ступінь централізації 1 (Таблиця 7).

Таблиця 7. Ступінь централізації мереж 1-6.						
	Кейс 1	Кейс 2	Кейс 3	Кейс 4	Кейс 5	Кейс 6
Ступінь централізації мереж	0.52	0.58	0.50	0.53	0.39	0.40

В усіх мережах ми побачили яскраво виражених організаторів мережі, які мали тривалі зв'язки з російськими замовниками, працювали з американськими постачальниками та підставними компаніями у третіх країнах. Таким чином **теоретичне очікування 2** також підтверджуються на прикладі 5 кейсі із 6. Так, 5 із 6 мережа мають чітко виражені центри мереж у вигляді осіб або компаній з високим значенням ступеня центральності у порівнянні з іншими вузлами мережі (Таблиця 8).

Таблиця 8. Ступінь центральності вузлів мереж 1-6.						
	Кейс 1	Кейс 2	Кейс 3	Кейс 4	Кейс 5	Кейс 6
Ступінь центральності вузлів, середнє значення мережі	3.7	4.9	3.1	3.1	3.1	4.5
Ступінь центральності вузла, який відрізняється від середнього значення ступеня центральності мережі більш ніж на два стандартних відхилення.	Ніколай Гольцев (18) SH Brothers Group (15)	KanRus Trading Company Inc. (12)	Максим Марченко (11)	Борис Лівшиць (16)	Ілля Кан (8)	відсутні

Ці мережі мають яскраво виражених організаторів, які є центром своїх мереж. Ніколай Гольцев у мережі 1 закуповував електроніку в США та експортував її до Росії через турецькі компанії, при цьому співпрацюючи із російськими замовниками протягом 12 років. Компанія KanRus Trading Company Inc. у мережі 2

використовувалась як основна ланка між США та Росією. Максим Марченко у мережі 3 займався відмиванням коштів та створенням підставних компаній в Гонконгу, а також спілкувався із російськими замовниками. Борис Лівшиць у мережі 4 контролював кілька фіктивних та банківських рахунків у Нью-Йорку, які використовували для багатьох поставок до Росії. Ілля Кан закупував постачання підсанкційних товарів до Росії з 2012 року, володіючи низкою американських компаній.

Більшість учасників мереж спілкувались саме з цими людьми або працювали з їхніми компаніями, і саме ці люди є основними обвинуваченими за вчинені злочини з порушення експортного контролю США. Наявність таких яскраво виражених центрів мереж спрощують процес координації всередині мережі, підвищують рівень довіри всіх учасників мережі до основного організатора. У двох випадках також відомо, що основні організатори співпрацювали із кінцевими російськими користувачами десятиліттями, що свідчить про важливість тривалого зв'язку організатора схеми із замовниками.

Окрім того наявність центрального організатора може бути наслідком відносно невеликої кількості вузлів у мережах. У кейсах 1-6 найменша мережа складається із 12 вузлів, а найбільша – із 25 вузлів. Тоді як мережі терористів або наркоторговців можуть складатися із сотень людей. Адже для обходу санкцій не потрібно будувати картелі або захоплювати території – достатньо відкрити декілька підставних компаній у третій країні і рахунок в американському банку. Така специфіка цього типу злочинів дозволяє координувати діяльність всієї мережі з одного центру.

З іншої сторони, можна ставитися до всіх мереж, які обходять санкції в інтересах конкретної країни, як до одної великої мережі. Адже кожна із мереж 1-6 виконувала завдання в інтересах, перш за все, військово-промислового комплексу Росії. З відкритих джерел невідомо, щоб ці шість мереж координувалися всі з одного штабу російських спецслужб, проте такий потенційний сценарій не варто відкидати. Така концептуалізація дає можливість подивитися на всі ці кейси як на окремі частини великої мережі, яка матиме зовсім інші характеристики, ніж кожна маленька мережа сама по собі. Проте станом на зараз немає фактів, які б свідчили про повну координацію цих мереж, тому все таки варто розглядати роботи цих мереж як незалежне обслуговування окремих російських компаній чи заводів.

Наявність таких яскраво виражених центрів може бути унікальною рисою мереж злочинців у цій сфері, проте для підтвердження цієї тези потрібно провести порівняльні дослідження мереж, що обходять санкції, із мережами наркоторговців, терористів тощо.

Таке дослідження 6 кейсів не дає можливості генералізувати висновки на всі мережі, які обходять міжнародні санкції. Тим не менш, у публічному доступі відсутні інші документи 2022-2024 років із судових справ у США, які б описували схеми обходу

санкцій із кримінальних справ. Тобто можна стверджувати, що брак даних про ці мережі є недоліком не тільки цієї конкретної роботи, але і цієї сфери загалом, адже йдеться про таємні мережі.

Серед інших обмежень такого підходу можна виокремити брак та ненадійність даних про роботу таких таємних мереж (Krebs, 2002). А також необхідність фокусуватися не тільки на ключових акторах мережах, але і на всіх інших вузлах (Basu, 2021). Щоб обійти ці обмеження, необхідно розширити методологію дослідження, що може стати основою для майбутніх досліджень мереж, які обходять міжнародні санкції. Для прикладу, можна рахувати різні типи параметру центральності, параметр щільності чи транзитивності, а також проаналізувати динаміку змін мереж протягом років.

Окрім цього варто розширити вибірку кримінальних справ та мереж, які обходять міжнародні санкції, за рахунок використання матеріалів кримінальних справ не тільки в США, але і в країнах ЄС або Великобританії. А також можна використати інформацію про мережі, які обходять не тільки антиросійські санкції, але і міжнародні санкції проти інших країн – Ірану, Китаю, Білорусі тощо. Така розширена вибірка дасть можливість визначити узагальнені характеристики мереж, що обходять міжнародні санкції, та зробити висновок про ефективність міжнародних санкцій *per se*.

Подальші дослідження мереж, які обходять міжнародні санкції, можуть допомогти загалом зрозуміти характер мереж транснаціональних злочинців і терористів. Адже люди, які порушують санкції, як ми побачили у кейсах 1-6, є справжніми транснаціональними злочинцями, які можуть отримати покарання у вигляді позбавлення волі на десятиліття. При цьому міжнародні санкції застосовують не тільки до бізнесу олігархів, компаній військово - промислового комплексу, але й до терористів. Тому дослідження мереж, що обходять міжнародні санкції, можуть запропонувати корисні висновки і для дослідників терористичних мереж.

Дослідження мереж, які обходять міжнародні санкції, потребують занурення у роботу цих мереж. Аналіз центральності вузлів у мережах є одним із найважливіших завдань, адже, на відміну від терористичних груп, які діють відокремлено, мережі обходу санкцій часто мають одного конкретного організатора або групу центральних людей, що працюють над створення всієї схеми, відкриття підставних компаній, банківських рахунках у різних країнах світу. У певних випадках ці групи можуть координуватися навіть спецслужбами тих чи інших країн.

РЕКОМЕНДАЦІЇ

Санкційна політика стала одним із інструментів протидії російській агресії проти України та проблемним питанням не тільки для України, яка безпосередньо веде війну, але і для країн санкційної коаліції, які використовують міжнародні санкції як інструмент тиску на Росію. Експортний контроль є одним із основних заборон, які реально впливають на здатність Росії купувати товари, необхідні для ведення війни – якби Росія могла купувати електроніку для ракет та дронів безпосередньо в західних виробників, це значно спрощувало б її логістичні витрати та строки поставок продукції. Саме тому схеми обходу цих заборон є критичною проблемою, з якою країни санкційної коаліції мають боротися. Одним із варіантів боротьби є ідентифікація та переслідування мереж людей та компаній, які організують ці схеми.

Основними стейкхолдерами, які дотичні до формування та реалізації санкційної політики є органи, які формують санкційну політику (Управління з контролю за іноземними активами (США), Міністерство торгівлі США, Бюро промисловості та безпеки (США), Європейська Комісія (ЄС), Генеральний директорат з питань фінансової стабільності, фінансових послуг та союзу ринків капіталу (ЄС) тощо) та органи, які розслідують порушення санкційної політики (Міністерство національної безпеки США, Федеральне бюро розслідувань (США), органи правопорядку країн-членів ЄС тощо).

На основі цієї роботи можна запропонувати наступні рекомендації для органів влади країн санкційної коаліції, які працюють над розслідуваннями порушень експортного контролю, санкційних режимів, а також органам влади, які формулюють санкційну політику цих країн.

1. Під час розслідування обходів міжнародних санкцій шукати основних організаторів схем замість того, щоб фокусуватись лише на підставних компаніях.
2. Після ідентифікації організатора схеми ідентифікувати всі банківські рахунки, компанії, засновані організатором, бізнес-партнерів – організатор схеми може мати доступ до всіх етапів схеми.
3. Під час розслідування обходів міжнародних санкцій шукати осіб, які раніше співпрацювали з потенційними кінцевими користувачами підсанкційної продукції – саме вони можуть бути організаторами схем закордоном в інтересах кінцевих користувачів.
4. Під час розслідування обходів міжнародних санкцій перевіряти зв'язок мережі, що обходить санкції, із російськими спецслужбами з метою пошуку фактів, які б дали можливість стверджувати, що всі такі мережі координуються з одного центру і можуть сприйматися як одна велика мережа.
5. Повідомляти приватні бізнеси про роботу мереж, які обходять міжнародні санкційні режими, створюючи підставні компанії та підроблюючи документи про кінцеве призначення продукції.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Allison, O., Hack, A. A., O'Shea, L. and Saiz, G. (2023). Illuminating the Role of ThirdCountry Jurisdictions in Sanctions Evasion and Avoidance (SEA). SOC ACE Research Paper No 21. Birmingham, UK: University of Birmingham.
2. Basu, K., & Sen, A. (2021). Identifying individuals associated with organized criminal networks: A social network analysis. *Social Networks*, 64, 42–54.
3. Bilousova, O., Hilgenstock, B., Ribakova, E., Shapoval N., Vlasyuk, A., Vlasiuk, V. (2024). Challenges of export controls enforcement. How Russia continues to import components for its military production. Kyiv School of Economics. 52 pp.
4. Borgatti, S. P., & Cross, R. (2003). A Relational view of information seeking and learning in social networks. *Management Science*, 44 (4), 432–445.
5. Borgatti, S. P., & Cross, R. (2003). A relational view of information seeking and learning in social networks. *Management Science*, 44(4), 432–445.
6. Bright, D. A., & Delaney, J. J. (2013). Evolution of a drug trafficking network: Mapping changes in network structure and function across time. *Global Crime*, 14(2-3), 238-260.
7. Bureau of Industry and Security. <https://www.bis.gov/ear>.
8. Byrne, Jack, Watling, J., Bronk, J., Somerville, G., Byrne, Joe, Crawford, J., & Baker, J. (2023). The Orlan complex: Tracking the supply chains of Russia's most successful UAV. Royal United Services Institute.
9. Early, B. R. (2009). Sleeping with your friends' enemies: An explanation of sanctions-busting trade. *International Studies Quarterly*, 53(1), 49–71
10. Ergün, E., & Usluel, Y. K. (2016). An Analysis of Density and Degree-Centrality According to the Social Networking Structure Formed in an Online Learning Environment. *Journal of Educational Technology & Society*, 19(4), 34–46. <http://www.jstor.org/stable/jeductechsoci.19.4.34>
11. EU goods worth at least \$1bn vanish in Russia 'ghost trade'. *Financial Times*. 2023.10.05. <https://www.ft.com/content/76fc91b2-3494-4022-83d0-9d6647b38e3d>
12. Felbermayr, G., Morgan, T. C., Syropoulos, C., & Yotov, Y. V. (2021a). Understanding economic sanctions: Interdisciplinary perspectives on theory and evidence. *European Economic Review*, 135: 103720. Interdisciplinary perspectives on theory and evidence. *European Economic Review*, 135: 103720.
13. FinCEN and the U.S. Department of Commerce's Bureau of Industry and Security Urge Increased Vigilance for Potential Russian and Belarusian Export Control Evasion Attempts. Financial crimes enforcement network. 2022.06.28. <https://www.fincen.gov/news/news-releases/fincen-and-us-department-commerces-bureau-industry-and-security-urge-increased>
14. Freeman, L. C. 1979. Centrality in social networks: I. Conceptual clarification. *Soc. Networks* 1 215–239.

15. Gary Clyde Hufbauer & Jeffrey J. Schott & Kimberly Ann Elliott, 2009. "Economic Sanctions Reconsidered, 3rd Edition (paper)," Peterson Institute Press: All Books, Peterson Institute for International Economics, number 4129, July.
16. Goyal, S. (2007). Connections: An Introduction to the Economics of Networks (STU-Student edition). Princeton University Press. <http://www.jstor.org/stable/j.ctt7s2j2>
17. Hellquist, Elin. "Either With us or Against us? Third-Country Alignment with EU Sanctions against Russia/Ukraine". Cambridge Review of International Affairs, vol. 29, issue 3 (2016), pp. 997-1.021.
18. Julei, F., Ying, F., Yang, W., Wang, S., (2014). Network analysis of terrorist activities. J. Syst. Sci. Complex 27, 1079–1094.
19. Krebs, V. E. (2002). Mapping networks of terrorist cells. Connections, 24(3), 43–52.
20. List of common high priority items (2024). Directorate-General for Financial Stability, Financial Services and Capital Markets Union. https://finance.ec.europa.eu/publications/list-common-high-priority-items_en
21. Lithuanian firms involved in schemes to circumvent Russia sanctions – intelligence. LRT. 2024.03.07. <https://www.lrt.lt/en/news-in-english/19/2216611/lithuanian-firms-involved-in-schemes-to-circumvent-russia-sanctions-intelligence>
22. Nuss, P., Graedel, T. E., Alonso, E., & Carroll, A. (2016). Mapping supply chain risk by network analysis of product platforms. Sustainable Materials and Technologies, 10, 14–22.
23. Perliger, A., & Pedahzur, A. (2011). Social Network Analysis in the Study of Terrorism and Political Violence. PS: Political Science and Politics, 44(1), 45–50. <http://www.jstor.org/stable/40984482>
24. Red Alert. Exporting High Risk Goods. Office of Financial Sanctions Implementation HM Treasury. 2023. <https://www.nationalcrimeagency.gov.uk/who-we-are/publications/687-necc-red-alert-exporting-high-risk-goods/file>
25. Ruys, T. (2017). Sanctions, Retorsions and Countermeasures: Concepts and International Legal Framework. In L. van den Herik (Ed.), Research Handbook on U.N. Sanctions and International Law (pp. 19-31). Edward Elgar Publishing.
26. Sparrow, M. K. (1991). The application of network analysis to criminal intelligence: An assessment of the prospects. Social Networks, 13, 251–274.
27. Ten Kate, S., Haverkamp, S., Mahmood, F., & Feldberg, F. (2010). Social Network Influences on Technology Acceptance: A Matter of Tie Strength, Centrality and Density. In BLED 2010 Proceedings (p. 40). Retrieved from <https://aisel.aisnet.org/bled2010/40>
28. Tostensen, A., & Bull, B. (2002). Are Smart Sanctions Feasible? World Politics, 54(3), 373–403. <http://www.jstor.org/stable/25054192>
29. Vira, V., Hansen, J., C4ADS. Using open data to combat transnational criminal networks. WCO news. 2016.02.14. <https://mag.wcoomd.org/magazine/wco-news-79/using-open-data-to-combat-transnational-criminal->

networks/?fbclid=IwAR1QI4H3lbuHyszMZiDG0R3NJ2ae0XxK9FmnAZ02jwTYH6p-shGnptEa99A

30. База даних санкцій, застосованих після нападу Росії на Україну. Війна та санкції. <https://sanctions.nazk.gov.ua/>.

31. Голішевська, А., Попович, І. Як родина виробника КАМАЗ постачає деталі з Австрії в росію. Trap Aggressor. 2023.12.22. <https://trap.org.ua/publications/yak-rodyna-vyrobnyka-kamaz-postachaie-detali-z-avstrii-v-rosiiu/>

32. Санкції щодо ВПК Росії – непослідовні. НАКО. 2023.11.15. <https://nako.org.ua/research/inconsistency-in-action-a-case-of-sanctioning-russian-military-industry>

ДОДАТКИ

Додаток 1. Вузли та зв'язки мереж 1-6.

Вузли мережі 1.	
Nikolay Goltsev	Russian and Canadian
Salimdzhon Nasriddinov	Russian and Tajikistan
Nasriddinov`s wife	
Kristina Puzyreva	Russian and Canadian
Co-conspirator 1	Russian
Co-conspirator 2	Russian
Co-conspirator 3	Russian
Co-conspirator 4	Russian
Robotronix Semiconductors LTD	
Electronic Network	Canada
SH Brothers Group	US
SN Electronics	US
Suntronic F.Z.E.	UAE
Testkomplekt	Russia
EKB-Neva	Russia
Radioavtomatika	Russia
Komtech	Russia
State Corporation Rostec	Russia

Зв'язки мережі 1.	
Texas-based electronics distributor	Nikolay Goltsev
SH Brothers Group	Co-conspirator 3
Turkish intermediary company	Co-conspirator 3
Nikolay Goltsev	SH Brothers Group
Salimdzhon Nasriddinov	SH Brothers Group
Kristina Puzyreva	SH Brothers Group
Nikolay Goltsev	Electronic Network
SH Brothers Group	Co-conspirator 1
SH Brothers Group	Suntronic F.Z.E.

Suntronic F.Z.E.	Petersburg Intelligent Transport Logistics
SH Brothers Group	Testkomplekt
SH Brothers Group	Hong Kong Company 1
Hong Kong Company 1	Testkomplekt
Nikolay Goltsev	Co-conspirator 2
Co-conspirator 2	Hong Kong Company 1
Hong Kong Company 1`s principal	Nikolay Goltsev
SH Brothers Group	Co-conspirator 4
SH Brothers Group	Komtech
Turkish company 1	Komtech
SH Brothers Group	Turkish company 1
Komtech`s founder and director	Co-conspirator 4
Texas company 1	SH Brothers Group
Turkish company 1	Salimdzhon Nasriddinov
Nikolay Goltsev	Co-conspirator 1
Chinese company	Nikolay Goltsev
Chinese company	Co-conspirator 1
SN Electronics	Nikolay Goltsev
SN Electronics	Salimdzhon Nasriddinov
Nasriddinov`s restaurant	SN Electronics
Nasriddinov`s restaurant	Salimdzhon Nasriddinov
Robotronix Semiconductors LTD	Nasriddinov`s restaurant
Robotronix Semiconductors LTD	Salimdzhon Nasriddinov
Robotronix Semiconductors LTD	Testkomplekt
Dasha	Co-conspirator 2
Dasha	Nikolay Goltsev
Kristina Puzyreva	Salimdzhon Nasriddinov
Kristina Puzyreva	SH Brothers Group

Вузли мережі 2.	
CYRIL GREGORY BUYANOVSKY	US

DOUGLAS EDWARD ROBERTSON	US
KanRus Trading Company Inc.	US
Russian Company-1	Russia
Individual-1	Russia
Russian Company-2	Russia
Individual-2	Russia
Russian Company-3	Russia
Individual-3	Russia
Russian Company-4	Russia
Individual-4	Russia
UAE Company-1	UAE
German Company-1	Germany
Armenian Company-1	Armenia

Зв'язки мережі 2.	
Source	Target
CYRIL GREGORY BUYANOVSKY	KanRus Trading Company Inc.
DOUGLAS EDWARD ROBERTSON	CYRIL GREGORY BUYANOVSKY
DOUGLAS EDWARD ROBERTSON	KanRus Trading Company Inc.
Russian Company-1	Individual-1
Russian Company-2	Individual-2
Russian Company-3	Individual-3
Individual-3	KanRus Trading Company Inc.
Individual-3	CYRIL GREGORY BUYANOVSKY
Individual-3	DOUGLAS EDWARD ROBERTSON
Russian Company-4	Individual-3
Russian Company-3	KanRus Trading Company Inc.
Russian Company-4	KanRus Trading Company Inc.
UAE Company-1	KanRus Trading Company Inc.

UAE Company-1	Russian Company-3
German Company-1	Russian Company-3
German Company-1	KanRus Trading Company Inc.
Armenian Company-1	Russian Company-1
Individual-2	CYRIL GREGORY BUYANOVSKY
Russian Company-2	KanRus Trading Company Inc.
German Company-1	UAE Company-1
UAE Company-1	KanRus Trading Company Inc.
Individual-1	CYRIL GREGORY BUYANOVSKY
Russian Company-1	KanRus Trading Company Inc.
Russian Company-1	DOUGLAS EDWARD ROBERTSON
Individual-3	Russian Company-4
Individual-1	KanRus Trading Company Inc.
Individual-1	DOUGLAS EDWARD ROBERTSON
Armenian Company-1	CYRIL GREGORY BUYANOVSKY
Armenian Company-1	DOUGLAS EDWARD ROBERTSON
Armenian Company-1	Russian Company-1
Armenian Company-1	Individual-1
Armenian Company-1	KanRus Trading Company Inc.

Вузли мережі 3.	
Maxim Marchenko	Russia
CC-1	Russia
CC-2	Russia
Company-1	US
Alice Components	Hong Kong

RG Solutions	Hong Kong
Infotechnika	Russia
NPO Electronic Systems	Russia
NPC Topaz	Russia
SSP LTD	Hong Kong
NPC Granat	Russia
Namfleg	Hong Kong
Neway Technologies Limited	Hong Kong
Radiofid Systems	Russia
MEC LLC	Russia

Зв'язки мережі 3.	
Source	Target
Maxim Marchenko	CC-1
Maxim Marchenko	CC-2
Alice Components	Company-1
CC-1	Company-1
RG Solutions	Company-1
RG Solutions	Alice Components
Maxim Marchenko	RG Solutions
RG Solutions	NPC Topaz
Maxim Marchenko	Infotechnika
RG Solutions	Infotechnika
SSP LTD	Infotechnika
RG Solutions	NPC Topaz
Namfleg	Maxim Marchenko
CC-2	NPC Granat
CC-2	SSP LTD
CC-2	NPC Topaz
Maxim Marchenko	Neway Technologies Limited
CC-1	Infotechnika
NPO Electronic Systems	Infotechnika
NPC Topaz	Infotechnika

Company-1	Neway Technologies Limited
Radiofid Systems	Company-1
Radiofid Systems	Maxim Marchenko
Alice Components	Maxim Marchenko
SSP LTD	Maxim Marchenko
MEC LLC	Maxim Marchenko
MEC LLC	RG Solutions
Maxim Marchenko	NPC Topaz
Neway Technologies Limited	Namfleg

Вузли мережі 4.	
Yevgeniy Grinin	Russia
Aleksey Ippolitov	Russia
Boris Livshits	Russia
Svetlana Skvortsova	Russia
Vadim Konoschenok	Russia
Alexey Brayman	
Vadim Yermolenko	US
Serniya Engineering	Russia
Moscow Engineering Physics Institute	Russia
Sertal	Russia
VNIIA	Russia
Majory LLP	UK
Photon Pro LLP	UK
Invention Bridge SL	Spain
Strandway LLC	US
FIAN	Russia
Advanced Web Services LLC	US
Crossgate LLC	US
Crosswell LLC	US
Divatek Trading Inc	US
Fennica Networks LLC	US
FF Networks LLC	US
Palmira Networks	US
Strand Networks LLC	US
Trailgate Systems LLC	US

Зв'язки мережі 4.	
Source	Target
Boris Livshits	Alexey Brayman
Aleksey Ippolitov	Yevgeniy Grinin
Aleksey Ippolitov	Svetlana Skvortsova
Svetlana Skvortsova	Yevgeniy Grinin
Aleksey Ippolitov	Serniya Engineering
Aleksey Ippolitov	Sertal
Yevgeniy Grinin	Serniya Engineering
Yevgeniy Grinin	Serniya Engineering
Svetlana Skvortsova	Sertal
Svetlana Skvortsova	Sertal
Yevgeniy Grinin	Boris Livshits
Svetlana Skvortsova	Boris Livshits
Strandway LLC	Boris Livshits
Aleksey Ippolitov	FIAN
Vadim Yermolenko	Boris Livshits
Alexey Brayman	Vadim Konoschenok
Advanced Web Services LLC	Boris Livshits
Crossgate LLC	Boris Livshits
Crosswell LLC	Boris Livshits
Divatek Trading Inc	Boris Livshits
Fennica Networks LLC	Boris Livshits
FF Networks LLC	Boris Livshits
Palmira Networks	Boris Livshits
Vadim Yermolenko	Strand Networks LLC
Vadim Yermolenko	Trailgate Systems LLC
Boris Livshits	Strand Networks LLC
Boris Livshits	Trailgate Systems LLC
Vadim Yermolenko	Alexey Brayman
Strandway LLC	Advanced Web Services LLC
Strandway LLC	Majory LLP
Strandway LLC	Photon Pro LLP
Strandway LLC	Invention Bridge SL
Boris Livshits	Vadim Konoschenok

Aleksey Ippolitov	Moscow Engineering Physics Institute
Yevgeniy Grinin	SVR
Aleksey Ippolitov	SVR
Svetlana Skvortsova	SVR
Boris Livshits	Photon Pro LLP
Svetlana Skvortsova	Photon Pro LLP

Вузли мережі 5.	
ILYA KAHN	U.S.- Israeli
Joint Stock Company Research and Development Center ELVEES	Russia
Ministry of Defense	Russia
Federal Security Service	Russia
Senesys Incorporated	US
Sensor Design Association	US
Family Member-1	
JSC Rusnano	Russia
Hong Kong Shipper	Hong Kong
U.S. Company-1	US
Named Employee-1	
Named Employee-2	
Taiwan Manufacturer	Taiwan

Зв'язки мережі 5.	
Source	Target
ILYA KAHN	Joint Stock Company Research and Development Center ELVEES
Joint Stock Company Research and Development Center ELVEES	Ministry of Defense
Joint Stock Company Research and Development Center ELVEES	Federal Security Service
ILYA KAHN	Senesys Incorporated
ILYA KAHN	Sensor Design Association
ILYA KAHN	Family Member-1
Joint Stock Company Research and Development Center ELVEES	JSC Rusnano
ILYA KAHN	Hong Kong Shipper

U.S. Company-1	Senesys Incorporated
Joint Stock Company Research and Development Center ELVEES	Sensor Design Association
Named Employee-1	Joint Stock Company Research and Development Center ELVEES
Named Employee-1	Hong Kong Shipper
Named Employee-1	ILYA KAHN
Named Employee-2	Hong Kong Shipper
Named Employee-2	ILYA KAHN
Taiwan Manufacturer	ILYA KAHN
Taiwan Manufacturer	Joint Stock Company Research and Development Center ELVEES
Taiwan Manufacturer	Senesys Incorporated
Taiwan Manufacturer	Sensor Design Association
Sensor Design Association	Hong Kong Shipper
Family Member-1	Senesys Incorporated

Вузли мережі 6.	
ARTHUR PETROV	Russia
CC-1	Russia
CC-2	Russia
LLC Electrocom VPK	Russia
Astraferos Technokosmos LTD	Cyprus
Company-1	
Company-2	
TRV-Engineering	Russia
U.S. Distributor-1	US
Logistics Company-1	Russia
RFID Company-1	Russia
U.S. Distributor-2	US
Aviasystems	Russia

Зв'язки мережі 6.	
Source	Target
ARTHUR PETROV	LLC Electrocom VPK
CC-1	LLC Electrocom VPK
CC-2	LLC Electrocom VPK
ARTHUR PETROV	Astraferos Technokosmos LTD

ARTHUR PETROV	CC-1
ARTHUR PETROV	CC-2
CC-1	CC-2
ARTHUR PETROV	Company-1
CC-1	Company-1
ARTHUR PETROV	Company-2
CC-2	Company-2
CC-1	LLC Electrocom VPK
CC-2	LLC Electrocom VPK
CC-2	LLC Electrocom VPK
TRV-Engineering	LLC Electrocom VPK
U.S. Distributor-1	ARTHUR PETROV
U.S. Distributor-1	Astrafteros Technokosmos LTD
Logistics Company-1	CC-1
ARTHUR PETROV	Logistics Company-1
Logistics Company-1	Astrafteros Technokosmos LTD
Logistics Company-1	LLC Electrocom VPK
RFID Company-1	LLC Electrocom VPK
RFID Company-1	CC-1
U.S. Distributor-2	ARTHUR PETROV
U.S. Distributor-2	Astrafteros Technokosmos LTD
U.S. Distributor-2	Company-1
CC-2	CC-1

Додаток 2. Матеріали кримінальних справ кейсів 1-6.

DMP:JAM/EHS
F. #2019R01707

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK
----- X

UNITED STATES OF AMERICA

- against -

NIKOLAY GOLTSEV,
SALIMDZHON NASRIDDINOV and
KRISTINA PUZYREVA

Defendants.

----- X

AFFIDAVIT AND
COMPLAINT IN SUPPORT
OF AN APPLICATION FOR
ARREST WARRANTS

(T. 18, U.S.C., §§ 554, 1349 and 2; T. 50,
U.S.C., §§ 4819(a)(1), 4819(a)(2)(A)-(G)
and 4819(b))

No. 23-M-956

EASTERN DISTRICT OF NEW YORK, SS:

Yevgeny Gershman, being duly sworn, deposes and states that he is a Special Agent with the United States Department of Homeland Security, Homeland Security Investigations, duly appointed according to law and acting as such:

Wire Fraud Conspiracy

In or about and between January 2022 and October 2023, both dates being approximate and inclusive, within the Eastern District of New York and elsewhere, the defendants NIKOLAY GOLTSEV, SALIMDZHON NASRIDDINOV and KRISTINA PUZYREVA, together with others, did knowingly and intentionally conspire to devise a scheme and artifice to defraud one or more U.S. companies by means of materially false and fraudulent pretenses, representations and promises, and for the purpose of executing such scheme and artifice, to transmit and cause to be transmitted by means of wire communication in interstate and foreign commerce, writings, signs, signals, pictures and sounds, to wit:

electronic communications, emails and other online communications and monetary transfers in and through the Eastern District of New York and elsewhere, contrary to Title 18, United States Code, Section 1343.

(Title 18, United States Code, Section 1349)

Smuggling Goods from the United States

In or about and between January 2022 and October 2023, both dates being approximate and inclusive, within the Eastern District of New York and elsewhere, the defendants NIKOLAY GOLTSEV, SALIMDZHON NASRIDDINOV and KRISTINA PUZYREVA, together with others, did knowingly and fraudulently export and send from the United States, merchandise, articles and objects, to wit: items on the Commerce Control List set forth in Title 15, Code of Federal Regulations, part 774, Supplement Number 1, and items on the Common High Priority List set forth in Title 15, Code of Federal Regulations, part 746, supplement number 4, contrary to United States laws and regulations, to wit: Title 50, United States Code, Sections 4819(a)(1), 4819(a)(2)(A)-(G) and 4819(b) and Title 15, Code of Federal Regulations, Sections 736.2, 746.5(a)(1)(ii) and 746.8(a)(1), and did fraudulently and knowingly receive, conceal and facilitate the transportation and concealment of such merchandise, articles and objects, prior to exportation, knowing the same to be intended for exportation contrary to such United States laws and regulations.

(Title 18, United States Code, Sections 554(a) and 2)

Conspiracy to Violate the Export Control Reform Act (“ECRA”)

In or about and between January 2022 and October 2023, both dates being approximate and inclusive, within the Eastern District of New York and elsewhere, the defendants NIKOLAY GOLTSEV, SALIMDZHON NASRIDDINOV and KRISTINA

PUZYREVA, together with others, did knowingly and willfully conspire to violate and to cause one or more violations of licenses, orders, regulations and prohibitions issued under the Export Control Reform Act, Title 50, United States Code, Sections 4810 et seq.

It was a part and an object of the conspiracy that the defendants NIKOLAY GOLTSEV, SALIMDZHON NASRIDINOV and KRISTINA PUZYREVA, together with others, would and did agree to export and cause to be exported from the United States to Russia items on the Commerce Control List, as set forth in Title 15, Code of Federal Regulations, Part 774, Supplement Number 1, and items on the Common High Priority List, as set forth in Title 15, Code of Federal Regulations, Part 746, Supplement Number 4, without having first obtained a license for such export from the U.S. Department of Commerce.

(Title 50, United States Code, Sections 4819(a)(1), 4819(a)(2)(A)-(G) and 4819(b))

The source of your deponent's information and the grounds for his belief are as follows:¹

1. I am a Special Agent with the United States Department of Homeland Security, Homeland Security Investigations and have been since 2016. I am responsible for conducting and assisting in investigations into the activities of individuals and criminal groups responsible for unlawful proliferation of sensitive and military technologies, export

¹ Because the purpose of this complaint is to set forth only those facts necessary to establish probable cause to arrest, I have not described all the relevant facts and circumstances of which I am aware. Communications referenced herein that have been translated into English are in draft form.

control violations and espionage by foreign governments and related criminal and counterintelligence activity. Through my training, education and experience, I am familiar with the techniques and methods of operation used by individuals involved in intelligence and criminal activities to conceal their behavior from detection by law enforcement authorities. I have participated in numerous investigations, during the course of which I have conducted physical and electronic surveillance, interviewed witnesses, examined financial records, executed court-authorized search warrants and used other techniques to secure relevant information.

2. I am familiar with the facts and circumstances set forth below from my participation in the investigation, my review of documents obtained pursuant to the investigation and reports of other law enforcement officers involved in the investigation. When I rely on statements made by others, such statements are set forth only in part and in substance unless otherwise indicated.

I. The Export Control Reform Act and Export Administration Regulations

3. On August 13, 2018, the President signed into law the National Defense Authorization Act of 2019, which included the Export Control Reform Act (“ECRA”). See 50 U.S.C. § 4801 et seq. ECRA provided permanent statutory authority for the Export Administration Regulations (“EAR”), Title 15, Code of Federal Regulations, Parts 730-774.

4. ECRA provided that “the national security and foreign policy of the United States require that the export, reexport, and in-country transfer of items, and specified activities of United States persons, wherever located, be controlled.” 50 U.S.C. § 4811. To that end, ECRA granted the President the authority to “(1) control the export, reexport,

and in-country transfer of items subject to the jurisdiction of the United States, whether by United States persons or foreign persons; and (2) the activities of United States persons, wherever located, relating to” specific categories of items and information. 50 U.S.C. § 4812. ECRA granted to the Secretary of Commerce the authority to establish the applicable regulatory framework. 50 U.S.C. § 4813.

5. Through the EAR, the U.S. Department of Commerce’s Bureau of Industry and Security (“BIS”) reviewed and controlled the export from the United States to foreign destinations of certain items. In particular, BIS placed restrictions on the export and reexport of items that it determined could make a significant contribution to the military potential or nuclear proliferation of other nations or that could be detrimental to the foreign policy or national security of the United States. Under the EAR, such restrictions depended on several factors, including the technical characteristics of the item, the destination country, the end user and the end use of the item.

6. The most sensitive items subject to EAR controls were identified on the Commerce Control List (“CCL”) set forth in Title 15, Code of Federal Regulations, Part 774, Supplement Number 1. Items listed on the CCL were categorized by Export Control Classification Number (“ECCN”), each of which was subject to export control requirements depending on destination, end use and end user of the item.

7. Since February 24, 2022, when Russia launched its invasion of Ukraine, BIS has implemented a series of stringent export controls that restrict Russia’s access to the technologies and other items that it needs to sustain its attack on Ukraine. As of April 8, 2022, license requirements for exports, reexports and transfers to or within Russia

were expanded to cover all items on the CCL. See 87 Fed. Reg. 12226 (Mar. 3, 2022); 87 Fed. Reg. 22130 (Apr. 14, 2022); 15 C.F.R. § 746.8.

8. On March 3, 2022, BIS imposed additional license requirements for exports, reexports and transfers to or within Russia of any items subject to the EAR that were identified under certain Schedule B or Harmonized Tariff Schedule 6 (“HTS”) numbers. See 87 Fed. Reg. 12856 (March 8, 2022); 15 C.F.R. Part 746, Supp. No. 4. HTS codes took their first six digits from the corresponding Harmonized System (“HS”) code, which was a standardized numerical method of classifying traded products that was used by customs authorities around the world.

9. On September 14, 2023, working in conjunction with the United Kingdom and European Union, BIS published a “Common High Priority Items List,” which identified items by their corresponding HS codes that Russia sought to procure for its weapons programs. See <https://www.bis.doc.gov/index.php/all-articles/13-policy-guidance/country-guidance/2172-russia-export-controls-list-of-common-high-priority-items>. According to BIS, these priority items posed a heightened risk of being diverted illegally to Russia because of their importance to Russia’s war efforts.

10. Through the EAR, BIS also published the Entity List, which identified certain foreign persons—including businesses, research institutions, government and private organizations, individuals and other types of legal persons—that were subject to specific export license requirements and policies, in addition to those found elsewhere in the EAR, due to a determination that such persons had engaged in activities contrary to U.S. national security and/or foreign policy interests. See 15 C.F.R. § 744.11; 15 C.F.R. Part 744, Supp. No. 4 (the Entity List).

11. An exporter generally was required to file Electronic Export Information (“EEI”) through the Automated Export System (“AES”) where, among other reasons, an export license was required or the value of the commodity being exported was more than \$2,500. 15 C.F.R. § 758.1. The EEI required an exporter to list, among other things, the destination country, the ultimate consignee’s name and address, the intermediate consignee’s name and address, and a description of the commodity to be exported. Failure to file EEI or providing false or misleading information in EEI was a violation of ECRA (see, e.g., 50 U.S.C. 4819(a)(2)(F)), the EAR (see 15 C.F.R. Part 758), 13 U.S.C. § 305 and the Foreign Trade Regulations (see 15 C.F.R. Par 30).

12. Under ECRA, it was a crime to willfully violate, attempt to violate, conspire to violate or cause a violation of any regulation, order, license or authorization issued pursuant to the statute, including the EAR. See 50 U.S.C. § 4819(a)(1).

II. The Defendants and Relevant Entities

13. OOO² Radioavtomatika (“Radioavtomatika”) is a Russian defense procurement firm based in Moscow, Russia that specializes in procuring foreign items, including U.S.-origin items, for Russia’s defense industry. On or about March 3, 2022, following Russia’s invasion of Ukraine, BIS added Radioavtomatika to its Entity List, which identifies foreign parties that are subject to additional export restrictions and license requirements. See 87 Fed. Reg. 13141 (Mar. 9, 2022). Also on or about March 3, 2022,

² “OOO” is the abbreviation for the Russian business entity type, “общество с ограниченной ответственностью,” which means limited private company and is roughly the equivalent of a limited liability company or LLC in the United States.

pursuant to Executive Order 14024, the U.S. Department of the Treasury's Office of Foreign Assets Control ("OFAC") added Radioavtomatika to its Specially Designated Nationals and Blocked Persons ("SDN") List; U.S. persons are generally prohibited from dealing with individuals and entities on the SDN List.

14. OOO Testkomplekt ("Testkomplekt") is a Moscow-based electronic components distributor specializing in semiconductors and microelectronics that was established in or about 2016. Testkomplekt has held a variety of contracts with Russian military entities, including State Corporation Rostec, a Moscow-based defense conglomerate. On or about May 19, 2023, pursuant to Executive Order 14024, OFAC added Testkomplekt to its SDN List.

15. OOO NEVA-EKB ("EKB-Neva") is a Moscow-based supplier of electronic components, including radio components, microcircuits, connectors, resonators, diodes, capacitors and resistors. On or about May 19, 2023, pursuant to Executive Order 14024, OFAC added EKB-Neva to its SDN List.

16. The defendant NIKOLAY GOLTSEV is a dual Russian and Canadian national who resides in Canada. GOLTSEV served as an account manager and purchasing coordinator for Electronic Network, Inc. ("Electronic Network"), a company based in Montreal, Canada. On or about February 24, 2023, BIS added Electronic Network to its Entity List. See 88 Fed. Reg. 12170 (Feb. 27, 2022).

17. The defendant SALIMDZHON NASRIDDINOV is a dual national of Russia and Tajikistan who resides in Brooklyn, New York. NASRIDDINOV is a published author regarding integrated systems and other electronic technologies. On or about June 11, 2021, NASRIDDINOV founded SH Brothers Group Inc. ("SH Brothers"), a company with

listed addresses in Brooklyn, New York. On or about January 30, 2023, NASRIDDINOV founded SN Electronics, Inc. (“SN Electronics”), a company with listed addresses in Brooklyn, New York. SN Electronics was registered in NASRIDDINOV’s wife’s name.

18. The defendant KRISTINA PUZYREVA is a dual Russian and Canadian national who resides in Canada. PUZYREVA is married to GOLTSEV.

19. Co-conspirator 1 is a Russian national who resides in Russia. Co-conspirator 1 conducted procurement operations for multiple Russian entities through Suntronic F.Z.E. (“Suntronic”), a front company in the United Arab Emirates (“UAE”).

20. Co-conspirator 2 is a Russian national who resides in Russia and conducted procurement operations for Testkomplekt.

21. Co-conspirator 3 is a Russian national who resides in Russia and conducted procurement operations for EKB-Neva.

22. Co-conspirator 4 is a Russian national who resides in Russia and served as the procurement manager for Radioavtomatika. In or about August 2022, Co-conspirator 4 left Radioavtomatika and began working for another Moscow-based electronics distributor, OOO Komtech (“Komtech”).

III. Overview of the Criminal Scheme

23. As described below, records obtained from court-authorized search warrants and other evidence, including business records such as invoices, shipping documents, wire transfers and financial documents, as well as customs records from the U.S. and foreign countries, have revealed that GOLTSEV, NASRIDDINOV, PUZYREVA and others have been involved in smuggling U.S.-origin dual-use electronics to Russia. Using the SH Brothers and SN Electronics corporate entities, the defendants sourced, purchased

and exported to Russia millions of dollars of dual-use electronics from U.S. manufacturers and distributors located in the Eastern District of New York and elsewhere. Many of these items required a license from BIS to be exported to Russia. Even for items that did not require such a license, the defendants made and caused to be made false and misleading statements in EEI to conceal the fact that Russia was the ultimate end destination and that certain entities and individuals in Russia were the ultimate end users. As such, the defendants and their co-conspirators caused U.S. companies to sell and export electronic components in violation of ECRA and other U.S. laws and regulations; process and accept payments in furtherance of such illicit transactions; and file false documents and fail to file documents with BIS and other U.S. government agencies, including required statements regarding the ultimate consignee and purchaser. The defendants and their co-conspirators also caused U.S. financial institutions to process millions of dollars in payments in violation of U.S. laws and regulations. Many of these transactions were processed through bank accounts held by SH Brothers and SN Electronics and correspondent accounts at New York City banks in New York City and within the Eastern District of New York.

24. Specifically, Russian companies that sought to acquire particular parts or items from the United States were relayed to GOLTSEV. GOLTSEV communicated directly with U.S. manufacturers and distributors, typically using aliases such as “Nick Stevens” and “Gio Ross.” In those communications, GOLTSEV misrepresented and omitted material information, including information about how the items would be used, the various parties involved in the transactions, and the identities of the ultimate Russian end users.

25. GOLTSEV and NASRIDDINOV then purchased the items, including electronic components and integrated circuits, from U.S. companies. NASRIDDINOV received the items at various addresses he controlled in Brooklyn, New York, where he supervised their repackaging and export. GOLTSEV and NASRIDDINOV exported these items from the United States and transshipped them to Russia and Russian end users, including Radioavtomatika, Komtech, Testkomplekt and EKB-Neva, through a variety of intermediary companies in Turkey, Hong Kong, China, India, the UAE and elsewhere. Some of these intermediary companies received U.S. exports solely from SH Brothers, including Robotronix Semiconductors LTD (“Robotronix”), which was listed as an intermediate consignee on approximately 32 shipments valued at more than \$600,000, ostensibly for end users in China. BIS added Robotronix to its Entity List on October 6, 2023. See 88 Fed. Reg. 70352 (Oct. 11, 2023).

26. Some of the electronic components and integrated circuits sourced, purchased and exported by the defendants were designated as “Tier 1” items on the Common High Priority Items List, which, according to BIS, were of the highest concern due to their critical role in the production of advanced Russian precision-guided weapons systems, Russia’s lack of domestic production, and limited global manufacturers. Indeed, some of the same makes, models and part numbers of electronic components exported by the defendants through SH Brothers were found in seized Russian weapons platforms and signals intelligence equipment in Ukraine, including the Torn-MDM radio reconnaissance complex, the RB-301B “Borisoglebsk-2” electronic warfare complex, the Vitebsk L370 airborne counter missile system, Ka-52 helicopters, the Izdeliye 305E light multi-purpose guided missile, Orlan-10 unmanned aerial vehicles (“UAVs”) and T-72B3 battle tanks.

27. GOLTSEV and NASRIDDINOV were aware that the electronics being shipped had potential military applications. In a February 23, 2023 message, NASRIDDINOV wrote to GOLTSEV, “Happy Defender of the Fatherland,” referring to the holiday in Russia and parts of the former Soviet Union celebrating those who served in the armed forces. NASRIDDINOV attached to the message a screenshot showing activity in an SH Brothers bank account. GOLTSEV responded, “happy holiday to you too my friend, we are defending it in the way that we can [smile emoji].”

A. GOLTSEV’s Relationship with Military End Users in Russia

28. Returns from court-authorized search warrants, as well as other evidence, shows GOLTSEV’s long-standing relationships with Radioavtomatika, Testkomplekt, EKB-Neva and other Russia-based entities. GOLTSEV has procured electronic components for such entities for more than 12 years.

29. Communications involving GOLTSEV and Russian procurement agents, including Co-conspirator 4 and others, described efforts to evade U.S. export controls and other laws and the fact that the electronic components were destined for military users in Russia. For example, in a text message exchange between GOLTSEV and Co-conspirator 4 on or about December 22, 2016, GOLTSEV advised that he “fully understands that this [ordered electronic component] is military in nature,” which Co-conspirator 4 directed GOLTSEV to “definitely send to Radioavtomatika, like in our agreement.” In another message exchange between GOLTSEV and Co-conspirator 4 on or about January 17, 2017, GOLTSEV stated, “I understand that this is a military end user” and recommended that Radioavtomatika should test the parts in their laboratory. In a subsequent message, Co-conspirator 4 advised GOLTSEV that Co-conspirator 4 was waiting for “the military to sign

the contract” before placing the order. In or about October 2021, Co-conspirator 4 again advised GOLTSEV that paperwork regarding an order of electronics stated that the items were destined for Russia. In response, GOLTSEV told Co-conspirator 4, “in that case, bill to World Jetta”— a reference to World Jetta (H.K.) Logistics Ltd., a Hong Kong company that BIS added to its Entity List on or about June 28, 2022—but confirmed that he would nevertheless send it to Radioavtomatika in Russia. In a message exchange on or about October 31, 2022, Co-conspirator 4’s subordinate employee asked GOLTSEV, “please tell me do you have these goods, [they are] priceless in Russia,” and listed several different electronic components, including coaxial switches and capacitors, that were barred from being shipped to Russia. GOLTSEV responded with price quotes for the items.

30. Communications between GOLTSEV and Russian procurement agents, including Co-conspirator 2, reflected a sophisticated understanding of U.S. export controls and sanctions. For example, on or about December 30, 2022, in a message exchange with Co-conspirator 2 regarding an order placed through SH Brothers, GOLTSEV requested “separate invoices . . . the ECCN[s] aren’t very pretty. We’ll ship them piecemeal.” In a message on or about February 23, 2023, GOLTSEV told Co-conspirator 2 that “Elnet [Electronic Network] got sanctioned . . . do me a favor. If anyone ever asks about me, don’t tell them who I am, where I am, etc. . . . Elnet’s been in trouble for a long time because they exported a lot to Russia.” Nevertheless, GOLTSEV confirmed he would be able to complete sales for “microchips, transistors, [and] circuits” because “we work with China, not Russia, therefore all is good.” In a subsequent conversation, Co-conspirator 2 again queried GOLTSEV about “any other USA companies that don’t mind selling to China.” GOLTSEV responded, “we have one for emergencies, but we’re keeping them as a last

resort.” Based on my training and experience, I assess that the reference to “China” was intended as a cover for the fact that GOLTSEV was using China as a transshipment location sending these controlled items to Russia.

31. GOLTSEV also received requests from Co-conspirator 3 to obtain items on the CCL that were controlled for anti-terrorism reasons. For example, on or about December 16, 2022, in response to a query, GOLTSEV advised Co-conspirator 3 that “76 pcs, you can buy them here with ECCN 3A991c.3.” In message on or about February 1, 2023, Co-conspirator 3 asked GOLTSEV, “ECCN: 5A991.b.4 can you get this?” and included a screenshot of a product from a Texas-based electronics distributor (“Texas Company 1”). Similarly, in a message on or about February 6, 2023, Co-conspirator 3 asked GOLTSEV, “can you get this ECCN? 4A994I.” Later, in a message on or about February 22, 2023, Co-conspirator 3 requested “40 pcs ECCN 5A991.b.1. Can you get this?” Between November 2022 and February 2023, SH Brothers made nine shipments to Co-conspirator 3 in Russia through a Turkish intermediary company.

B. The Establishment and Use of SH Brothers

32. Following the imposition of additional sanctions and export controls in response to Russia’s invasion of Ukraine in February 2022, GOLTSEV, NASRIDDINOV and PUZYREVA began using SH Brothers to facilitate illicit exports to Russia.

33. In a text message exchange between NASRIDDINOV and GOLTSEV on or about and between June 8, 2022 and June 9, 2022, NASRIDDINOV stated, “I spoke with the guys, we will set it up through America, I got to Moscow, tomorrow will also have a meeting, we decided upon logistics, if you have people in Moscow we can also meet and discuss the scheme so that they would pick up from Moscow.” GOLTSEV responded that

he had “many orders,” but that it was “becoming difficult to do business here [in Canada through Electronic Network], maybe it will be easier to do through the US . . . everything is loaded from the USA . . . everything that needs to be received, payment place the orders, get the goods together and unload it in any ‘friendly’ country.”

34. In or about and between August 2022 and September 2023, U.S. Customs and other records show that SH Brothers exported more than 250 shipments of electronic components, valued at more than \$7 million, to third-country transshipment companies; the shipments were then unlawfully diverted to Russia. During this same period, financial records, including wire transactions through correspondent accounts at New York City banks and within the Eastern District of New York, reflected millions of dollars in payments from Russian entities to these transshipment companies.

35. For example, in or about and between March 2023 and May 2023, SH Brothers shipped approximately \$404,949 worth of integrated circuits and other electronics to Co-conspirator 1 and his front company Suntronic in the UAE, which were then sent to Petersburg Intelligent Transport Logistics, a Russian entity that OFAC added to its SDN list on or about May 19, 2023. Notably, the Internet Protocol (“IP”) address for Suntronic, which was used to communicate with GOLTSEV about the orders, corresponded to a location in St. Petersburg, Russia, rather than the UAE.

C. SH Brothers Shipments to Testkomplekt, Komtech and Suntronic

36. In or about and between September 2022 and November 2022, customs and other records show that SH Brothers exported approximately 15 shipments of electronic components, valued at approximately \$352,000, to Testkomplekt in Russia through a Hong Kong intermediary company (“Hong Kong Company 1”). These exports included a

shipment on or about September 8, 2022 of connectors manufactured by a Texas company; a shipment on or about September 15, 2022 of connectors manufactured by a Pennsylvania and Switzerland-based company; a shipment on or about September 28, 2022 of computer modules manufactured by a Minnesota company; and a shipment on or about October 2, 2022 of converters manufactured by a Massachusetts company.

37. In or about November 2022, U.S. Customs and Border Protection (“CBP”) detained several shipments made by SH Brothers to Hong Kong Company 1 that were ultimately destined for Testkomplekt in Russia. In electronic message exchanges, Co-conspirator 2 repeatedly queried GOLTSEV about the status of these detained shipments and provided GOLTSEV with false information that GOLTSEV could use to respond to CBP inquiries. GOLTSEV communicated with CBP using the alias “Nick Stevens” and an SH Brothers email address with the signature “Procurement Department” and the SH Brothers’s Brooklyn, New York address. When asked about Hong Kong Company 1’s principal, GOLTSEV responded that the person had a Chinese-sounding surname rather than a Russian one.

38. In or about August 2022, SH Brothers made a shipment of microchips to Co-conspirator 4’s company, Komtech, through a Turkish intermediary (“Turkish Company 1”). These microchips had a Tier 1 HTS code listed on the Common High Priority Items List and required a license from BIS to be exported to Russia. Co-conspirator 4 acted as a go-between with GOLTSEV and Komtech’s founder and director. Specifically, in a message on or about August 31, 2022, Komtech’s founder and director requested that Co-conspirator 4 procure 3,000 microchips made by an Arizona-based manufacturer. Co-conspirator 4 sourced the microchips through GOLTSEV and SH

Brothers. SH Brothers received several payments from Turkish Company 1, including an October 3, 2022 payment for \$5,300. The wire details for this payment listed the part number of the microchips and denoted “QTY 2000.”

39. In a message exchange on or about April 21, 2023, Co-conspirator 4 and GOLTSEV discussed shipping the microchips through China or Turkey, ultimately deciding to make the shipment through Turkish Company 1 to “avoid problems.” GOLTSEV provided Co-conspirator 4 with an SH Brothers invoice for 3,000 pieces of the requested microchip. The invoice listed the applicable HTS codes and payment information for an SH Brothers bank account in Brooklyn, New York. Shipping records reflected that a package containing the microchips was mailed to SH Brothers from Texas Company 1 on or about April 17, 2023. Two days later, on or about April 25, 2023, the same items were sent by NASRIDINOV to Turkish Company 1 in Turkey.

40. Between in or about November 2022 and August 2023, SH Brothers exported approximately 27 shipments, valued at approximately \$1,086,058, to Suntronic. These shipments were then sent to Russian end users including Petersburg Intelligent Transportation Logistics. One such shipment on or about June 23, 2023 was for transceivers carrying a Tier 1 HTS code listed on the Common High Priority Items List, which required a license from BIS to be exported to Russia. These types of transceivers have been found in Russian UAVs in Ukraine. Notably, Suntronic received approximately \$15 million from Petersburg Intelligent Transportation Logistics in or about and between October 2022 and February 2023.

41. GOLTSEV communicated with Co-conspirator 1 to facilitate these shipments. In a message exchange on or about January 9, 2023, GOLTSEV informed Co-

conspirator 1 that he needed an “end user declaration,” to which Co-conspirator 1 responded, “darn.” GOLTSEV replied, “or at least let me know what end user to put in there and then send it tomorrow, but it needs to match the application.” Co-conspirator 1 responded, “then lets put the one we used last time,” and the two agreed to falsely list a UAE company as the end user.

42. Similarly, in or about February and March 2023, GOLTSEV and Co-conspirator 1 also communicated about falsifying the names of end users. In a message in or about February 2023, GOLTSEV advised Co-conspirator 1 to “write something more substantial [to the U.S. company] so that there are no more questions.” Co-conspirator 1 responded, “is it better to provide them with a Chinese end user,” to which GOLTSEV stated, “yes should be ok.” In a message on or about March 3, 2023, Co-conspirator 1 asked GOLTSEV if it was possible to make one shipment paid “via the Chinese company,” since “each one separately so expensive, or does it mean extra trouble at customs?” GOLTSEV responded, “no sir, more than 50-60 will trigger a lot of interest it’s better to break it up.”

D. The Establishment of SN Electronics

43. On or about and between November 8, 2022 and November 15, 2022, GOLTSEV and NASRIDINOV exchanged a series of messages in which GOLTSEV commented that shipping to Russia via third countries had become “dangerous” and discussed a shipment of electronic components that had been detained by U.S. officials at John F. Kennedy International Airport (“JFK Airport”) in Queens, New York. NASRIDINOV responded that “Ukrainians alleged that they’re being bombed from parts from there [a U.S. company], maybe that’s why they started investigating everything?”

GOLTSEV replied, “we need to figure out why they keep holding the package . . . I don’t really understand how they figured [it] out.” In a subsequent message, on or about November 9, 2022, GOLTSEV commented that, “in the future we will need to load from several companies, not to attract attention . . . for now large packages will be dangerous until we understand what they figured out . . . we will need to think of diversifying the load . . . so that not everything is moving from the same deck.”

44. In response to increased scrutiny from U.S. officials, including the delay or detention of several outbound shipments from SH Brothers at JFK Airport, in or about January 2023, GOLTSEV and NASRIDDINOV began using SN Electronics to order and export electronic components. In a text message exchange on or about and between January 31, 2023 and February 10, 2023, NASRIDDINOV confirmed to GOLTSEV that the “new company is already functioning . . . Its called SN Electronics.” GOLTSEV responded, “Wonderful sir. Eagerly waiting for Tax ID sir. We had problems with some large orders from [Texas Company 1] . . . we will reorder later from SN.” NASRIDDINOV later provided GOLTSEV with SN Electronics’ registered address in Brooklyn, New York, which was also the address of a restaurant that NASRIDDINOV controlled.

45. GOLTSEV and NASRIDDINOV then used SN Electronics to obtain approximately \$36,871 worth of non-reflective switches from Texas Company 1 for Co-conspirator 2 and Testkomplekt. These non-reflective switches had Tier 1 HTS codes that were included on the Common High Priority Items List and required a license from BIS to be exported to Russia.

46. GOLTSEV and NASRIDDINOV initially placed the order for these non-reflective switches from Texas Company 1 through SH Brothers. In or about January

2023, Texas Company 1 cancelled the order for SH Brothers and told GOLTSEV that the “manufacturer requires that shipments of this product be direct to an END CUSTOMER from an AUTHORIZED DISTRIBUTOR only.” Subsequently, GOLTSEV placed the same order through SN Electronics, using the alias “Gio Ross” in his email communications with Texas Company 1 and falsely claiming in an email on or about February 15, 2023 that SN Electronics was a “prototype and design manufacturing company.” Texas Company 1 shipped the order to an SN Electronics address in Brooklyn, New York on or about February 21, 2023. Once the shipment was made from Texas Company 1 to the SN Electronics address in Brooklyn—which, in reality, was NASRIDDINOV’s restaurant—shipping records revealed that, on or about February 27, 2023, the items were exported by NASRIDDINOV to Robotronix in Hong Kong, a transshipment company frequently utilized by Testkomplekt.

E. The Defendants Profited from the Criminal Scheme

47. The defendants and their co-conspirators profited from their criminal scheme. On or about September 15, 2022, in a text message from NASRIDDINOV to GOLTSEV, NASRIDDINOV boasted, “SH [Brothers] is one of the best companies in the world, it’s time to move forward onto the stock exchange and stock market, capital should be in the billions, we are working.” GOLTSEV responded, “pushing components to those who need it I can do, everything else you will have to teach me [three smile emojis].”

48. In a text message exchange on or about January 13, 2023, GOLTSEV complained to PUZYREVA that a subordinate of Co-conspirator 2 “asked me to make 80 accounts . . . I am making accounts for 3 mln [i.e., million]. Fingers hurting already from the laptop.” PUZYREVA responded, “Lot of money? We will get rich.” Later, on or about January 20, 2023, GOLTSEV messaged PUZYREVA, “Dasha [Co-conspirator 2’s

employee] paid. 700k.” Notably, financial records revealed wire transfers totaling approximately \$700,000 into an SH Brothers account on or about and between January 18, 2023 and January 26, 2023 from the Hong Kong-based Robotronix in connection with an order for Testkomplekt.

49. PUZYREVA utilized numerous bank accounts to make financial transactions in furtherance of the scheme. For example, PUZYREVA was the signatory on two New York-based bank accounts, one that listed NASRIDDINOV’s home address in Brooklyn, New York as the address of record. Statements for these accounts reflected large cash deposits made in Brooklyn that corresponded with trips that PUZYREVA and the GOLTSEV made from Canada to meet with NASRIDDINOV. Some of these deposits were in amounts just under \$10,000. Notably the Internal Revenue Service (“IRS”) maintains a transaction reporting requirement providing that any person who, during trade or business, receives more than \$10,000 cash in a single transaction is required report the transaction to the IRS. For example, on or about December 27, 2022, a \$9,800 cash deposit was made into one of PUZYREVA’s accounts at an automated teller machine (“ATM”) in Manhattan, New York. On or about May 23, 2022, a cash deposit of \$8,700 was made into one of PUZYREVA’s accounts at an ATM in Manhattan, while a \$4,000 deposit was made on the same day into the same account from an ATM in Brooklyn located near an address used by NASRIDDINOV and SH Brothers. On or about March 13, 2023, a cash deposit of \$9,700 was made into one of PUZYREVA’s accounts at an ATM in Manhattan. These deposits were then transferred to accounts held and used by PUZYREVA and GOLTSEV in Canada.

WHEREFORE, your deponent respectfully requests that an arrest warrant be issued for the defendants NIKOLAY GOLTSEV, SALIMDZHON NASRIDINOV and KRISTINA PUZYREVA, so that they may be dealt with according to law.

IT IS FURTHER REQUESTED that this Court issue an order sealing, until further order of the Court, all papers submitted in support of this application, including this Affidavit and any arrest warrants issued, with the exception that the complaint and arrest warrant can be unsealed for the limited purpose of disclosing the existence of, or disseminating, the complaint and/or arrest warrant to relevant United States, foreign or intergovernmental authorities, at the discretion of the United States and in connection with efforts to prosecute the defendant or to secure the defendant's arrest, extradition or expulsion. Based on my training and experience, I have learned that criminals actively search for criminal affidavits on the Internet and disseminate them to other criminals as they deem appropriate, such as by posting them publicly through online forums. Premature disclosure of the contents of this Affidavit and related documents will seriously jeopardize the investigation, including by giving targets an opportunity to flee or continue flight from

prosecution, destroy or tamper with evidence, change patterns of behavior and notify confederates.



Yevgeny Gershman
Special Agent
United States Department of Homeland Security,
Homeland Security Investigations

Sworn to before me this
30th day of October, 2023



THE HONORABLE LOIS BLOOM
UNITED STATES MAGISTRATE JUDGE
EASTERN DISTRICT OF NEW YORK

**TO: Clerk's Office
UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK**



**APPLICATION FOR LEAVE
TO FILE DOCUMENT UNDER SEAL**

US v. Goltsev et al

23-MJ-956
Docket Number

SUBMITTED BY: Plaintiff ___ Defendant ___ DOJ
Name: Artie McConnell
Firm Name: USDOJ-EDNY
Address: _____

Phone Number: 718-254-7150
E-Mail Address: artie.mcconnell@usdoj.gov

INDICATE UPON THE PUBLIC DOCKET SHEET: YES ___ NO

If yes, state description of document to be entered on docket sheet:

MANDATORY CERTIFICATION OF SERVICE:

A.) ___ A copy of this application either has been or will be promptly served upon all parties to this action, B.) ___ Service is excused by 31 U.S.C. 3730(b), or by the following other statute or regulation: _____; or C.) ___ This is a criminal document submitted, and flight public safety, or security are significant concerns. (Check one)

10/30/2023
DATE

/s/ Artie McConnell
SIGNATURE

A) If pursuant to a prior Court Order:

Docket Number of Case in Which Entered: _____
Judge/Magistrate Judge: _____
Date Entered: _____

B) If a new application, the statute, regulation, or other legal basis that authorizes filing under seal

**ORDERED SEALED AND PLACED IN THE CLERK'S OFFICE,
AND MAY NOT BE UNSEALED UNLESS ORDERED BY
THE COURT.**

DATED: ~~XXXXXX~~ Central Islip, NEW YORK

Brooklyn, NY 10/30/23

Lois Bloom

U.S. MAGISTRATE JUDGE

RECEIVED IN CLERK'S OFFICE _____
DATE

UNITED STATES DISTRICT COURT

District of Kansas
(Kansas City Docket)

UNITED STATES OF AMERICA,

Plaintiff,

v.

CASE NO. 23-20010-DDC/TJJ
Filed Under Seal

CYRIL GREGORY BUYANOVSKY,
a.k.a. KIRILL BUYANOVSKY,

and

DOUGLAS EDWARD ROBERTSON,

Defendants.

INDICTMENT

THE GRAND JURY CHARGES:

At all times material to this Indictment:

BACKGROUND

1. Since at least October 2020 to the present, CYRIL GREGORY BUYANOVSKY, a/k/a Kirill Buyanovsky, and DOUGLAS EDWARD ROBERTSON, the defendants, conspired to circumvent U.S. export laws and regulations in order to sell,

repair, and ship from the United States sophisticated avionics equipment to customers around the world that operate Russian-built aircraft. Avionics are the electronics installed in aircraft and can include communications, navigation, flight control, and threat detection systems.

2. In the course of exporting avionics equipment from the United States through their company, KanRus Trading Company Inc. (“KanRus”), which is located in the District of Kansas, BUYANOVSKY and ROBERTSON repeatedly concealed and misstated the true end users, value, and end destinations of their exports by creating false invoices; submitting false information on export documents; failing to file required export documents; transshipping items through third-party countries, such as Germany, the United Arab Emirates (“UAE”), Cyprus, and Armenia; exporting items to intermediary companies that then reexported the items to the ultimate end destinations; and receiving payments from foreign bank accounts located in the UAE, Cyprus, Russia, and Armenia.

3. After the Russian Federation’s unprovoked invasion of Ukraine on February 24, 2022, and the imposition of additional restrictions on the export of avionics from the United States to Russia, BUYANOVSKY and ROBERTSON continued to export avionics to Russia despite knowing that such exports required a license from the U.S. Department of Commerce, which they neither sought nor obtained.

Individuals and Companies

4. The defendant CYRIL GREGORY BUYANOVSKY, also known as Kirill Buyanovsky, was a naturalized U.S. citizen who resided in Douglas County, Kansas.

BUYANOVSKY was the president and owner of KanRus. BUYANOVSKY previously worked at an avionics manufacturer as an engineer.

5. The defendant DOUGLAS EDWARD ROBERTSON was a U.S. citizen who resided in Johnson County, Kansas. ROBERTSON was a commercial pilot and operated KanRus with BUYANOVSKY.

6. KanRus was registered in the District of Kansas and supplied Western avionics equipment, including U.S.-origin equipment, and repair services for Russian-manufactured aircraft.

7. “Russian Company-1” was located in Moscow, Russia and was a Russian aircraft parts distributor. “Individual-1,” whose identity is known to the Grand Jury, was a Russian national and the chief executive officer of Russian Company-1.

8. “Russian Company-2” was located in Krasnodar, Russia and provided aerial services using its fleet of helicopters. “Individual-2,” whose identity is known to the Grand Jury, was an engineer working for Russian Company-2.

9. “Russian Company-3” was located in Moscow, Russia and was a Russian aircraft maintenance, repair, and overhaul company. “Individual-3,” whose identity is known to the Grand Jury, was an intermediary who negotiated and processed orders from Russian Company-3 for KanRus, BUYANOVSKY, and ROBERTSON.

10. “Russian Company-4” was located in Moscow, Russia and was a Russian aircraft parts distributor. “Individual-3” was an intermediary who negotiated and processed orders from Russian Company-4 for KanRus, BUYANOVSKY, and ROBERTSON.

11. “UAE Company-1” was located in Ajman, UAE and was a trading company that sent KanRus funds on behalf of Russian Company-3.

12. “German Company-1” was located in Schöneck, Germany and was a logistics company that Russian Company-3 used to send and receive avionics equipment to and from KanRus in the United States.

13. “Armenian Company-1” was located in Yerevan, Armenia and was a company that Russian Company-1 used to transship avionics equipment to Russia.

The Statutory and Regulatory Background

The Export Control Reform Act and Export Administration Regulations

14. The Export Administration Regulations (“EAR”), Title 15, Code of Federal Regulations, Sections 730-774, were promulgated by the United States Department of Commerce, Bureau of Industry and Security (“BIS”) to regulate the export of goods, technology, and software from the United States. Under the Export Control Reform Act (“ECRA”), it was a crime to violate, attempt to violate, conspire to violate, or cause a violation of any regulation, order, license, or authorization issued pursuant to the statute, including the EAR, according to Title 50, United States Code, Section 4819(b). Willful violations of the EAR constituted criminal offenses under the ECRA, as provided in Title 50, United States Code, Section 4819(b).

15. Through the EAR, BIS reviewed and controlled the export of certain items from the United States to foreign countries in accord with Title 15, Code of Federal Regulations, Sections 734.2-3. In particular, BIS placed restrictions on the export and reexport of items that it determined could make a significant contribution to the military

potential of other nations or that could be detrimental to the foreign policy or national security of the United States. Under the EAR, such restrictions depended on several factors, including the technical characteristics of the item, the destination country, the end user, and the end use of the item.

16. The most sensitive items subject to the EAR controls were identified on the Commerce Control List (“CCL”) set forth in Title 15, Code of Federal Regulations, part 774, Supplement Number 1. Items listed on the CCL were categorized by an Export Control Classification Number (“ECCN”), each of which was subject to export control requirements depending on destination, end use, and end user of the item.

17. On February 24, 2022, in response to the Russian Federation’s unprovoked invasion of Ukraine, the U.S. Department of Commerce imposed new license requirements on exports and reexports to Russia. As of February 24, 2022, any item classified under any ECCN in Categories 3 through 9 of the CCL required a license to be exported to Russia. *See* Volume 87, Federal Register, Page 12226 (published Mar. 3, 2022).

The Commerce Control List Items

18. A Traffic Alert and Collision Avoidance System (“TCAS”), or airborne collision avoidance system, is a family of airborne devices that function independently of the ground-based air traffic control system and provide collision avoidance protection for a broad spectrum of aircraft types. A TCAS is composed of many components, including a computer processor unit, transponders, control and display panels, and antennas.

19. During the relevant period, certain components of a TCAS were on the CCL and classified by BIS under ECCN 7A994 (other navigation direction finding equipment, airborne communication equipment, all aircraft inertial navigation systems not controlled under 7A003 or 7A103, and other avionic equipment, including “parts” and “components”).

20. During the relevant time period, the following avionics were on the CCL and classified by BIS under ECCN 7A994 (navigation/communication systems): Honeywell BendixKing KI-203 installation kit, Honeywell BendixKing KT-74 transponder, and Honeywell BendixKing KA-61 L-Band antenna. As of February 24, 2022, an export license was required from the Department of Commerce to export these avionics to Russia.

Export and Shipping Records

21. Pursuant to U.S. law and regulations, exporters or their authorized agents, such as shippers or freight forwarders, are required to file certain forms and declarations concerning the export of goods and technology from the United States. Typically, those documents are filed electronically through the Automated Export System (“AES”), which is administered by the U.S. Department of Homeland Security, Customs and Border Protection (“CBP”).

22. The Electronic Export Information (“EEI”) (formerly known as the Shipper’s Export Declaration (“SED”)) is the required documentation submitted to the U.S. Government through the AES in connection with an export shipment from the United States. Exporters or their authorized agents are required to file accurate and

truthful EEI for every export of goods from the United States with a value of \$2,500 or more. An EEI also is required regardless of the value of the goods if the goods require an export license. Title 15, Code of Federal Regulations, Sections 758.1, 30.2

23. A material part of the EEI and AES, as well as other export filings, is information concerning the end user and ultimate destination of the export. The identity of the end user may determine whether the goods: (a) may be exported without any specific authorization or license from the U.S. Government; (b) may be exported with the specific authorization or license from the U.S. Government; or (c) may not be exported from the United States.

24. As of June 29, 2020, all exports to Russia of items on the CCL, regardless of value, required an EEI filing. Title 15, Code of Federal Regulations, Section 758.1(b)(10).

25. The purpose of these requirements is to strengthen the U.S. Government's ability to prevent the export of certain items to unauthorized destinations and end users because the EEI and AES aid in targeting, identifying, and when necessary, confiscating suspicious or illegal shipments before exportation. Title 15, Code of Federal Regulations, Section 30.1(b).

COUNT 1

CONSPIRACY TO COMMIT OFFENSES AGAINST THE UNITED STATES [18 U.S.C. § 371]

26. Paragraphs 1 to 25 of the introductory allegations are restated and realleged as if set forth herein.

27. Between at least in or about 2020 and continuing to the present, the exact dates being unknown to the Grand Jury, in the District of Kansas and elsewhere, the defendants,

**CYRIL BUYANOVSKY, a.k.a. KIRILL BUYANOVSKY,
and
DOUGLAS EDWARD ROBERTSON,**

did knowingly and willfully combine, conspire, confederate, and agree with each other and with others known and unknown to the Grand Jury, including individuals associated with Russian Company-1, Russian Company-2, Russian Company-3, and Russian Company-4, to commit offenses against the United States, that is:

- a. to willfully export and cause the exportation of goods from the United States to Russia without first having obtained the required licenses from the Department of Commerce in violation of Title 50, United States Code, Section 4819(a), and Title 15, Code of Federal Regulations, Section 764.2;
- b. to knowingly fail to file and submit false and misleading export information through the EEI and the AES, and cause the same, in violation of Title 13, United States Code, Section 305, and Title 15, Code of Federal Regulations, Section 30.71; and
- c. to fraudulently and knowingly export and send and attempt to export and send from the United States merchandise, articles, and objects contrary to laws and regulations of the United States, and receive, conceal, buy, sell, and facilitate the transportation, concealment, and sale of such merchandise, articles, and objects, prior to exportation, knowing the same to be intended for exportation

contrary to laws and regulations of the United States, in violation of Title 18, United States Code, Section 554.

Objects of the Conspiracy

28. The objects of the conspiracy were:

a. to acquire avionics equipment that was manufactured and sold in the United States on behalf of entities that operated Russian-built aircraft in Russia and other countries;

b. to repair and recertify in the United States avionics equipment that was used in Russian-built aircraft located and operated outside of the United States;

c. to export avionics equipment from the United States directly and indirectly, to Russia and Russian end users located in other countries;

d. to conceal the prohibited activities and transactions from detection by the U.S. Government so as to avoid penalties and disruption of the illegal activities;

e. to profit through these illegal activities; and

f. to evade the prohibitions and licensing requirements of the ECRA and EAR.

Manner and Means of the Conspiracy

29. Defendants BUYANOVSKY and ROBERTSON and other co-conspirators known and unknown to the Grand Jury used the following manner and means, among others, to accomplish the objects of the conspiracy:

- a. BUYANOVSKY, ROBERTSON, and other co-conspirators, including individuals associated with Russian Company-1, Russian Company-2, Russian Company-3, and Russian Company-4, used email and other means to communicate;
- b. Individuals associated with Russian Company-1, Russian Company-2, Russian Company-3, and Russian Company-4 solicited quotes from and negotiated with BUYANOVSKY and ROBERTSON for the purchase and repair of U.S. avionics equipment for Russian customers and customers that operated Russian-built aircraft;
- c. BUYANOVSKY and ROBERTSON purchased items from companies in the United States to fulfill orders from Russian customers, including by providing false information to the U.S. companies;
- d. BUYANOVSKY and ROBERTSON used coded language in their email communications to conceal their illegal conduct;
- e. BUYANOVSKY, ROBERTSON, and other co-conspirators, including individuals associated with Russian Company-1, Russian Company-2, and Russian Company-3, arranged for shipment of the U.S. goods from the United

States to transshipment points in Germany, the UAE, Cyprus, and Armenia to conceal the true end users and end destinations;

f. BUYANOVSKY and ROBERTSON falsified export and shipping records regarding shipments from the United States, including by providing false and misleading information to the shippers and freight forwarders, to conceal the true value of the goods, the ultimate destination of the goods, and the ultimate end user of the goods;

g. Individuals associated with Russian Company-1, Russian Company-2, and Russian Company-3 transferred funds for the purchase and shipment of the goods through bank accounts in the UAE, Russia, Cyprus, and Armenia to KanRus's bank account in the United States; and

h. BUYANOVSKY, ROBERTSON, and other co-conspirators, including individuals associated with Russian Company-1, caused the U.S. goods to be exported from the United States to individuals and entities in Russia without obtaining the required licenses from the Department of Commerce.

Overt Acts in Furtherance of the Conspiracy

30. In furtherance of the conspiracy and to achieve the objects thereof, Defendant BUYANOVSKY, Defendant ROBERTSON, and others committed and caused to be committed the following overt acts, among others, in the District of Kansas and elsewhere:

February 4, 2021 Export to Russian Company-2 in South Sudan

31. On or about October 14, 2020, Individual-2, an engineer at the helicopter company Russian Company-2, sought a quote to repair a computer component of a TCAS that was located in South Sudan. After BUYANOVSKY advised that the component could not be imported from or exported to South Sudan, BUYANOVSKY and Individual-2 agreed to ship the component from and return it to the UAE.

32. On or about November 11, 2020, Individual-2 emailed a draft invoice to BUYANOVSKY, which BUYANOVSKY then forwarded to ROBERTSON and asked him to look at before the component was shipped. The invoice listed the customer as a UAE company, did not mention Russian Company-2 or South Sudan, and falsely listed the value of the component as \$100.

33. On or about November 11, 2020, BUYANOVSKY emailed the aforementioned invoice back to Individual-2, along with a separate stamped invoice that listed the true value of the transaction as \$10,950. Individual-2 responded and asked whether the value of the component could be undervalued on the shipping invoice (*i.e.*, the invoice that would accompany the component when it was shipped) to lower the customs fees at the destination. BUYANOVSKY agreed to lower the value on the shipping invoice.

34. On or about November 25, 2020, Russian Company-2 made a payment from a Cypriot bank account to KanRus's bank account for this export.

35. On or about December 5, 2020, Russian Company-2 shipped the TCAS computer component from the UAE to KanRus in the District of Kansas. The reported U.S. customs value on the shipment was \$100.

36. Upon receipt of the TCAS computer component, BUYANOVSKY emailed a U.S. company to request pricing for the repair. During those communications, the U.S. company requested that BUYANOVSKY complete an end-use and end-user statement. BUYANOVSKY forwarded the request to Individual-2, who completed and returned the statement. BUYANOVSKY then forwarded the end-use and end-user statement to the U.S. company. The statement claimed, among other things, that Russian Company-2 was the end user and that the component would be delivered to Russia. The statement failed to mention South Sudan.

37. On or about February 4, 2021, BUYANOVSKY and ROBERTSON exported the repaired TCAS computer component to the address of another UAE company that Individual-2 had provided to BUYANOVSKY.

38. On or about February 4, 2021, BUYANOVSKY caused the shipper to fail to file an EEI in connection with this export.

February 26, 2021 Export to Russian Company-3 in Russia

39. On or about November 11, 2020, Individual-3 from Russian Company-3 emailed ROBERTSON a list of avionics equipment for KanRus to repair in the United States, along with a shipping label that showed the equipment being shipped from German Company-1 to KanRus. Individual-3 also sent ROBERTSON a proforma

customs invoice that valued the equipment at \$380 and listed the shipper as a UAE company that had the same name as Russian Company-3.

40. On or about November 20, 2020, ROBERTSON emailed Individual-3 and described the specific pieces of avionics equipment that he had received from Individual-3. One of the pieces of equipment was a TCAS computer processor called a TPU. Regarding the TPU, ROBERTSON wrote, “TPU has a ФСБ [*i.e.*, FSB] sticker on it!!!” In response, Individual-3 wrote, “Interesting about sticker, you can remove and after stick on back?” FSB is the acronym for the Federal Security Service of the Russian Federation, which is the principal intelligence and security agency of the Russian government.

41. On or about January 27, 2021, ROBERTSON emailed Individual-3 an invoice for the repairs with a total value of \$28,769. The invoice listed German Company-1 as the recipient company and UAE Company-1 as the payor company.

42. On or about February 9, 2021, UAE Company-1 made a payment to KanRus’s U.S. bank account for this export.

43. The next day, on or about February 10, 2021, Individual-3 emailed ROBERTSON a proposed “shipping” invoice that undervalued the repaired goods at \$3,645.

44. On or about February 25, 2021, ROBERTSON asked Individual-3, “can I change value to less than \$2500? Less paperwork for me.”

45. On or about February 26, 2021, ROBERTSON exported some of the repaired avionics equipment to German Company-1, specifically the TPU processor and a radar sensor.

46. On or about February 26, 2021, ROBERTSON sent Individual-3 a copy of the shipping label and invoice that undervalued the equipment at \$2,275.

47. On or about February 26, 2021, ROBERTSON caused the shipper to fail to file an EEI in connection with this export.

April 1, 2021 Export of Large Avionics Shipment to Russian Company-3

48. On or about January 20, 2021, Individual-3 emailed ROBERTSON to ask for a quote for an order of multiple avionics components, including a TPU processor, antennas, and transponders. ROBERTSON provided a quote and asked, “When is [Russian Company-3] wanting to pay?”

49. On or about January 27, 2021, ROBERTSON emailed Individual-3 a stamped invoice for the shipment valuing the goods at \$159,625. As with the February 26, 2021 export, UAE Company-1 was listed as the payor company and German Company-1 was listed as the recipient company.

50. On or about February 8, 2021, UAE Company-1 sent \$159,625 to KanRus’s U.S. bank account. Later that day, BUYANOVSKY emailed ROBERTSON and told him that the order was “fully funded to the tune of 159625 this morning.”

51. After on or about February 8, 2021, ROBERTSON and BUYANOVSKY proceeded to purchase the avionics equipment from U.S. companies.

52. On or about March 29, 2021, ROBERTSON emailed a freight forwarder an invoice for this shipment that listed the value of the goods as \$6,118 and the recipient as Germany Company-1. ROBERTSON also attached a Shipper's Letter of Instructions that identified German Company-1 as the ultimate consignee and incorrectly listed the ECCN for the components as EAR99.

53. On or about April 1, 2021, ROBERTSON caused the avionics equipment to be exported.

54. On or about April 1, 2021, ROBERTSON caused the shipper to file a false and misleading EEI that listed the value of the export as \$6,118 and the ultimate consignee as Germany Company-1 when, in fact, the avionics shipment was valued at \$159,625 and was destined for Russian Company-3.

February 28, 2022 Attempted Export to Russian Company-1 and Detention

55. On or about February 7, 2022, Individual-1 placed an order with BUYANOVSKY to order Honeywell BendixKing KT-74 transponders from a U.S. company and ship them to Russia. Individual-1 also told BUYANOVSKY that after BUYANOVSKY received the transponders from the U.S. supplier and received payment from Individual-1, the transponders needed to be sent to Individual-1 in Russia.

56. On or about February 10, 2022, Russian Company-1 made a payment from a Russian bank account to KanRus's bank account for four KT-74 transponders.

57. On or about February 18, 2022, Russian Company-1 made a payment from a Russian bank account to KanRus's bank account for four more KT-74 transponders.

58. On or about February 28, 2022, ROBERTSON attempted to export the eight KT-74 transponders to Russian Company-1 in Russia, but the shipment was detained by the U.S. Government, after which BIS directly informed ROBERTSON that a license was required to export the KT-74 transponders to Russia.

April 29, 2022 Export to Laos for Russian Company-4

59. On or about January 27, 2022, Individual-3 sent ROBERTSON an invoice to purchase two Honeywell BendixKing KT-74 transponders, two Honeywell BendixKing KN-53 navigation receivers, and two Honeywell BendixKing KN-53 installation kits and export them to Russian Company-4 in Russia for \$27,806.

60. On or about January 31, 2022, Russian Company-4 made a payment from its Russian bank account to KanRus's U.S. bank account for this export.

61. On or about March 8, 2022, after Russia's invasion of Ukraine, the U.S. Government's imposition of additional restrictions on exports and reexports to Russia, and the U.S. Government's detention of KanRus's attempted export to Russian Company-1, ROBERTSON emailed BUYANOVSKY. ROBERTSON attached a proposed letter to send to Individual-3, which described the current options for shipping as either shipping within the U.S. or shipping to a company in a neutral country that was not a logistics company and did not have ties to Russia.

62. On or about March 8, 2022, ROBERTSON emailed the "shipping options" letter to Individual-3.

63. After on or about March 8, 2022, ROBERTSON and Individual-3 exchanged emails discussing possible shipping options, including whether specific companies in the UAE or Laos would be acceptable recipients.

64. On or about March 30, 2022, Individual-3 sent ROBERTSON an email that stated that Russian Company-4 wanted to ship the avionics equipment directly to Laos.

65. On or about April 27, 2022, ROBERTSON exchanged emails with Individual-3 in which he stated, among other things, that “things are complicated in USA,” and that the invoice amount needed to be less than \$50,000 because, otherwise, there would be “more paperwork and visibility” and “This is NOT the right time for either.”

66. On or about April 29, 2022, ROBERTSON caused the avionics equipment to be exported to Laos.

May 20, 2022 Export to Russian Company-1 via Cyprus

67. On or about April 26, 2022, Individual-1, who was the chief executive officer of Russia Company-1, booked a flight from Russia to Cyprus scheduled to depart on or about May 14, 2022.

68. On or about May 16, 2022, BUYANOVSKY ordered seven Honeywell BendixKing KI-203 installation kits for Individual-1. These kits were on the CCL, classified by BIS under ECCN 7A994, and required a license from the Commerce Department to be exported or reexported to Russia.

69. On or about May 20, 2022, Individual-1 made a payment from a Cypriot bank account to KanRus’s bank account for this export.

70. On or about May 20, 2022, ROBERTSON caused the seven installation kits to be exported to Individual-1 at a residential address in Cyprus.

71. On or about May 20, 2022, ROBERTSON caused the shipper to fail to file an EEI in connection with this export.

72. On or about May 20, 2022, BUYANOVSKY emailed the invoice and shipping label for this export to Individual-1.

73. On or about May 26, 2022, Individual-1 received the package of seven KI-203 installation kits in Cyprus.

74. On or about May 28, 2022, Individual-1 flew back to Russia from Cyprus.

75. At no time did either ROBERTSON or BUYANOVSKY obtain the required license from the Commerce Department to export or reexport the KI-203 installation kits to Russia.

June 16, 2022 Export to Russian Company-1 via Armenia

76. On or about June 9, 2022, Armenian Company-1 emailed BUYANOVSKY and asked for an offer for eight KT-74 transponders to be exported to Yerevan, Armenia. The eight transponders were the same make and model of the eight transponders that ROBERTSON and BUYANOVSKY had attempted to export to Individual-1 of Russian Company-1 in February 2022 as described in paragraphs 55 to 58. BUYANOVSKY then forwarded the proposed invoice for the shipment to ROBERTSON and wrote that, “The V [*i.e.*, the first initial of Individual-1’s last name] connection requested an invoice and for some reason they wanted the transportation cost to Yerevan. . . . Is export department ok with this?”

77. On or about June 16, 2022, ROBERTSON caused the eight KT-74 transponders to be exported to Armenian Company-1. The KT-74 transponders were on the CCL, classified by BIS under ECCN 7A994, and required a license from the Commerce Department to be exported or reexported to Russia.

78. On or about June 16, 2022, ROBERTSON caused the shipper to fail to file an EEI for this export.

79. On or about June 28, 2022, Armenian Company-1 reexported the KT-74 transponders from Armenia to Russia.

80. At no time did either ROBERTSON or BUYANOVSKY obtain the required license from the Commerce Department to export or reexport the KT-74 transponders to Russia.

July 18, 2022 Export to Russian Company-1 via Armenia

81. On or about July 11, 2022, ROBERTSON and BUYANOVSKY emailed each other about another export to Armenian Company-1. The subject line of the email exchange was, “V” – the first initial of Individual-1’s last name. BUYANOVSKY told ROBERTSON that a “somewhat more proper sequence of events can now proceed” and that “V will pay once they get the invoice.”

82. Also on or about July 11, 2022, Armenian Company-1 made a payment from an Armenian bank account to KanRus’s bank account for eight Honeywell BendixKing KA-61 L-Band antennas.

83. On or about July 18, 2022, ROBERTSON emailed the shipping documents for this export to BUYANOVSKY and caused the export of the eight KA-61 antennas to

Armenian Company-1. The KA-61 antennas were on the CCL, classified by BIS under ECCN 7A994, and required a license from the Commerce Department to be exported or reexported to Russia.

84. On or about July 18, 2022, ROBERTSON caused the shipper to fail to file an EEI for this export.

85. On or about July 27, 2022, the Armenian company reexported the eight KA-61 antennas to Russia.

86. At no time did either ROBERTSON or BUYANOVSKY obtain the required license from the Commerce Department to export or reexport the KA-61 antennas to Russia.

87. All in violation of Title 18, United States Code, Section 371.

COUNTS 2-4

**UNLAWFUL EXPORT OF U.S.-ORIGIN CONTROLLED GOODS TO RUSSIA
[50 U.S.C. § 4819]**

88. The factual allegations in paragraphs 1 to 87 are hereby realleged and incorporated as if set forth in this paragraph.

89. On or about the dates listed for each count, in the District of Kansas and elsewhere, the defendants,

**CYRIL BUYANOVSKY, a.k.a. KIRILL BUYANOVSKY,
and
DOUGLAS EDWARD ROBERTSON,**

knowingly and willfully exported and attempted to export and caused to be exported from the United States to Russia the items identified for each count, without first having obtained the required authorization and license from the Commerce Department:

Count	Approximate Date of Export	Exported Items
2	May 20, 2022	Seven (7) KI-203 installation kits
3	June 16, 2022	Eight (8) KT-74 transponders
4	July 18, 2022	Eight (8) KA-61 antennas

in violation of Title 50, United States Code, Section 4819; Title 15, Code of Federal Regulations, Section 764.2; and Title 18, United States Code, Section 2.

COUNTS 5-7

SUBMITTING FALSE OR MISLEADING EXPORT INFORMATION [13 U.S.C. § 305]

90. The factual allegations in paragraphs 1 to 87 are hereby realleged and incorporated as if set forth in this paragraph.

91. On or about the dates listed for each count, in the District of Kansas and elsewhere, the defendants,

CYRIL BUYANOVKSY, a.k.a. KIRILL BUYANOVSKY, and DOUGLAS EDWARD ROBERTSON,

knowingly and willfully failed to file and submitted false and misleading information through the Electronic Export Information and the Automated Export System, and caused the same, in connection with the exported items identified in each count:

Count	Approximate Date of Export	Exported Items
5	February 4, 2021	TRC-899 TCAS computer component
6	February 26, 2021	TPU-67A TCAS computer processor; ART-2100 radar sensor
7	April 1, 2021	TPU-67B TCAS computer processor; MST-67A transponder; two (2) IVA-81D TCAS speed indicators; PS-578 transponder; ANT-67A antenna

in violation of Title 13, United States Code, Section 305; Title 15, Code of Federal Regulations, Section 30.71; and Title 18, United States Code, Section 2.

COUNTS 8-13

SMUGGLING GOODS FROM THE UNITED STATES [18 U.S.C. § 554]

92. The factual allegations in paragraphs 1 to 87 are hereby realleged and incorporated as if set forth in this paragraph.

93. On or about the dates listed for each count, in the District of Kansas and elsewhere, the defendants,

CYRIL BUYANOVSKY, a.k.a. KIRILL BUYANOVSKY, and DOUGLAS EDWARD ROBERTSON,

fraudulently and knowingly exported and sent and attempted to export and send from the United States the merchandise, articles, and objects identified in each count, contrary to the laws and regulations of the United States, to wit, Title 50, United States Code, Section 4819; Title 15, Code of Federal Regulations, Section 764.2; Title 13, United States Code, Section 305; and Title 15, Code of Federal Regulations, Section 30.71, and

fraudulently and knowingly received, concealed, bought, sold, and facilitated the transportation, concealment, and sale of such merchandise, articles, and objects, prior to exportation, knowing the same to be intended for export contrary to such laws and regulations of the United States:

Count	Approximate Date of Export	Exported Items
8	February 4, 2021	TRC-899 TCAS computer component
9	February 26, 2021	TPU-67A TCAS computer processor; ART-2100 radar sensor
10	April 1, 2021	TPU-67B TCAS computer processor; MST-67A transponder; two (2) IVA-81D TCAS speed indicators; PS-578 transponder; ANT-67A antenna
11	May 20, 2022	Seven (7) KI-203 installation kits
12	June 16, 2022	Eight (8) KT-74 transponders
13	July 18, 2022	Eight (8) KA-61 antennas

in violation of Title 18, United States Code, Sections 554 and 2.

FORFEITURE NOTICE

94. The allegations contained in paragraphs 1 to 93 and Counts 1-13 of this Indictment are hereby realleged and incorporated by reference for the purpose of alleging forfeiture pursuant to Title 50, United States Code, Section 4819, Title 13, United States Code, Section 305, Title 18, United States Code, Section 981(a)(1)(C), and Title 28, United States Code, Section 2461.

95. Upon conviction of one or more of the offenses set forth in Counts 1-4 of this Indictment, the defendants shall forfeit to the United States, pursuant to Title 50,

United States Code, Section 4819, any property: used or intended to be used in any manner to commit or facilitate the offenses; constituting or traceable to the gross proceeds taken, obtained, or retained, in connection with or as a result of the violations; or constituting an item or technology that is exported or intended to be exported in violation of the offenses. The property to be forfeited includes, but is not limited to, the following:

A. A forfeiture money judgment against each defendant in an amount equal to the amount of gross proceeds obtained or derived by that defendant from the commission of Counts 1-4.

96. Upon conviction of one or more of the offenses set forth in Counts 5-7 of this Indictment, the defendants shall forfeit to the United States of America, pursuant to Title 13, United States Code, Section 305, any interest in, security of, claim against, or property or contractual rights of any kind in the goods or tangible items that were the subject of the offenses; any interest in, security of, claim against, or property or contractual rights of any kind in tangible property that was used in the export or attempt to export that was the subject of the offenses; and any property constituting, or derived from, any proceeds obtained directly or indirectly as a result of the offenses.

97. Upon conviction of one or more of the offenses set forth in Counts 8-13 of this Indictment, the defendants shall forfeit to the United States of America, pursuant to Title 18, United States Code, Section 981(a)(1)(C) and Title 28, United States Code, Section 2461, any property, real or personal, which constitutes or is derived from proceeds traceable to the offenses. The property to be forfeited includes, but is not limited to, the following:

A. A forfeiture money judgment against each defendant in an amount equal to the amount of gross proceeds obtained or derived by that defendant from the commission of Counts 8-13.

98. If any of the property described above, as a result of any act or omission of the defendants:

- A. cannot be located upon the exercise of due diligence;
- B. has been transferred or sold to, or deposited with, a third party;
- C. has been placed beyond the jurisdiction of the court;
- D. has been substantially diminished in value; or
- E. has been commingled with other property which cannot be divided without difficulty,

the United States of America shall be entitled to forfeiture of substitute property pursuant to Title 21, United States Code, Section 853(p).

A TRUE BILL.

March 1, 2023
DATE

s/Foreperson
FOREPERSON OF THE GRAND JURY

DUSTON J. SLINKARD
UNITED STATES ATTORNEY

By: /s/ Ryan Huschka
RYAN HUSCHKA
Assistant United States Attorney
District of Kansas
500 State Avenue, Suite 360

Kansas City, Kansas 66101
Ph: (913) 551-6730
Fax: (913) 551-6541
Email: ryan.huschka@usdoj.gov
Ks. S. Ct. No. 23840

By: /s/ Scott C. Rask
SCOTT C. RASK
Assistant United States Attorney
District of Kansas
500 State Avenue, Suite 360
Kansas City, Kansas 66101
Ph: (913) 551-6730
Fax: (913) 551-6541
Email: scott.rask@usdoj.gov
Ks. S. Ct. No. 15643

By: /s/ Adam P. Barry
ADAM P. BARRY
Trial Attorney
National Security Division
U.S. Department of Justice
950 Pennsylvania Avenue, NW
Washington, D.C. 20530
Ph: (202) 233-0788
Fax: (202) 532-4251
Email: adam.barry@usdoj.gov
Cal. Bar No. 294449

IT IS REQUESTED THAT THE TRIAL BE HELD IN KANSAS CITY, KANSAS

PENALTIES

Count 1, Conspiracy

- Punishable by a term of imprisonment of not more than five. 18 U.S.C. § 371.
- A term of supervised release of not more than three years. 18 U.S.C. § 3583(b)(2).
- A fine not to exceed \$250,000. 18 U.S.C. § 3571(b)(3).
- A mandatory special assessment of \$100. 18 U.S.C. § 3013(a)(2)(A).
- Forfeiture.

Counts 2-4, Export Goods to Russia

- Punishable by a term of imprisonment of not more than twenty years. 50 U.S.C. § 4819.
- A term of supervised release of not more than three years. 18 U.S.C. § 3583(b)(2).
- A fine not to exceed \$1,000,000. 50 U.S.C. § 4819.
- A mandatory special assessment of \$100. 18 U.S.C. § 3013(a)(2)(A).
- Forfeiture.

Counts 5-7, False Export Information

- Punishable by a term of imprisonment of not more than five years. 13 U.S.C. § 305 and 15 C.F.R. § 30.71(a).
- A term of supervised release of not more than three years. 18 U.S.C. § 3583(b)(2).

- A fine not to exceed \$10,000 per violation. 13 U.S.C. § 305(a), (f); 18 U.S.C. § 3571(e).
- A mandatory special assessment of \$100. 18 U.S.C. § 3013(a)(2)(A).
- Forfeiture.

Counts 8-13, Smuggling

- Punishable by a term of imprisonment of not more than ten years. 18 U.S.C. § 554.
- A term of supervised release of not more than three years. 18 U.S.C. § 3583(b)(2).
- A fine not to exceed \$250,000. 18 U.S.C. § 3571(b)(3).
- A mandatory special assessment of \$100. 18 U.S.C. § 3013(a)(2)(A).
- Forfeiture.

Approved:


JENNIFER N. ONG/SHIVA LOGARAJAH
Assistant United States Attorneys

Before: THE HONORABLE JUDITH C. McCARTHY
United States Magistrate Judge
Southern District of New York

UNITED STATES OF AMERICA

v.

MAXIM MARCHENKO,

Defendant.

23mj6181

SEALED COMPLAINT

Violations of 18 U.S.C. §§ 371, 554,
1343, 1349, and 1956

COUNTY OF OFFENSE:
DUTCHESS

SOUTHERN DISTRICT OF NEW YORK, ss.:

JASON WAKE, being duly sworn, deposes and says that he is a Special Agent with the Federal Bureau of Investigation (“FBI”), and charges as follows:

COUNT ONE

(Conspiracy to Defraud the United States)

1. From at least in or about May 2022, up to and including in or about August 2023, in the Southern District of New York and elsewhere, MAXIM MARCHENKO, the defendant, and others known and unknown, knowingly and intentionally combined, conspired, confederated, and agreed together and with each other to defraud the United States and agencies thereof, by impairing, impeding, obstructing, and defeating, through deceitful and dishonest means, the lawful functions of the U.S. Census Bureau, U.S. Department of Commerce, and U.S. Customs and Border Patrol, agencies of the United States, in the enforcement of export control laws.

2. In furtherance of the conspiracy and to effect the illegal object thereof, MAXIM MARCHENKO, the defendant, and others known and unknown, committed the overt acts set forth in paragraphs 15 through 25 of this Complaint, among others.

(Title 18, United States Code, Section 371.)

COUNT TWO

(Conspiracy to Commit Money Laundering)

3. From at least in or about May 2022, up to and including in or about August 2023, in the Southern District of New York and elsewhere, MAXIM MARCHENKO, the defendant, and others known and unknown, knowingly and intentionally combined, conspired, confederated, and

agreed together and with each other to commit money laundering in violation of Title 18, United States Code, Section 1956(a)(2)(A).

4. It was part and an object of the conspiracy that MAXIM MARCHENKO, the defendant, and others known and unknown, would and did transport, transmit, and transfer, and attempt to transport, transmit, and transfer, a monetary instrument and funds to a place in the United States from and through a place outside the United States, with the intent to promote the carrying on of specified unlawful activity, to wit, (a) smuggling goods from the United States, in violation of Title 18, United States Code, Section 554, and (b) wire fraud, in violation of Title 18, United States Code, Section 1343.

(Title 18, United States Code, Section 1956(h).)

COUNT THREE
(Conspiracy to Smuggle Goods from the United States)

5. From at least in or about May 2022, up to and including in or about August 2023, in the Southern District of New York and elsewhere, MAXIM MARCHENKO, the defendant, and others known and unknown, knowingly and intentionally combined, conspired, confederated, and agreed together and with each other to commit an offense against the United States, to wit, smuggling goods from the United States, in violation of Title 18, United States Code, Section 554.

6. It was a part and an object of the conspiracy that MAXIM MARCHENKO, the defendant, and others known and unknown, would and did fraudulently and knowingly export and send from the United States, attempt to export and send from the United States, and cause to be exported and sent from the United States, merchandise, articles, and objects, contrary to laws and regulations of the United States, to wit, MARCHENKO unlawfully caused and attempted to cause companies in the United States to export OLED micro-displays subject to the Export Administration Regulations (“EAR”), Title 15, Code of Federal Regulations, Parts 730-774, from the United States to the Russian Federation (“Russia”), contrary to Title 50, United States Code, Section 4819(a)(2)(F).

7. In furtherance of the conspiracy and to effect the illegal objects thereof, MAXIM MARCHENKO, the defendant, and others known and unknown, committed the overt acts set forth in paragraphs 15 through 25 of this Complaint, among others.

(Title 18, United States Code, Section 371.)

COUNT FOUR
(Promotional Money Laundering)

8. From at least in or about May 2022, up to and including in or about August 2023, in the Southern District of New York and elsewhere, MAXIM MARCHENKO, the defendant, and others known and unknown, transported, transmitted, and transferred, and attempted to transport, transmit, and transfer, a monetary instrument and funds to a place in the United States from and through a place outside the United States, with the intent to promote the carrying on of specified unlawful activity, to wit, (a) smuggling goods from the United States, in violation of Title 18,

United States Code, Section 554, and (b) wire fraud, in violation of Title 18, United States Code, Section 1343.

(Title 18, United States Code, Section 1956(a)(2)(A) and 2.)

COUNT FIVE
(Smuggling Goods from the United States)

9. From at least in or about May 2022, up to and including in or about August 2023, in the Southern District of New York and elsewhere, MAXIM MARCHENKO, the defendant, and others known and unknown, fraudulently and knowingly exported and sent from the United States, attempted to export and send from the United States, and caused to be exported and sent from the United States, merchandise, articles, and objects, contrary to laws and regulations of the United States, to wit, MARCHENKO unlawfully caused companies in the United States to export OLED micro-displays subject to the EAR, Title 15, Code of Federal Regulations, Parts 730–744, from the United States to Russia, contrary to Title 50, United States Code, Section 4819(a)(2)(F).

(Title 18, United States Code, Sections 554(a) and 2.)

COUNT SIX
(Conspiracy to Commit Wire Fraud)

10. From at least in or about May 2022, up to and including in or about November 2022, in the Southern District of New York and elsewhere, MAXIM MARCHENKO, the defendant, and others known and unknown, knowingly and willfully combined, conspired, confederated, and agreed together and with each other to commit wire fraud in violation of Title 18, United States Code, Section 1343.

11. It was part and an object of the conspiracy that MAXIM MARCHENKO, the defendant, and others known and unknown, knowingly having devised and intending to devise a scheme and artifice to defraud, and for obtaining money and property by means of false and fraudulent pretenses, representations, and promises, would and did transmit and cause to be transmitted by means of wire, radio, and television communication in interstate and foreign commerce, writings, signs, signals, pictures, and sounds for the purpose of executing such scheme and artifice, in violation of Title 18, United States Code, Section 1343, to wit, MARCHENKO and others known and unknown agreed to make and cause false statements to be made to a U.S. company in order to fraudulently obtain OLED micro-displays, and to send and receive, and to cause others to send and receive, emails and other electronic communications to and from the Southern District of New York and elsewhere in furtherance of that scheme.

(Title 18, United States Code, Section 1349.)

COUNT SEVEN
(Wire Fraud)

12. From at least in or about May 2022, up to and including in or about November 2022, in the Southern District of New York and elsewhere, MAXIM MARCHENKO, the defendant, knowingly having devised and intending to devise a scheme and artifice to defraud, and

for obtaining money and property by means of false and fraudulent pretenses, representations, and promises, transmitted and caused to be transmitted by means of wire, radio, and television communication in interstate and foreign commerce, writings, signs, signals, pictures, and sounds, for the purpose of executing such scheme and artifice, to wit, MARCHENKO engaged in a scheme to make and cause false statements to be made to a U.S. company in order to fraudulently obtain OLED micro-displays, and sent and received, and caused others to send and receive, emails and other electronic communications to and from the Southern District of New York and elsewhere, in furtherance of that scheme.

(Title 18, United States Code, Sections 1343 and 2.)

The bases for my knowledge and for the foregoing charges are, in part, as follows:

13. I have been an FBI Special Agent since in or about August 2014. I am currently assigned to the Counterintelligence Division of the FBI's New York Field Office, which focuses on cases involving, among other things, sanctions evasion, export control violations, counter-proliferation, wire fraud, bank fraud, and money laundering. During my time as an FBI Special Agent, I have become familiar with some of the ways in which criminal actors avoid export controls, evade sanctions, and smuggle goods and technology from the United States, and I have participated in numerous investigations involving sanctions evasion, export control violations, and smuggling.

14. This affidavit is based upon my participation in the investigation of this matter, including my conversations with law enforcement agents and other individuals, my review of law enforcement reports and records, and my review of business records, phone records, email communications, text messages, and draft summaries and translations of such documents, communications, and messages. Because this affidavit is being submitted for the limited purpose of establishing probable cause, it does not include all the facts that I have learned during the course of my investigation. Where the contents of documents and the actions, statements, and conversations of others are reported herein, they are reported in substance and in part, except where otherwise indicated. Where figures, calculations, and dates are set forth herein, they are approximate, unless stated otherwise.

Overview

15. Based on my participation in this investigation, including my conversations with other law enforcement agents and other individuals, my review of law enforcement reports and records, and my review of business records, shipping records, email communications and messages obtained pursuant to judicially authorized search warrants, and draft summaries and translations of such documents and communications, I have learned the following, in substance and in part:

a. As set forth in greater detail below, the FBI and the Bureau of Industry and Security ("BIS") of the U.S. Department of Commerce ("Department of Commerce") have been investigating an illicit procurement network responsible for smuggling sensitive U.S. technologies out of the United States to Russia (the "Procurement Network").

b. MAXIM MARCHENKO, the defendant, and two co-conspirators ("CC-1" and "CC-2"), are Russian nationals who have held primary roles in operating the Procurement

Network. As set forth in greater detail below, one of the main goals of the Procurement Network is to fraudulently obtain large quantities of dual-use, military grade micro-electronics, specifically dual-use OLED micro-displays manufactured by a particular American company based in Dutchess County, New York (“Company-1,” and the “Micro-Displays”)¹, for shipment to Russia. The Micro-Displays that the Procurement Network have smuggled to Russia have civilian applications, such as medical and veterinary imaging, digital cameras, and video games, and military applications, such as rifle scopes, night-vision goggles, thermal optics, and other weapon systems.

c. As described in more detail below, MARCHENKO’s primary role in the Procurement Network is and was to maintain front companies based in Hong Kong. The Procurement Network used MARCHENKO’s front companies to send payments to U.S. distributors, such as Company-1, in an effort to conceal the source of the funds (*i.e.*, Russia). Additionally, the Procurement Network used MARCHENKO’s front companies as transshipment points between the U.S. distributors, such as Company-1, and the end users in Russia. At times, MARCHENKO, acting on behalf of the Procurement Network, also communicated directly with U.S. distributors on behalf of his front companies.

d. Since Russia’s invasion of Ukraine in February 2022, and the tightening of U.S. export controls, the Procurement Network has operated with a cover story to conceal the fact—from U.S. Government agencies and Company-1—that the Micro-Displays are and were going to Russia. As part of the cover story, members of the Procurement Network falsely stated to U.S. distributors, *e.g.*, Company-1, that the Micro-Displays were not going to Russia, but instead going to the People’s Republic of China and other countries for scientific research, knowing that U.S. distributors like Company-1 were required to provide end user information to government agencies, such as the U.S. Census Bureau (“Census Bureau”), Department of Commerce, and U.S. Customs and Border Patrol (“CBP”).

e. To further bolster their cover story, members of the Procurement Network, including MARCHENKO, arranged for transshipment points to front companies outside of Russia. To arrange shipments to these various transshipment points, including in Hong Kong, the Procurement Network utilized the services of a Hong Kong-based freight forwarding company (the “Freight Forwarder”), which is known to provide freight forwarding services to Russia.

f. The Procurement Network has also used front companies in Hong Kong, operated principally by MARCHENKO, to conceal the fact that payment for the Micro-Displays comes from Russia. In total, between in or about May 2022 and in or about August 2023, MARCHENKO’s front companies have funneled a total of more than \$1.6 million to the United States in support of the Procurement Network’s efforts to smuggle the Micro-Displays to Russia.

¹ These Micro-Displays are subject to the Export Administration Regulations (“EAR”) and are classified as EAR99. The EAR regulate the export of “dual use” items — items that have both a commercial application and a military or strategic use — which could contribute to the military potential of other nations or be detrimental to United States foreign policy or national security. *See* 15 C.F.R. § 730.3.

g. Finally, over the course of their operations, members of the Procurement Network sent messages amongst themselves about evading U.S. Government scrutiny, and the need to “support the legend [cover story] that . . . we know nothing about Russia.”

The Defendant, CC-1, CC-2, and Relevant Entities

16. Based on my participation in this investigation, including my conversations with other law enforcement agents and other individuals; my review of open-source materials; my review of a November 2022 nonimmigration visa application submitted by MAXIM MARCHENKO (the “MARCHENKO Visa Application”), the defendant, to the United States Citizenship and Immigration Services; my review of business records, email communications and messages obtained pursuant to judicially authorized search warrants; and draft summaries and translations of such documents and communications, I have learned the following, in substance and in part:

a. MARCHENKO is a Russian national who resides in Hong Kong. MARCHENKO operates Alice Components Co. Ltd. (“Alice Components”), a Hong Kong-based company, and is the business owner/director of Neway Technologies Limited (“Neway”). Neway is a Hong Kong-based company that is located at an address on Castle Peak Road in Hong Kong (the “Castle Peak Address”). MARCHENKO also operates RG Solutions Limited (“RG Solutions”), which is located at the Castle Peak Address.

b. MARCHENKO listed a phone number ending in 1175 (the “1175 Number”) and a particular email address (“Email Address-1”) on the MARCHENKO Visa Application. MARCHENKO uses both the 1175 Number and Email Address-1 to communicate with CC-1.

c. CC-1 is a Russian national who works for Infotechnika, a Russia-based electronics seller. Between at least in or about April 2019 and at least in or about January 2023, Infotechnika used the Freight Forwarder to ship goods to Russia. Infotechnika also shared the same physical address as NPO Electronic Systems, a Russian electronics reseller. In or about March 2022, following the Russian invasion of Ukraine, the BIS imposed further sanctions against Russia by the addition of entities to the Entity List, including NPO Electronic Systems, for having been involved in, contributed to, or otherwise supported the Russian security services, military and defense sectors, and military and/or defense research and development efforts.² Additionally, Infotechnika shares an IP address and phone number with OOO NPTC Topaz, a/k/a “NPC Topaz,” another Russia-based company.

d. As part of the cover story engineered by the Procurement Network, CC-1 has masqueraded as an employee for SSP LTD, a Hong Kong-based company located at the Castle Peak Address where some of MARCHENKO’s other front companies operate, as described above, and as “Amy Chan”—a purported purchase manager for Alice Components, another one of

² The Department of Commerce’s Entity List identifies entities for which there is reasonable cause to believe the entities have been involved, are involved, or pose a significant risk of being or becoming involved in activities contrary to the national security or foreign policy interests of the United States. *See* 15 C.F.R. § 744 Supp. No. 4. A license is required to export any item regulated under the EAR to an entity on the Entity List. *See* 15 C.F.R. §§ 744.11, 744.16.

MARCHENKO's front companies. I believe that CC-1 and "Amy Chan" are one and the same for the reasons described *infra* in paragraph 22(c).

e. As part of the Procurement Network's efforts, CC-1 communicates with U.S. distributors, masquerades as "Amy Chan," and works with MARCHENKO and CC-2 to smuggle the Micro-Displays from the United States through Hong Kong to Russia. CC-1 uses a phone number ending in 7407 (the "7407 Number") to communicate with MARCHENKO at the 1175 Number. CC-1 also emails, using an Infotechnika email account, MARCHENKO at Email Address-1.

f. CC-2 is a Russian national who is a director at NPC Topaz and the supervisor of CC-1. Additionally, CC-2 is a 25% shareholder of NPC Granat, a Russian company in the electronics production industry. NPC Granat was placed on the Entity List by the Department of Commerce in or about September 2016 because NPC Granat was identified as operating in Russia's arms or related material sector. *See* Exec. Order 13661; 81 Fed. Reg. 61595. As part of the Procurement Network with MARCHENKO and CC-1, CC-2 arranges for payments from Russian companies to MARCHENKO's Hong Kong-based front companies. MARCHENKO then passes along those payments to companies in the United States for, among other things, the Micro-Displays.

Background on Applicable Export Regulations and Laws

17. Based on my training and experience, review of open-source materials, and conversations with other law enforcement agents and individuals, I have learned the following:

a. An exporter generally must file an Electronic Export Information ("EEI") with the Census Bureau when the value of a commodity being exported classified under each individual Schedule-B³ number is over \$2,500 or if a validated export license is required to export the commodity (regardless of value). 15 C.F.R. § 758.1(b). An EEI "is a statement to the United States Government that the transaction occurred as described" and includes "basic information such as the names and addresses of the parties to a transaction." 15 C.F.R. § 758.1(a).

b. An EEI can be filed by the U.S. Principal Party in Interest ("USPPI") (*e.g.*, the exporter), an authorized agent of the USPPI (*e.g.*, a freight forwarder), or the Foreign Principal Party in Interest ("FPPI") (*e.g.*, the ultimate consignee).

c. Typically, the carrier also files the EEI with the CBP.

d. Among other things, the EEI lists the country of the intended destination for goods being shipped outside the United States, the ultimate consignee's name and address, the intermediate consignee's name and address, and a description of the commodities to be exported.

³ Schedule-B is a U.S.-specific classification code for exporting goods from the United States. It is administered by the Census Bureau's Foreign Trade Division, which keeps records of exports by country as well as the quantity and value in U.S. dollars. The Schedule-B is built upon the first 6-digits of the international Harmonized System (HS) code, which is administered by the World Customs Organization, and an additional 4-digits for statistical analysis.

e. The EEI is used by the Census Bureau to collect trade statistics and by the BIS of the Department of Commerce for export control purposes.

f. As detailed below, the Procurement Network has ordered and caused shipments of Micro-Displays to be exported. At all relevant times the shipments of Micro-Displays were classified under Schedule-B and valued at more than \$2,500 and thus required an EEI for export.

g. Section 4819(a)(1), Title 50, United States Code, provides, in relevant part, that it is “unlawful for a person to violate, attempt to violate, conspire to violate, or cause a violation of . . . any of the unlawful acts described in paragraph (2).”

h. Section 4819(a)(2)(F), Title 50, United States Code, in turn, provides, in relevant part, that “[n]o person may make any false or misleading representation, statement, or certification, or falsify or conceal any material fact, either directly to the Department of Commerce, or an official of any other United States agency. . . or indirectly through any other person . . . in connection with the preparation, submission, issuance, use, or maintenance of any export control document or any report filed or required to be filed pursuant to the Export Administration Regulations . . . [or] for the purpose of or in connection with effecting any export, reexport, or in-country transfer of an item subject to the Export Administration Regulations.”

Background on the Flow of U.S.-Sourced Electronics to Russia

18. Based on my training and experience, review of open-source materials, conversations with other law enforcement agents and individuals, and review of and email communications and messages obtained pursuant to judicially authorized search warrants, and draft translations and summaries of these communications and messages, I have learned the following

a. Russia is highly dependent on Western-sourced micro-electronics for its military’s hardware, including components manufactured or sold in the United States. Russia relies on third-party transshipment hubs and clandestine procurement and payment networks, such as the Procurement Network, to secure access to such U.S.-sourced electronics.

b. Russia’s weapons systems and military platforms—including rocket systems, drones, ballistic missiles, tactical radios, and electronic warfare devices—contain a range of predominantly Western-sourced components and micro-electronics that are critical to their functions.

c. On or about December 16, 2022, MAXIM MARCHENKO, the defendant, sent CC-2 the link to an article titled, “The supply chain that keeps tech flowing to Russia.”⁴ Based on my review of the article, I know that the article discusses how, despite U.S. export restrictions against Russia, especially recent restrictions on sensitive technology following Russia’s invasion of Ukraine, the global supply chain continues to feed Russia with Western computer components and other electronics by shipping them through other locations like Hong Kong. As described in

⁴ <https://www.reuters.com/investigates/special-report/ukraine-crisis-russia-tech-middlemen/>.

more detail below, I have learned that MARCHENKO shared this article during the course of the Procurement Network's operations.

The Procurement Network's Operations Prior to February 2022

19. Based on my training, experience, conversations with other law enforcement agents and individuals, review of records and email communications maintained by Company-1, and review of open-source materials, I have learned the following, in substance and in part:

a. In or about October 2014, Radiofid Systems ("Radiofid"), a Russia-based company, became a customer of Company-1, which is based in Dutchess County, New York. Prior to purchasing the Micro-Displays, Radiofid submitted a presale questionnaire to Company-1 stating that the Micro-Displays were to be used in rescue kits for Emercom Russia—a Russian state-owned civil defense organization. Radiofid also submitted an additional presale questionnaire in or about February 2016 and indicated that the Micro-Displays would be incorporated into the same end product for the same end use for the same end country—*i.e.*, Emercom in Russia. The email address listed on the questionnaire is the same email address as the one provided on a 2016 nonimmigrant visa application by a computer scientist at NPC Granat.

b. Between in or about November 2017 and in or about June 2021, Radiofid ordered from Company-1 a total of approximately 868 Micro-Displays, identified with a specific Company-1 part number ("Part Number-1"). At least some of these orders Micro-Displays were shipped in multiple shipments to Radiofid to the attention of "Maxim" at the Castle Peak Address. The 1175 Number was listed as the phone number for "Maxim."

c. Between in or about November 2017 and in or about July 2021, Radiofid ordered from Company-1 a total of approximately 4,350 Micro-Displays, identified with a specific Company-1 part number ("Part Number-2"). At least some of these orders Micro-Displays were shipped in multiple shipments to Radiofid to the attention of "Maxim" at the Castle Peak Address. The 1175 Number was listed as the phone number for "Maxim."

d. In internal records, Company-1 categorized Radiofid's 2020 and 2021 orders of the Micro-Displays as "Military."

e. In or about October 2021 and in or about December 2021, Neway—one of the Hong Kong-based front companies associated with MAXIM MARCHENKO, the defendant—wired a total of approximately \$136,630 to Company-1 for some of Radiofid's prior orders.

f. Because the items identified by Part Number-1 and Part Number-2 listed above were shipped to a "Maxim"—a reference to the defendant's first name—at an address and phone number associated with MARCHENKO, and because payment was remitted by MARCHENKO's front company, Neway, I believe that at least some of the Radiofid orders of Micro-Displays from Company-1 were shipped to and paid for by MARCHENKO on behalf of organizations and end users in Russia, *i.e.*, Radiofid and Emercom.

20. Based on my review of draft translations of messages sent or received by MAXIM MARCHENKO, the defendant, I have learned that during the time period of the Radiofid orders MARCHENKO exchanged several messages with CC-1 and CC-2 that referenced Company-1,

Part Number-1, Part Number-2, payment to Company-1, and tracking information for packages shipped by Company-1 from Dutchess County, New York. For example:

a. In or about December 2018, MARCHENKO informed CC-2 that Company-1 had received the payment. A few weeks later, CC-2 sent MARCHENKO the following message: “[Part Number-2] 1100pcs.” In or about November 2020, CC-2 sent MARCHENKO a message and referenced 65 Micro-Displays from Company-1.

b. On or about June 16, 2021, CC-1 sent MARCHENKO the following message: “Hi! [Company-1] has shipped us, I don’t have any documents yet but I have a track - 1ZV671740455295558.” Based on my training, experience, participation in this investigation, and the fact that the message references shipping and “track,” I believe that the alphanumeric number provided is a tracking number for a Company-1 shipment.

c. On or about December 6, 2021, MARCHENKO sent the following message to CC-1, which appears to be a message that MARCHENKO received from the vice president of a foreign bank: “Dear Maxim, Since the word ‘ELECTRONIC COMPONENTS’ was an entity hit the sanctions, going forward please avoid using it. You can use the short form ‘Elect Comp’ instead.” Based on my training, experience, and participation in this investigation, I believe the bank employee is advising MARCHENKO how to avoid sanctions. Two days later, MARCHENKO told CC-1: “This is [Company-1].”

d. On or about December 24, 2021, CC-1 sent MARCHENKO an invoice from Company-1 to Radiofid for the purchase of 650 Micro-Displays with Part Number-1. Approximately one hour later, MARCHENKO sent CC-1 confirmation that Neway wire transferred approximately \$122,955 to Company-1.

e. Based on the above messages between MARCHENKO, CC-1, and CC-2, including the references to Company-1, the inclusion of Company-1 invoices to Radiofid, and the inclusion of tracking information for a Company-1 shipment, I believe that the Procurement Network, specifically, MARCHENKO, CC-1, and CC-2, ordered Micro-Displays from Company-1 prior to in or about February 2022 on behalf of organizations and end users in Russia, *i.e.*, Radiofid and Emercom.

Company-1’s February 2022 Decision to Cease Business with Russian Entities

21. Based on my review of Company-1’s records and communications and my conversations with other law enforcement agents and individuals, I have learned, in substance and in part, the following:

a. In or about February 2022, an executive at Company-1 sent an internal email to other employees notifying them that Company-1 and its board had decided not to sell their products to Russian customers or to customers who ship their products to Russia. The executive explained:

Probably more than obvious at this time, but the Company and Board have decided it is no longer right for us to sell or ship to Russian customers and risk that our displays will be used in devices

that could put US or NATO forces in harm's way, or support Russia's unlawful invasion of Ukraine and its human rights abuse.

b. In or about May 2022, a Company-1 employee responded to an email from a Radiofid representative. In substance and in part, the Company-1 employee explained that business between the United States and Russia was on hold and, Company-1 needed to wait for the situation to resolve before it shipped their micro-displays again to Russia.

The Procurement Network Employs a Cover Story to Illicitly Gain Access to the Micro-Displays

22. Based on my training, experience, conversations with other law enforcement agents and individuals, review of records and email communications maintained by Company-1, review of open-source materials, bank records, and email communications and messages obtained pursuant to judicially authorized search warrants, and draft summaries and translations of such documents and communications, I have learned the following, in substance and in part:

a. Alice Components became a new customer of Company-1 shortly after Company-1 decided it would no longer fulfill orders to Russian customers or customers who shipped their goods to Russia. As described further below, members of the Procurement Network—specifically, MAXIM MARCHENKO, the defendant, CC-1, and CC-2—were involved with Alice Components orders, just as they were with Radiofid. Thus, I believe the Procurement Network shifted to using Alice Components in an attempt to obtain the Micro-Displays because Company-1 would no longer do business with Radiofid—a Russian entity.

b. On or about March 24, 2022, “Amy” from Alice Components submitted a pre-sale questionnaire to Company-1 prior to purchasing the Micro-Displays. In the questionnaire, “Amy” stated that Alice Components was a wholesale distributor of electronic components and a contract manufacturer. Additionally, “Amy” stated that the Micro-Displays would be incorporated into “electron microscopes” for “medical research” and the end-user countries were listed as “China, Hong Kong, Malaysia, [and] Europe.” Alice Components expected to purchase 3,000 to 5,000 Micro-Displays annually. “Amy Chan” signed the questionnaire as the purchase manager of Alice Components and certified that all of the facts in the questionnaire were true and that the Micro-Displays would not be used “for any purpose or [sent] to any end user contrary to the representations made.”

c. Based on my review of subpoena returns and pen register information from an Internet Service Provider, I have learned that “Amy Chan” (who sometimes goes by “Amy”) from Alice Components uses an email address with the same IP address as the phone using the 7407 Number, which is associated with CC-1. Additionally, based on my review of contact information contained in a cloud-based account belonging to MARCHENKO, I have learned that he saved the 7407 Number in the name of CC-1 at Infotechnika. Finally, after “Amy Chan” began interacting with an undercover FBI agent, I know that the 7407 Number—used by CC-1—was often times almost immediately in touch with MARCHENKO. For these reasons, I believe that “Amy Chan” is a fictitious online persona that CC-1 used to help illicitly procure the Micro-Displays.

June 2022: Alice Components Orders 500 Micro-Displays from Company-1

d. In or about June 2022, Alice Components ordered 500 Micro-Displays with Part Number-2 from Company-1 for approximately \$292,050 (the “June Order”). The invoice listed Alice Components as the entity to be billed and the Freight Forwarder as the entity that the displays should be shipped to. Company-1 shipped the June Order from Dutchess County, New York to the Freight Forwarder in two shipments on or about June 30, 2022, and on or about August 4, 2022. As described further below, MARCHENKO used one of his Hong Kong front companies (RG Solutions) to mask the fact that payment for the June Order originated in Russia.

e. As set forth above, *see supra* ¶ 17(a), an EEI is a mandatory declaration filed with the Census Bureau, CBP, and Department of Commerce, among other agencies, for all shipments outside of the United States valued over \$2,500. Among other things, the EEI lists the country of the intended destination for goods being shipped outside the United States. Based on the information provided to Company-1, *see supra* ¶ 22(d), both EEIs for the June Order (one for the June 30, 2022 shipment and the other for the August 4, 2022 shipment) listed the destination for the shipment as Hong Kong and the ultimate consignee as the Freight Forwarder, also in Hong Kong.

f. As set forth in more detail, *see infra* ¶¶ 22(g) – (J), in or about June 2022 (*i.e.*, when the June Order was placed), MARCHENKO received a contract for RG Solutions to sell electronic components to MEC LLC (a Russian company); RG Solutions then received a total of approximately \$292,000 (*i.e.*, the cost of the June Order) from NPC Topaz and that wire transfer referenced the contract between RG Solutions and MEC LLC; and RG Solutions then wired approximately \$183,000 to Company-1. In addition, MARCHENKO sent multiple invoices to CC-1 (at Infotechnika) from both RG Solutions and SSP LTD that billed either NPC Topaz or MEC LLC for Micro-Displays. Based on this sequence of events, I believe that the Procurement Network placed the June Order on behalf of a Russian end user.

g. Around the time that Alice Components placed the June Order, MARCHENKO received a contract from a Russian company for the sale of electronic components. Specifically, on or about June 15, 2022, CC-1 emailed a contract (in Russian and English) to MARCHENKO. The contract was for RG Solutions, represented by MARCHENKO, to sell “electronic components” to MEC LLC, a Russia-based company. The contract was to be paid out in U.S. dollars and was to be effective until December 29, 2025. The contract contained the following reference number: “№ RU/30580500/00055.”

h. MARCHENKO continued to send invoices to CC-1 for the Micro-Displays. Based on my training, experience, and involvement in this investigation, I have learned that banks often require customers to provide additional documentation to explain large transfers of money into or out of an account. Accordingly, I believe these invoices were designed to provide assurance to inquiring banks for the large money transfers between MARCHENKO’s Hong Kong front companies and the Russian end users for the products. As an example, on or about June 20, 2022, MARCHENKO sent CC-1 at Infotechnika an invoice from RG Solutions. The invoice billed NPC Topaz for 150 pieces of Part Number-2—a version of the Micro-Displays—which was to be shipped to NPC Topaz at an address located in Russia. As another example, between in or about June 2022 and in or about November 2022, MARCHENKO sent CC-1 at Infotechnika five invoices from SSP LTD (one of MARCHENKO’s Hong Kong-based front companies) or RG

Solutions to MEC LLC for a total of approximately 959 Micro-Displays, identified with Part Number-2, for approximately \$1.9 million.

i. Following the June Order, MARCHENKO received several messages from CC-1 and CC-2 that referenced the June Order. For example, on or about June 20, 2022, CC-2 messaged MARCHENKO: “Hi. Today I sent you 58 (your [sic] orders) and 292 (to [sic] pay for displays with RG), I think the bank will pay for the week.” Based on my training, experience, and participation in this investigation, I believe “292” is a reference to the approximately \$292,050 that Alice Components owed Company-1 for the June Order. As another example, a few days later, CC-1 emailed MARCHENKO an invoice from Company-1 to Alice Components for the June Order and asked that MARCHENKO pay the invoice. CC-1 also told MARCHENKO: “Be sure to pay from RG Solutions Limited.”

j. Shortly thereafter, on or about June 23 and 27, 2022, RG Solutions received two wire transfers totaling \$292,000 (each wire was for \$146,000) from OOO NPTC TOPAZ, where CC-2 is a director. The wire transfers listed a Russian address for OOO NPTC TOPAZ. The wire transfers both contained the following text: “PAYMENT UNDER THE CONTRACT RU/30580500/00045 OF 20.05.2022,PROFORMA INVOICE RG 201706128 OF 20.06.2022 CONSUMER GOODS.” Based on my participation in this investigation, I know that the contract reference number in this wire transfer information is nearly identical (but for one digit) to the reference number for the contract between RG Solutions and MEC LLC described in paragraph 22(g) above. On or about June 28, 2022, CC-1 messaged MARCHENKO to confirm that funds had been sent to him to pay Company-1: “The money to pay for [Company-1] has gone from us.”

k. On or about June 29 and 30, 2022, Company-1 received two wire transfers to its U.S. bank account from RG Solutions, located in Hong Kong, for a total of approximately \$183,000. On those days, MARCHENKO sent CC-1 wire transfer confirmations of payments from RG Solutions to Company-1. Based on this sequence of events, and my involvement in this investigation, I believe the money to pay for the Micro-Displays, which were falsely represented as not going to Russia, were paid for by CC-1 and CC-2 from Russia.

August 2022: Alice Components Attempts to Order 2,000 More Micro-Displays from Company-1

l. On or about July 1, 2022, CC-1 (posing as Amy) requested on behalf of Alice Components that an account manager at Company-1 (the “Account Manager”) provide a quote for 2,000 Micro-Displays. The Account Manager asked CC-1: “Please confirm this does not include Russia or Ukraine for end country.” CC-1 replied: “I confirm that this does not include Russia or Ukraine for end country.”

m. On or about August 26, 2022, Company-1 issued an invoice to Alice Components for an order of 2,000 Micro-Displays with Part Number-2 for a total of \$1,038,400 (the “August Order”). The August Order was to be shipped to the Freight Forwarder. CC-1 later forwarded this invoice to MARCHENKO and, in substance and in part, asked that he pay the invoice from RG Solutions.

n. In or about September 2022, CC-1 sent MARCHENKO the following messages about the August Order:

CC-1: Can you pay us [Company-1] with RG solution ?
[sic]

CC-1: Hi! On [Company-1] how to start paying - very waiting for payment . It is obligatory from rg solution to send them . [sic]

o. Alice Components and CC-1 continued to falsely represent to Company-1 that the end users of the Micro-Displays were not in Russia. For example, on or about September 12, 2022, CC-1 re-submitted a presales questionnaire for Alice Components to Company-1 to provide information regarding the ultimate consignee, which was listed as the National Health Commission of the People's Republic of China. The questionnaire provided the same ultimate production application information as the March 2022 questionnaire—*i.e.*, that the Micro-Displays were to be incorporated into electron microscopes for medical research and the end-user countries were China, Hong Kong, Malaysia, and Europe. As another example, in or about September 2022, CC-1 and the Account Manager exchanged emails regarding how Alice Components planned to use the Micro-Displays. In substance and in part, CC-1 explained how the micro-displays would be used in the microscope and confirmed that Alice Components would be performing the assembly of the eyepiece board that contained the micro-displays.

p. On or about September 27 and 28, 2022, RG Solutions, located in Hong Kong, wired a total of approximately \$180,000 to Company-1's bank account in the United States as a deposit for the August Order.

q. On or about November 2, 2022, a Company-1 executive, at the direction of law enforcement, informed CC-1 that Company-1 would not be able to fulfill Alice Components's order for 2,000 Micro-Displays for compliance-related reasons. The executive stated that Company-1 would return the advance payment it had received and then referred Alice Components to an undercover company (the "UC Company")⁵, which it described as a distributor of Company-1's Micro-Displays. In response, CC-1 asked Company-1 to return the prior payment to an account in the name of RG Solutions.

The Procurement Network Continues Its Efforts to Obtain the Micro-Displays Using Misrepresentations

23. Based on my training, experience, and conversations with other law enforcement agents and individuals, review of records and email communications maintained by Company-1, review of open-source materials, bank records, and email communications and messages obtained pursuant to judicially authorized search warrants, and draft summaries and translations of such documents and communications, I have learned the following, in substance and in part:

⁵ An undercover company is a business or company that an undercover agent purports to exist and operate when in fact that business does not actually exist and is part of a law enforcement operation.

a. On or about November 2, 2022, CC-1 (posing as “Amy Chan”) emailed an undercover FBI agent (the “UC”), who was posing as an employee of the UC Company. In the email, CC-1 expressed an interest in purchasing 2,500 pieces of Part Number-2 (a version of the Micro-Displays), noting that Alice Components previously purchased the parts directly from Company-1. Approximately one week later, CC-1 emailed the UC and stated that the Micro-Displays would be used in electron microscopes for medical research. Additionally, CC-1 stated that the end user would be the National Health Commission of the People’s Republic of China.

Alice Components Purchases 50 Micro-Displays from the UC Company

b. On or about November 15, 2022, CC-1 emailed a purchase order form to the UC for 50 Micro-Displays, with Part Number-2 from Company-1, for \$32,500. CC-1 agreed that Alice Components would purchase 2,450 Micro-Displays in the future. A few days later, CC-1 emailed MAXIM MARCHENKO, the defendant, and attached an invoice from the UC Company to Alice Components for 50 Micro-Displays from Company-1 with Part Number-2. The invoice was for approximately \$33,600. CC-1 advised that “it’s better to pay from RG Solution (you definitely can’t from Neway).” CC-1 also attached the bank account information for the UC Company. Based on my training, experience, and involvement in this investigation, I believe CC-1 was telling MARCHENKO not to use “Neway” because Neway was the entity MARCHENKO used to pay for Russia-based Radiofid purchases from Company-1. In other words, CC-1 was warning MARCHENKO not to use “Neway” to maintain the cover that the Micro-Displays would not be going to Russia.

c. On or about November 23, 2022, the UC Company received a wire transfer to its U.S. bank account for approximately \$33,600 from Namfleg Limited (“Namfleg”), a Hong Kong jewelry retailer at the Castle Peak Address. The Namfleg website lists Neway—with the Castle Peak Address, which is shared by many of MARCHENKO’s other front companies—as a point of contact. Thus, because Neway is listed as a point of contact and because MARCHENKO remitted payment from Namfleg after being requested to by CC-1, I believe Namfleg is another of MARCHENKO’s Hong Kong front companies.

d. On or about November 28, 2022, CC-1 (posing as “Amy Chan”) emailed the UC that the 50 Micro-Displays could be sent to the Freight Forwarder if the UC Company had trouble shipping to the originally provided address.

e. On or about November 30, 2022, the UC Company shipped the 50 Micro-Displays to the Freight Forwarder (“Shipment-1”). The UC then emailed the tracking number to CC-1 for Shipment-1. Shortly thereafter, an IP address connected to NPC Granat—the Russia-based electronics company associated with CC-2, *see supra* ¶ 16(f)—checked the tracking information for Shipment-1. Over the next approximately three days, multiple IP address connected to NPC Granat checked the tracking information for Shipment-1. I believe this indicates that Alice Components was purchasing Micro-Displays, and MARCHENKO was paying for such Micro-Displays, for provision to a company in Russia, and not the National Health Commission of the People’s Republic of China.

Alice Components Orders 2,450 More Micro-Displays from the UC Company

f. On or about December 1, 2022, the UC sent CC-1 an invoice from the UC Company for 2,450 of Company-1’s Micro-Displays, referencing Part Number-2. The displays were to be shipped to the Freight Forwarder for a total of approximately \$1,594,000. CC-1 later forwarded this invoice to MARCHENKO. That same day, CC-2 sent the following message to MARCHENKO: “And on Monday, I’ll start sending \$1.6 million to pay [Company-1].” MARCHENKO and CC-2 then began discussing specifically how CC-2 would pay MARCHENKO, with CC-2 asking “[h]ow much can I pay per SSP”—a reference to SSP LTD, one of MARCHENKO’s Hong Kong front companies. MARCHENKO responded: “up to 300k usd,” and CC-2 responded, in part, that he was “going down the beaten path: old bank-small payments.” Based on my training, experience, and involvement in this investigation, I believe CC-2 was telling MARCHENKO that he (CC-2) would pay MARCHENKO for the Micro-Displays from his Russian bank accounts like he had previously. *See supra* ¶ 22(i), (j). Indeed, two weeks later, CC-2 messaged MARCHENKO that he, in fact, had made a payment of “100k.”

g. Between in or about December 2022 and in or about February 2023, Alice Components made fourteen separate wire transfers from the Hong Kong-based accounts of several of MARCHENKO’s front companies—Namfleg, SSP Limited, and RG Solutions—to the UC Company’s bank account located in Manhattan, New York, as displayed below. In total, Alice Components transferred approximately \$1,333,294.85.

Date	Entity Sending Wire	Amount
November 25, 2022	Namfleg	\$33,594.85
December 13, 2022	RG Solutions	\$99,980.00
December 15, 2022	RG Solutions	\$99,980.00
December 19, 2022	RG Solutions	\$99,980.00
December 19, 2022	RG Solutions	\$99,980.00
December 21, 2022	RG Solutions	\$99,980.00
December 21, 2022	RG Solutions	\$99,980.00
December 22, 2022	RG Solutions	\$99,980.00
December 28, 2022	RG Solutions	\$99,980.00
January 27, 2023	SSP Limited	\$99,972.00
January 31, 2023	SSP Limited	\$99,972.00
February 2, 2023	SSP Limited	\$99,972.00
February 3, 2023	SSP Limited	\$99,972.00
February 8, 2023	SSP Limited	\$99,972.00
	Total:	\$1,333,294.85

h. In addition to attempting to conceal the true source of funds from the UC Company by using MARCHENKO's Hong Kong companies to send the payments, just as they had for the June Order and August Order from Company-1, members of the Procurement Network continued to make misrepresentations in support of their cover story that the Micro-Displays were not going to Russia. For example, on or about January 30, 2023, CC-1 (posing as "Amy") submitted a "Statement By Ultimate Consignee and Purchaser," also known as a Form BIS-711,⁶ to the UC Company. The Form contained an explicit warning that the "making of any false statements or concealment of any material fact in connection with [the Form BIS-711] may result in imprisonment or fine." CC-1 stated that the Micro-Displays were to be used in ophthalmological microscopes and "glasses 3D visualization for the microscopes." The end-user countries were listed as "China, HK [Hong Kong], Malaysia, Europe"—*i.e.*, not Russia.

i. On or about February 14, 2023, the UC informed CC-1 (posing as "Amy Chan") that a shipment containing 700 of the 2,450 remaining Micro-Displays ("Shipment-2") had been shipped and provided the shipment tracking information. Over the next approximately three days, IP addresses associated with NPC Granat (the Russian company) checked the tracking information for Shipment-2. Shortly thereafter, on or about March 2, 2023, CC-1 messaged MARCHENKO and asked him to send \$294,000 to the UC Company.

***The Procurement Network Makes Overt Attempts to Evade U.S. Law Enforcement Scrutiny
After Shipment-2 Is Detained***

j. On or about March 4, 2023, the UC informed CC-1 (posing as "Amy Chan") that the Department of Commerce had detained Shipment-2 because of a concern that it would be diverted to prohibited end users in Russia. On or about March 6, 2023, CC-1 messaged MARCHENKO and provided MARCHENKO with the name and phone number for the UC.

k. That day, MARCHENKO, using the 1175 Number, had a recorded phone conversation with the UC. During that phone call, in substance and in part, MARCHENKO identified himself as "Maxim" from "Alice Components" and stated that he worked with "Amy"—a reference to CC-1's fictitious persona. MARCHENKO then falsely explained that payment for the Alice Components' orders was coming from a third party because of a problem with the bank account and that a lot of accounts were closed. As described above, MARCHENKO knew that this representation was false: he and other members of the Procurement Network discussed using his front companies in Hong Kong to obfuscate the fact that payment for the Micro-Displays came from Russia. *See supra* ¶¶ 20(c), (d); 22(i); 23(c).

l. While Shipment-2 was detained, CC-1 (posing as "Amy Chan") initially asked the UC, on or about March 13, 2023, to ship the Micro-Displays to SSP LTD, which was located at the Castle Peak Address in Hong Kong. Later, CC-1, who expressed frustration to the

⁶ Form BIS-711, also known as a Statement by Ultimate Consignee and Purchaser, provides information on the foreign importer receiving the U.S. technology and how the technology will be used. Federal regulations require the ultimate consignee or purchaser to provide either a statement on company letterhead with certain information or the Form BIS-711. *See* 15 C.F.R. § 748.11(c).

UC about Shipment-2 being detained, sent an email to the UC, asking the UC Company to issue a refund to Alice Components and provided the bank account information for SSP LTD.

m. While Shipment-2 was detained, CC-1, CC-2, and MARCHENKO remained in contact about Shipment-2.

n. In or about July 2023, the UC informed CC-1 (posing as “Amy Chan”) that the Department of Commerce had released Shipment-2 and that the UC Company was in possession of it.

o. On or about August 14, 2023, the UC and MARCHENKO exchanged several messages about the Micro-Displays that Alice Components ordered from the UC Company:

UC: I still haven't heard from you. I'm not sure where you want to go from here . . . I'm going to move the items from my office to our warehouse for storage until I hear from you.

MARCHENKO: hi, no one can come to US for pickup

MARCHENKO: can you send low value parcel by USPS

MARCHENKO: make value below 2500usd

UC: This is over a million dollars worth of product. Are you sure that is a good idea?

MARCHENKO: less risk

MARCHENKO: do before

MARCHENKO: split for few parcel

UC: Where do you want me to ship them to? How many split parcels do you want?

MARCHENKO: how its paked [sic] now?

MARCHENKO: try 100pcs first

UC: I think multiple shipment creates more risk. I can put a paid invoice in the box for a lower amount like you said. Who did you put on the end user form?

MARCHENKO: below 2500usd no need

MARCHENKO then provided the contact information for Namfleg. Based on my training, experience, I believe, in instructing the UC to package and send the Micro-Displays in this fashion, MARCHENKO was trying to circumvent the requirement to provide an EEI (“below 2500usd no need”) and thus avoid reporting the true destination of these goods (Russia).

Members of the Procurement Network Sought to Avoid U.S. Government Scrutiny and Maintain Their Cover Story

24. Based on my training, experience, conversations with other law enforcement agents and individuals, review of records and email communications maintained by Company-1, review of open-source materials, bank records, and email communications and messages obtained pursuant to judicially authorized search warrants, and draft summaries and translations of such documents and communications, I have learned the following, in substance and in part:

a. Members of the Procurement Network were wary of U.S. Government scrutiny of their illicit activities and openly discussed the need to maintain their cover story.

b. For instance, on or about June 29, 2022, MARCHENKO and CC-2 exchanged the following messages about actions the United States had taken against Chinese companies that violated sanctions by supporting the Russian defense apparatus and the need for the Procurement Network to proceed with care:

MARCHENKO: The White House blacklisted five Chinese companies for violating sanctions by supporting Russian military and defense companies.

This includes Connec Electronic, King Pai Technology, Sinno Electronics, Winninc Electronic, and World Jetta (HK) Logistics.

— Today’s action sends a strong message to businesses and individuals around the world that if they seek to support Russia, the United States will take action, — said U.S. Deputy Secretary of Commerce Alan Esteves.

CC-2: So we’ll be even more careful

c. Similarly, on or about March 14 and 15, 2023, MARCHENKO sent multiple messages to CC-1 about banks being sanctioned by OFAC. In particular, MARCHENKO sent a message about an NPC Topaz transaction being returned because it was sent by a sanctioned bank.

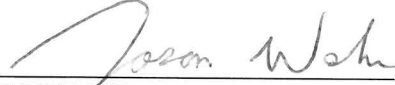
d. Members of the Procurement Network also discussed inventing other fictitious covers to potentially obtain more goods from Company-1. For instance, on or about September 30, 2022, CC-1 emailed MARCHENKO and asked him to contact Company-1 about 170 pieces of Part Number-2 (*i.e.*, a specific version of the Micro-Displays). CC-1 instructed

MARCHENKO to make the request from “a third party company that hasn’t passed before (can’t be Neway, RG Solution, IRZ).” CC-1 further told MARCHENKO that the application would be a viewfinder for an action camera and stated that the project would require 5,000 pieces in a year. Based on my training, experience, and participation in this investigation, I believe that CC-1 asked MARCHENKO to order more Micro-Displays from Company-1 using another one of MARCHENKO’s front companies and creating another false cover story that Company-1 was not familiar with so as to avoid arousing scrutiny or suspicion for future orders.

e. Finally, on or about March 6, 2023—the day MARCHENKO reached out to the UC to discuss the Department of Commerce detaining Shipment-2—CC-1 bluntly told MARCHENKO that: “We support the legend that we are Alice Components and we know nothing about Russia.” Based on my training, experience, and involvement in this investigation, I believe CC-1 was reassuring MARCHENKO that CC-1 was committed to the cover story created by the Procurement Network in light of U.S. Government scrutiny of the Procurement Network’s efforts to smuggle sensitive technologies to Russia.

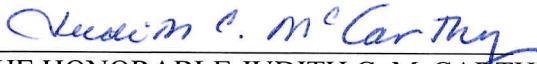
25. In summary, based on my training, experience, and participation in this investigation, including, among other things, the fact that (1) prior to in or about February 2022, MARCHENKO paid for and received at least some orders from Company-1 on behalf of Radiofid, whose end user was listed as an entity in Russia; (2) Alice Components became a customer of Company-1 shortly after Russia invaded Ukraine in or about February 2022 and Company-1 decided it would not sell to Russian customers or customers who shipped their goods to Russia; (3) Alice Components used third party companies associated with MARCHENKO to pay Company-1 and the UC Company, and these third party companies often received payment from Russian companies prior to paying Company-1 or the UC Company; (4) MARCHENKO sent or received messages about evading sanctions and banks returning certain transactions due to sanctions; (5) CC-2, who is connected to Russian companies OOO NPTC Topaz and NPC Granat, which is on the Department of Commerce’s Entity List, messaged MARCHENKO that payment (equal to outstanding balances Alice Components owed to Company-1 and the UC Company) would be sent to MARCHENKO’s front company, RG Solutions; (6) CC-1 often instructed MARCHENKO to pay Company-1 or the UC Company; (7) CC-1, in a conversation with MARCHENKO, referred to Alice Components as a “legend”; (8) IP addresses associated with Russian company NPC Granat checked on the status of Shipment-1 and Shipment-2 shortly after the tracking information was provided to CC-1; (9) MARCHENKO told the UC to split the Micro-Displays into multiple parcels and declare that the value of the package was under \$2,500, likely to avoid filing an EEI; and (10) MARCHENKO’s companies sent or received invoices, or had contracts with, Russia-based companies for Micro-Displays, I believe members of the Procurement Network, including MARCHENKO, falsely represented to Company-1 and the UC Company that the Micro-Displays were destined for countries other than Russia with the belief that these false representations would be passed along to U.S. government agencies.

WHEREFORE, I respectfully request that a warrant be issued for the arrest of MAXIM MARCHENKO, the defendant, and that he be arrested, and imprisoned or bailed, as the case may be.



JASON WAKE
Special Agent
Federal Bureau of Investigation

Sworn to me this 25th day of August, 2023.



THE HONORABLE JUDITH C. McCARTHY
United States Magistrate Judge
Southern District of New York



U.S. Department of Justice

*United States Attorney
Eastern District of New York*

JAM

*271 Cadman Plaza East
Brooklyn, New York 11201*

December 13, 2022

By ECF

The Honorable Hector Gonzalez
United States District Judge
Eastern District of New York
225 Cadman Plaza East
Brooklyn, New York 11201

Re: United States v. Yevgeniy Grinin et al.
Docket No. 22-CR-409 (S-1) (HG)

Dear Judge Gonzalez:

The government writes regarding bail for defendants Alexey Brayman and Vadim Yermolenko, who have been arrested and charged in the above-referenced superseding indictment (the “Superseding Indictment”). Defendant Vadim Konoshchenok has also been taken into custody in Estonia and will undergo extradition proceedings to the United States.

The government respectfully requests that the Court set bail in the amount of \$250,000 for Brayman and \$500,000 for Yermolenko, with each secured by real property or other reliable surety. Both defendants should also be required to surrender their passports. As described in the Superseding Indictment and herein, the defendants present flight risks and have significant ties to foreign jurisdictions, including non-extradition countries.¹

I. Relevant Background

The Superseding Indictment charges seven defendants with facilitating the activities of the Serniya procurement network (the “Serniya Network”), which operated under the direction of Russia’s intelligence services to acquire sensitive military and dual use technologies for the Russian military, defense sector and research institutions. In or about March 2022, both the U.S. Department of Commerce and the U.S. Department of the

¹ Detailed herein is a proffer of the relevant facts and a discussion of the applicable law pertaining to the pretrial detention of the defendant. See United States v. LaFontaine, 210 F.3d 125, 130-31 (2d Cir. 2000) (government entitled to proceed by proffer in detention hearings).

Treasury’s Office of Foreign Assets Control (“OFAC”) levied sanctions on several individuals and entities in the Serniya Network. According to OFAC’s press release, the designation was part of “its crackdown on the Kremlin’s sanctions evasion networks and technology companies, which are instrumental to the Russian Federation’s war machine.”

One of the Serniya Network’s primary operatives in the United States was defendant Boris Livshits, a Russian national who formerly lived in Brooklyn, New York. As alleged in the Superseding Indictment, Livshits would interface directly with U.S. companies and purchase export-controlled items requested by the Serniya Network for Russian end users. In doing so, Livshits would misrepresent and omit material information to companies, banks and government agencies, including information about how the item would be used, the various parties involved in the transaction, and the identity of the ultimate end user. Livshits also utilized dozens of U.S.-based front companies and bank accounts that were used to obfuscate the role of Russian or sanctioned entities in transactions.

As described in the Superseding Indictment, the defendants Brayman and Yermolenko worked closely with Livshits in furtherance of the scheme. Both Brayman and Yermolenko would alter, forge, and destroy shipping documents, invoices and other business records to unlawfully export items from the United States. Yermolenko also opened numerous shell companies and bank accounts, made structured deposits and withdrawals, and made material misrepresentations to U.S. financial institutions in order facilitate the scheme and avoid detection. Brayman used his residence in New Hampshire as a frequent transshipment point for items that were unlawfully exported from the U.S. and ultimately destined for Russia. These shipments continued after the March 2022 sanctions were levied on the Serniya Network.

In addition to other transshipment points throughout the world, Brayman sent illicit shipments to Konoshchenok in Estonia, where Konoshchenok would smuggle U.S.-origin items across the border into Russia. As described in the Superseding Indictment, during one such attempt on October 27, 2022, Konoshchenok was detained attempting to cross into Russia from Estonia with approximately 35 different types of semiconductors and electronic components, including several U.S.-origin and export-controlled items ordered by Livshits.

Konoshchenok has also been repeatedly stopped by Estonian border officials attempting to smuggle tens of thousands of rounds worth of American-made and export-controlled ammunition into Russia, including 6.5 mm, 7 mm, .338 and .300 Winchester Magnum rounds, which are commonly used by snipers, as well as military-grade .223 rounds. In doing so, Konoshchenok used an Estonian front company called “Stonebridge Resources” and communicated frequently with Livshits and other coconspirators about sourcing, transporting and paying for the ammunition. For example, in one message, Konoshchenok explicitly stated that he will “take the other car [with] the bullets, the shell casings.” In another message exchange, Konoshchenok is given an order of “6.5 mm 147 gn – 1000 pcs . . . 6.5 mm 156 gn – 900 pcs . . . 7 mm 190gn – 400 pcs284win – 100 pcs . . . The first three are bullets. The fourth one is casings.” Konoshchenok is clear that his fee is “10%” because he “can’t do less. Sanctions . . . Sanction item for 10%.” To consummate one transaction, Livshits

advised Konoshchenok to “fabricate” or “draw” the “receipt” and other documents. In another message, Livshits asked Konoshchenok if he can “send the money to Stonebridge” and misrepresent the purpose of the payment, “for example for auto parts.”

Konoshchenok is suspected of being an active Russian intelligence operative. In electronic communications, Konoshchenok explicitly identified himself as a “Colonel” with Russia’s Federal Security Service (“FSB”), the successor agency to the Soviet KGB, which oversaw the Serniya Network. In one electronic message exchange, Konoshchenok described how he just received a new “passport photo” and enclosed a photograph of himself wearing his FSB uniform:



Incident with Konoshchenok’s arrest on December 6, 2022, Estonian authorities searched a warehouse held in the name of Konoshchenok’s son and recovered approximately 375 pounds worth of ammunition.

II. Legal Standard

Under the Bail Reform Act, Title 18, United States Code, Section 3141, et seq., federal courts are empowered to order a defendant’s detention pending trial upon a determination that the defendant is either a danger to the community or a risk of flight. See 18 U.S.C. § 3142(e) (a judicial officer “shall” order detention if “no condition or combination of conditions would reasonably assure the appearance of the person as required and the safety of

any other person and the community”). A finding of risk of flight must be supported by a preponderance of the evidence. See United States v. Jackson, 823 F.2d 4, 5 (2d Cir. 1987).

In addition, the Bail Reform Act lists the following factors to be considered in the detention analysis: (1) the nature and circumstances of the offenses charged; (2) the weight of the evidence against the defendant; (3) the history and characteristics of the defendant; and (4) the nature and seriousness of the danger to any person or the community that would be posed by the defendant’s release. See 18 U.S.C. § 3142(g). As discussed below, these factors weigh against pretrial release and necessitate a sizable bail package.

III. The Court Should Set Substantial and Securitized Bail

As set forth below, the factors to be considered in the detention analysis show that the defendants present substantial risks of flight that can only be mitigated by a substantial, fully secured bond.

The charged offenses are extremely serious. The defendants are charged with participating in a transnational fraud, money laundering and sanctions evasion scheme controlled by a foreign power that is actively engaged in armed conflict. While the investigation is ongoing, the evidence amassed against Brayman and Yermolenko is substantial, including, inter alia, (1) electronic communications between Brayman, Yermolenko, Livshits and other coconspirators; (2) invoices, shipping documents and other business records containing false information, including official forms filed with the Department of Commerce and other government agencies; (3) bank and tax records reflecting the establishment and use of shell companies and illicit money movements; and (4) items recovered from Brayman’s residence during the execution of a court-authorized search warrant, including documents related to export-controlled items and multiple cell phones of Chinese or foreign origin. See, e.g., United States v. Fishenko, No. 12-CR-626, 2013 WL 3934174, at *2 (E.D.N.Y. July 30, 2013) (evidence of “pertinent recorded conversations and email exchanges that reveal [the defendant’s] role in the conspiracy” weighed against release). The defendants also face a significant term of incarceration should they be convicted, which provides powerful incentive for them to flee. See, e.g., United States v. Bruno, 89 F. Supp. 3d 425, 431 (E.D.N.Y. 2015) (“When the sentence . . . upon conviction is likely to be long . . . a defendant has stronger motives to flee.”).

While both Brayman and Yermolenko have strong ties to the United States and their respective home districts, they both maintain significant connections to foreign countries, and the government would have limited ability to recapture or extradite them if they were to flee. Notably, Brayman is an Israeli citizen. While the government acknowledges that Brayman has been aware of the investigation since the search warrant execution at his home in October 2022, the fact that he has now been indicted necessarily increases the risk of potential flight.

IV. Conclusion

For all of these reasons, the government respectfully submits that the defendants represent a serious risk of flight if released on bond. As such, a secured bond of at least \$500,000 for Yermolenko, a secured bond of at least \$250,000 for Brayman, and surrender of their passports and travel documents are necessary to ensure their return to court.

Respectfully submitted,

BREON PEACE
United States Attorney

By: /s/ Artie McConnell
Artie McConnell
Assistant U.S. Attorney
(718) 254-7000

cc: Clerk of Court (by ECF)
Defense Counsel (by email)

UNITED STATES DISTRICT COURT

for the

Eastern District of New York

United States of America

v.

YEVGENIY GRININ et al

)
)
)
)
)
)

Case No. 22-CR-409 (HG)

Defendant

ARREST WARRANT

To: Any authorized law enforcement officer

YOU ARE COMMANDED to arrest and bring before a United States magistrate judge without unnecessary delay

(name of person to be arrested) VADIM KONOSHCHENOK

who is accused of an offense or violation based on the following document filed with the court:

- Indictment Superseding Indictment Information Superseding Information Complaint
- Probation Violation Petition Supervised Release Violation Petition Violation Notice Order of the Court

This offense is briefly described as follows:

Title 18, United States Code, Section 371 (conspiracy to defraud to the United States); Title 50, United States Code, Section 4819(a) (conspiracy to violate the Export Control Reform Act); and Title 18, United States Code, Section 554(a) (smuggling goods from the United States);

Date: 12/05/2022

[Redacted Signature]

Issuing officer's signature

City and state: Brooklyn, New York

[Redacted Name]

Printed name and title

[Redacted Title]

Return

This warrant was received on (date) _____, and the person was arrested on (date) _____
at (city and state) _____.

Date: _____

Arresting officer's signature

Printed name and title

★ DEC 05 2022 ★

BROOKLYN OFFICE

AAS:JAM
F. #2021R01110

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK

----- X

UNITED STATES OF AMERICA

- against -

YEVGENIY GRININ,
ALEKSEY IPPOLITOV,
BORIS LIVSHITS,
SVETLANA SKVORTSOVA,
VADIM KONOSHCHENOK,
ALEXEY BRAYMAN and
VADIM YERMOLENKO,

Defendants.

SUPERSEDING
INDICTMENT

Cr. No. 22-409 (S-1) (HG)
(T. 13, U.S.C., § 305(a)(1); T. 18,
U.S.C., §§ 371, 554, 981(a)(1)(C),
982(a)(1), 982(a)(2), 982(b)(1), 1343,
1349, 1956(h), 1957(a), 1957(b),
1957(d)(1), 2 and 3551 et seq.; T. 21,
U.S.C., § 853(p); T. 28, U.S.C.,
§ 2461(c); T. 50, U.S.C., §§ 4819(a)(1),
4819(a)(2)(A)-(G), 4819(b),
4819(d)(1), 4819(d)(2), 1705(a) and
1705(c); T. 15, C.F.R., §§ 736.2(b)(1)
and 746.8(a)(1))

----- X

THE GRAND JURY CHARGES:

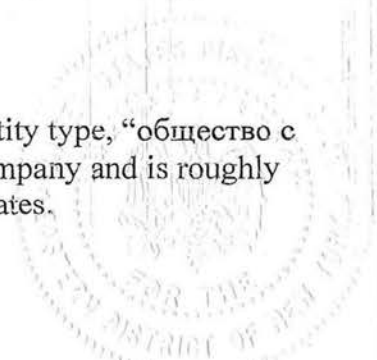
INTRODUCTION

At all times relevant to this Superseding Indictment, unless otherwise indicated:

I. The Serniya Procurement Network

1. OOO¹ Serniya Engineering (“Serniya”) was a wholesale machinery and equipment company based in Moscow, Russia. Serniya headed an illicit procurement network operating under the direction of Russia’s intelligence services (collectively, the

¹ “OOO” is the abbreviation for the Russian business entity type, “общество с ограниченной ответственностью,” which means limited private company and is roughly the equivalent of a limited liability company or LLC in the United States.



“Serniya Network”), which evaded U.S. and Western sanctions to acquire sensitive military grade and dual use technologies, including advanced semiconductors, for the Russian military, defense sector and research institutions. The Serniya Network’s clients included the following Russian companies and entities: State Corporation Rostec, the state-owned defense conglomerate; State Atomic Energy Corporation Rosatom (“Rosatom”); JSC Rusnano, the state-owned nanotechnology company; the National Research Nuclear University of the Moscow Engineering Physics Institute; the Ministry of Defense; the Foreign Intelligence Service (“SVR”); and various components of the Federal Security Service (“FSB”), Russia’s principal security agency and the main successor agency to the Soviet Union’s KGB, including the Department of Military Counterintelligence and the Directorate for Scientific and Technological Intelligence, commonly known as “Directorate T.”

2. OOO Sertal (“Sertal”) was a wholesale machinery and equipment company based in Moscow, Russia. As described herein, Sertal operated within the Serniya Network and in turn utilized a network of front companies, shell entities and bank accounts throughout the world, including in the United States, to source, purchase and ship export-controlled items from the U.S. to Russia.

3. Sertal was an FSB-accredited contractor authorized to conduct highly sensitive and classified procurement activities. In on about August 2020, Sertal obtained a renewal of its license from the FSB, allowing it to “carry out work related to the use of information constituting a state secret up to the top-secret level.”² In an August 31, 2020

² Unless otherwise indicated, all quoted communications contained herein are translations of written or spoken Russian.

letter to the All-Russian Research Institute of Automation (“VNIIA”), a Rosatom subsidiary that developed nuclear weapons and their components, Sertal’s General Director confirmed the reissuance of its FSB license, stating that, “since June 2016, Sertal LLC has successfully performed and is performing work using information constituting a state secret . . . we suggest that you further consider our company as a potential supplier of complex equipment, devices and components.”

4. On or about March 3, 2022, Serniya and Sertal were added to the U.S. Department of Commerce (“DOC”) Bureau of Industry and Security (“BIS”) Entity List (the “Entity List”), found at Title 15, Code of Federal Regulations, part 774, Supplement Number 4. The Entity List imposed additional license requirements and export restrictions due to a determination that the entities included on the list had engaged in activities contrary to U.S. national security or foreign policy interests. BIS added Serniya and Sertal to the Entity List because of their relationship to the Russian government and in response to Russia’s invasion of Ukraine beginning in February 2022. Specifically, BIS indicated that Serniya, Sertal and other entities were sanctioned because they “have been involved in, contributed to, or otherwise supported the Russian security services, military and defense sectors, and military and/or defense research and development efforts.” 87 Fed. Reg. 13141. BIS adopted a “policy of denial” with respect to Serniya and Sertal, indicating that BIS would not authorize a license to export items to Serniya or Sertal.

5. On or about March 31, 2022, pursuant to Executive Order 14024, the U.S. Department of the Treasury’s Office of Foreign Assets Control (“OFAC”) designated Serniya, Sertal and several other entities in the Serniya Network and added them to the list of Specially Designated Nationals and Blocked Persons (the “SDN List”). According to

OFAC's press release, the designation was part of "its crackdown on the Kremlin's sanctions evasion networks and technology companies, which are instrumental to the Russian Federation's war machine." OFAC described Serniya as:

the center of a procurement network engaged in proliferation activities at the direction of Russian Intelligence Services. This network operates across multiple countries to obfuscate the Russian military and intelligence agency end-users that rely on critical western technology. Serniya and Moscow-based OOO Sertal work to illicitly procure dual-use equipment and technology for Russia's defense sector.

6. OFAC also designated several individuals and companies operating in the Serniya Network, including United Kingdom-based Majory LLP, United Kingdom-based Photon Pro LLP, and Spain-based Invention Bridge SL, among others, identifying them as "front companies utilized by Serniya to facilitate its procurement of key equipment for the Government of the Russian Federation."

II. The Defendants

7. The defendant YEVGENIY GRININ was a Russian national who resided in Russia. GRININ worked for Sertal as its Technical Director and was an executive officer of Photon Pro LLP, a front company used by the Serniya Network. On or about March 9, 2022, BIS added Photon Pro to the Entity List. On or about March 31, 2022, pursuant to Executive Order 14024, OFAC added GRININ to its SDN List for "being a leader, official, senior executive officer, or member of the board of directors of Photon Pro LLP."

8. The defendant ALEKSEY IPPOLITOV was a Russian national who resided in Russia. IPPOLITOV was affiliated with the All-Russian Scientific Research Institute of Electromechanics, a Moscow-based research institute and a subsidiary of

ROSCOSMOS, the Russian state space corporation, which developed satellites and military spacecraft. IPPOLITOV was also affiliated with the All-Russian Research Institute for Optical and Physical Measurements (“VNIIOFI”). VNIIOFI was added to the Entity List on April 7, 2022.

9. The defendant BORIS LIVSHITS was a Russian national who resided in Russia and previously lived in Brooklyn, New York. LIVSHITS owned and/or controlled several front companies that operated on behalf of the Serniya Network. These entities conducted no actual business and were used to obfuscate the role of Russian or sanctioned entities in transactions.

10. The defendant SVETLANA SKOVORTSOVA was a Russian national who resided in Russia. SKOVORTSOVA worked for Sertal as Advisor to the General Director under the supervision of the defendant YEVGENIY GRININ.

11. The defendant VADIM KONOSHCHENOK was a Russian national who resided in Estonia.

12. The defendant ALEXEY BRAYMAN was a lawful permanent resident of the United States who resided in New Hampshire.

13. The defendant VADIM YERMOLENKO was a United States citizen who resided in New Jersey.

III. The Statutory and Regulatory Background

A. The International Emergency Economic Powers Act and the Relevant Sanctions Orders and Regulations Relating to Russia

14. The International Emergency Economic Powers Act (“IEEPA”), codified at Title 50, United States Code, Sections 1701 through 1708, conferred upon the

President the authority to deal with unusual and extraordinary threats to the national security and foreign policy of the United States. Section 1705 provided, in part, that “[i]t shall be unlawful for a person to violate, attempt to violate, conspire to violate, or cause a violation of any license, order, regulation, or prohibition issued under this chapter.” 50 U.S.C.

§ 1705(a).

15. In 2014, pursuant to his authorities under the IEEPA, the President issued Executive Order 13660, which declared a national emergency with respect to Russia’s violation of the sovereignty of Ukraine by asserting authority over the Crimea region. To address this national emergency, the President blocked all property and interest in property that were then or thereafter came within the United States or the possession or control of any United States person, of individuals determined by the Secretary of the Treasury to meet one or more enumerated criteria. These criteria included, but were not limited to, individuals determined to be responsible for or complicit in, or who engaged in, actions or policies that threaten the peace, security, stability, sovereignty or territorial integrity of Ukraine; or who materially assisted, sponsored or provided financial, material or technological support for, or goods or services to, individuals or entities engaging in such activities. Executive Order 13660 prohibited, among other things, transferring, paying, exporting, withdrawing and otherwise dealing in any interest in property in the United States owned by a person whose property and interests in property were blocked (a “blocked person”), as well as the making of any contribution or provision of funds, goods or services by a United States person to or for the benefit of a blocked person and the receipt of any contribution or provision of funds, goods or services by a United States person from any such blocked person.

16. The national emergency declared in Executive Order 13660 with respect to the situation in Ukraine remained in continuous effect since 2014 and was renewed on March 2, 2022, following Russia's most recent invasion of Ukraine.

17. On multiple occasions, the President expanded the scope of the national emergency declared in Executive Order 13660, including through: (1) Executive Order 13661, issued on March 16, 2014, which addressed the actions and policies of the Russian Federation with respect to Ukraine, including the deployment of Russian Federation military forces in the Crimea region of Ukraine; and (2) Executive Order 13662, issued on March 20, 2014, which addressed the actions and policies of the Government of the Russian Federation, including its purported annexation of Crimea and its use of force in Ukraine. Executive Orders 13660, 13661 and 13662 were collectively referred to as the "Ukraine-Related Executive Orders." On February 21, 2022, the President again expanded the scope of the national emergency, finding that the Russian Federation's purported recognition of the so-called Donetsk People's Republic and Luhansk People's Republic regions of Ukraine contradicted Russia's commitments under the Minsk agreements and threatened the peace, stability, sovereignty and territorial integrity of Ukraine.

18. The Ukraine-Related Executive Orders authorized the Secretary of the Treasury to take such actions, including the promulgation of rules and regulations, and to employ all powers granted to the President under the IEEPA, as necessary to carry out the purposes of those orders. The Ukraine-Related Executive Orders further authorized the Secretary of the Treasury to redelegate any of these functions to other offices and agencies of the U.S. Government.

19. To implement the Ukraine-Related Executive Orders, OFAC issued certain Ukraine-Related Sanctions Regulations. These regulations incorporated by reference the prohibited transactions set forth in the Ukraine-Related Executive Orders. See 31 C.F.R. § 589.201. The regulations also provided that the names of persons designated directly by the Ukraine-Related Executive Orders, or by OFAC pursuant to the Ukraine-Related Executive Orders, whose property and interests were therefore blocked, would be published in the Federal Register and incorporated into the SDN List, published on OFAC's website. Id. n.1.

B. The Export Control Reform Act and Export Administration Regulations

20. The Export Administration Regulations ("EAR"), 15 C.F.R. §§ 730-774, were promulgated by BIS to regulate the export of goods, technology and software from the United States. Under the Export Control Reform Act ("ECRA"), it was a crime to violate, attempt to violate, conspire to violate or cause a violation of any regulation, order, license or authorization issued pursuant to the statute, including the EAR. See 50 U.S.C. § 4819(a)(1). Willful violations of the EAR constituted criminal offenses under the ECRA, and carried a 20-year maximum term of imprisonment and up to a \$1,000,000 fine. See 50 U.S.C. § 4819(b).

21. Through the EAR, the BIS reviewed and controlled the export from the United States to foreign countries of certain U.S. items. See 15 C.F.R. §§ 734.2-.3. In particular, the BIS placed restrictions on the export and re-export of items that it determined could make a significant contribution to the military potential or nuclear proliferation of other nations or that could be detrimental to the foreign policy or national security of the United States. Under the EAR, such restrictions depended on several factors, including the

technical characteristics of the item, the destination country, the end user and the end use of the item.

22. The most sensitive items subject to the EAR controls were identified on the Commerce Control List (“CCL”) set forth in Title 15, Code of Federal Regulations, part 774, Supplement Number 1. Items listed on the CCL were categorized by Export Control Classification Number (“ECCN”), each of which was subject to export control requirements depending on destination, end use and end user of the item.

23. The BIS published the names of certain foreign persons—including businesses, research institutions, government and private organizations, individuals and other types of legal persons—that were subject to specific license requirements for the export, reexport and/or transfer (in-country) of specified items. These persons comprised the Entity List found at Title 15, Code of Federal Regulations, part 774, Supplement Number 4. The persons on the Entity List were subject to individual licensing requirements and policies supplemental to those found elsewhere in the EAR, due to a determination that such persons had engaged in activities contrary to U.S. national security and/or foreign policy interests.

24. In response to Russia’s 2022 invasion of Ukraine, the DOC imposed new license requirements on exports to Russia. As of February 24, 2022, any item classified under any ECCN in Categories 3 through 9 of the CCL required a license to be exported to Russia. See 87 Fed. Reg. 12226 (Mar. 3, 2022). As of April 8, 2022, the license requirement for export to Russia was expanded to cover all items on the CCL. See 87 Fed. Reg. 22130 (Apr. 14, 2022). These rules were codified in Title 15, Code of Federal Regulations, part 746.8, which stated, “a license is required, excluding deemed exports and deemed reexports, to export, reexport, or transfer (in-country) to or within Russia or Belarus

any item subject to the EAR and specified in any Export Control Classification Number (ECCN) on the CCL.”

25. Federal law required that any international shipment where a valid export license is required or where the commodity classified is over \$2,500 be logged in the Automated Export System (“AES”) via an Electronic Export Information (“EEI”) filing. Failure to make an EEI filing or providing false or misleading information on an EEI filing in the AES was a violation of 13 U.S.C. § 305.

IV. Overview of the Criminal Scheme

26. Since at least 2017, the defendants YEVGENIY GRININ, ALEKSEY IPPOLITOV, BORIS LIVSHITS, SVETLANA SKVORTSOVA, VADIM KONOSHCHENOK, ALEXEY BRAYMAN, VADIM YERMOLENKO and their co-conspirators in the Serniya Network unlawfully sourced, purchased and shipped millions of dollars in military and sensitive dual-use technologies from U.S. manufacturers and vendors located in the Eastern District of New York and elsewhere (collectively, the “U.S. Companies”) for Russian end users, in violation of IIEPA, ECRA and other U.S. criminal statutes. These items included advanced electronics and sophisticated testing equipment used in quantum computing, hypersonic and nuclear weapons development and other military and space-based military applications.

27. To effectuate the scheme, the defendants YEVGENIY GRININ, ALEKSEY IPPOLITOV, BORIS LIVSHITS, SVETLANA SKVORTSOVA, VADIM KONOSHCHENOK, ALEXEY BRAYMAN, VADIM YERMOLENKO and their co-conspirators made and caused to be made material misrepresentations and omissions, both orally and in writing, with respect to invoices, end use statements, financial records and

shipping documents, among other items, to conceal the nature of these illicit procurement transactions. By doing so, the defendants and their co-conspirators caused the U.S. Companies to sell and export sensitive military and dual-use items in violation of IEEPA, ECRA, and other U.S. laws and regulations; process and accept payments in furtherance of such illicit transactions; and fail to file documents with the DOC, BIS and other U.S. government entities, including license applications and required statements regarding the ultimate consignee and purchaser. The defendants and their co-conspirators also caused U.S. financial institutions to process millions of dollar-based payments in violation of IEEPA, ECRA and other U.S. laws and regulations. Several of these transactions were processed through correspondent accounts at New York City banks and within the Eastern District of New York.

28. To purchase and export items from the U.S. Companies, the defendants YEVGENIY GRININ, ALEKSEY IPPOLITOV, BORIS LIVSHITS, SVETLANA SKVORTSOVA, VADIM KONOSHCHENOK, ALEXEY BRAYMAN, VADIM YERMOLENKO and their co-conspirators in the Serniya Network routed and layered transactions through a variety of front companies and bank accounts located in jurisdictions throughout the world. Specifically, items were shipped from the U.S. Companies to various locations in the United States and Europe that corresponded to fictitious addresses registered to shell companies controlled by the Serniya Network. Items were repackaged and reshipped to several intermediate locations in Europe and Asia before arriving in Russia. Common transshipment points included locations in Estonia, Finland, Germany and Hong Kong. Payments were also layered, with money being transferred to accounts in the names of shell companies held at different banks in jurisdictions throughout the world before

eventually arriving in Russia. Additionally, shipping documents understated the value of the exports from the U.S. to avoid applicable reporting requirements, thereby avoiding additional scrutiny. Accordingly, the defendants and their co-conspirators disguised the audit trail of shipments and payments and concealed the true Russian end users for items purchased from the U.S. Companies.

V. The Defendants' Involvement in the Serniya Network

29. The defendant ALEKSEY IPPOLITOV acted as a liaison between Serniya and Sertal on the one hand, and Russian end users in the defense and technology sectors on the other. IPPOLITOV solicited orders from Russian end users who sought to acquire a particular item or part from the United States. IPPOLITOV then relayed the request to employees at Sertal and Serniya, including the defendants YEVGENIY GRININ and SVETLANA SKVORTSOVA, who were tasked with procuring the desired component from the U.S. Companies. IPPOLITOV oversaw the purchase and shipping of the items from the U.S. Companies through the Serniya Network's front companies and bank accounts.

30. The defendants YEVGENIY GRININ and SVETLANA SKVORTSOVA decided how to fulfill orders placed by Russian end users, including those orders placed through the defendant ALEKSEY IPPOLITOV. GRININ and SKVORTSOVA secured funding and shipping for the transactions, as well as assisted in preparing documents with false and misleading information in furtherance of the scheme. The fact that a specific item was subject to U.S. export controls and regulations was often apparent to the conspirators. For example, in a July 25, 2019 email, a Serniya employee asked GRININ, "[C]an you help me obtain these items [high-performance pressure transducers] from the States? These pressure transducers fall under export controls. What

information will be needed from me?” Similarly, a June 2020 email exchange between GRININ, SKVORTSOVA and other Serniya and Sertal employees was titled “URGENT: Important Announcement about US Export Regulation Changes” and specifically described the definition of “military end-users.”

31. The defendants YEVGENIY GRININ and SVETLANA SKVORTSOVA frequently tasked the defendant BORIS LIVSHITS to interface directly with the U.S. Companies and purchase items requested by Russian end users. In doing so, GRININ, SKVORTSOVA and LIVSHITS discussed methods to evade U.S. export controls and other criminal laws. For example, in an email exchange on or about December 17, 2018, LIVSHITS opined to SKVORTSOVA that “complications with export [of an item from the U.S.] will not be known until order.” After SKVORTSOVA asked for clarification, LIVSHITS responded, “The same as usual—with export control and finding out who the buyer and the final user and why it is bought, for what application. . . [a]s it was then with the [prior transaction involving a part from a U.S. Company], it seemed harmless purchase, [but still] took a month of correspondence with them.” Similarly, in an email on or about March 15, 2022, after Serniya and Sertal were added to the BIS Entity List, LIVSHITS wrote to SKVORTSOVA, “When ordering in the USA, the price is significantly more expensive . . . [as well as] difficulties with export from there—[the item] is subject to EAR.” In another instance, in response to an inquiry from a U.S. Company, LIVSHITS asked GRININ to provide an explanation for how a particular item would be used and the identity of the end user. After GRININ responded with a technical explanation, LIVSHITS sent an invoice falsely listing the end user as Strandway LLC, a front company controlled by LIVSHITS, at an address in New York City.

32. The defendant BORIS LIVSHITS also counseled breaking up larger orders to avoid detection by law enforcement. For example, in response to a September 4, 2019 inquiry from the Physics Institute of the Russian Academy of Sciences (“FIAN”), the defendant ALEXEY IPPOLITOV emailed the defendant YEVGENIY GRININ about obtaining a “chip set” of 45 advanced semiconductors and other items from a Dallas-based technology company (“U.S. Company 1”). On September 4, 2019, IPPOLITOV forwarded a document from FIAN to GRININ titled “Foreign Equipment for FIAN.” GRININ, in turn, forwarded the document to the defendant SVETLANA SKVORTSOVA, and in a September 6, 2019 email, GRININ proposed tasking the defendant BORIS LIVSHITS with helping fulfill the order. On September 6, 2019, after GRININ and SKVORTSOVA contacted LIVSHITS and requested a price quote, GRININ, SKVORTSOVA and LIVSHITS discussed the requested semiconductors and other comparable items. In one email, LIVSHITS cautioned that the part required an export license and that “you need to buy such positions carefully, at 5-10 pieces at a time.”

33. In another example, in a July 16, 2020 email to the defendant SVETLANA SKVORTSOVA, LIVSHITS warned that “such a large and expensive order would draw unwanted attention and suspicion . . . break up the order into smaller orders over a time period.” LIVSHITS further advised that “the U.S. Department of Commerce Bureau of Industry and Security can cause problems and deny the shipment,” and suggested that he could order the parts from his U.S. companies, as well as entities in Estonia and Finland, over a two- to three-week period.

34. The defendant BORIS LIVSHITS, who spoke English, communicated with the U.S. Companies through in-person meetings, telephonic conversations and in email

and text exchanges. In those communications, LIVSHITS misrepresented and omitted material information, including information about how the item would be used, the various parties involved in the transaction, and the identity of the ultimate Russian end user.

35. For example, the defendant BORIS LIVSHITS often used the alias “David Wetzky” to communicate with the U.S. Companies to frustrate due diligence efforts by the U.S. Companies. In or about April and May 2022, after Serniya and Sertal were added to both the BIS Entity List and the SDN List, LIVSHITS used the alias to contact an Illinois-based electronics distributor (“U.S. Company 2”) via email and inquire about purchasing a variety of dual-use oscilloscopes, including models that were controlled by the DOC under ECCN 3A992.a for reasons of anti-terrorism. In or about April 2022, U.S. Company 2 sold LIVSHITS one of these oscilloscopes for approximately \$25,000; invoices and other records falsely listed “Strandway LLC” and “David Wetzky” as the purchaser and end user of the item. The item was shipped to an address in Merrimack, New Hampshire (the “New Hampshire Residence”), which was the home address of defendant ALEXEY BRAYMAN. On May 9, 2022, BRAYMAN shipped a package from the New Hampshire Residence to a location in Hamburg, Germany with the label reading “OSCILLOSCOPE – USED, NO WARR” and denoting the same make and model purchased from U.S. Company 2. The value of the item was falsely listed as \$2,482.

36. The defendants ALEXEY BRAYMAN and VADIM YERMOLENKO assisted the defendant BORIS LIVSHITS in unlawfully exporting dual-use and controlled items from the United States. Specifically, YERMOLENKO shipped packages to BRAYMAN at the New Hampshire Residence, which was a frequent transshipment point for items that were unlawfully exported from the United States to Russia. For example,

regarding one shipment, LIVSHITS instructed YERMOLENKO, "We need to send DHL to Germany, to the same company" with the items' description falsely being listed as "Duffle bag size L -\$300" and "Duffle bag size XL - \$550." YERMOLENKO sent LIVSHITS a shipping invoice that YERMOLENKO had signed addressed to the New Hampshire Residence. LIVSHITS then forwarded the invoice to the defendants YEVGENIY GRININ and SVETLANA SKVORTSOVA.

37. Additionally, while acting under the defendant BORIS LIVSHITS' direction, the defendants ALEXEY BRAYMAN and VADIM YERMOLENKO altered or destroyed shipping documents and other business records, as well as facilitated payments in furtherance of illicit transactions. For example, in a May 23, 2018 email to YERMOLENKO, LIVSHITS instructed "Before sending, you need to ask your people to open the box, take a picture and send it to me—the part itself, on both sides and the invoice that is attached. To be sure that they sent exactly what we ordered. Throw away the original invoice and DO NOT send it to Germany!" In another message from YERMOLENKO to LIVSHITS on October 29, 2018, an attached invoice from the U.S. branch of a Taiwanese technology conglomerate listed YERMOLENKO as the exporter from a New Jersey address and stated that the item was

controlled by the U.S. Government and authorized for export only to the country of ultimate destination for use by the ultimate consignee or end-user(s) herein identified. They may not be resold, transferred, or otherwise disposed of, to any other country or to any person other than the authorized ultimate consignee or end-user(s), either in their original form or after being incorporated into other items, without first obtaining approval from the U.S. government or as otherwise authorized by U.S. law and regulations.

38. Similarly, in a February 12, 2022 message, the defendant BORIS LIVSHITS asked the defendant ALEXEY BRAYMAN to “take a photo of the contents for me . . . and if there are financial paper there, remove them.” Later, in a March 10, 2022 communication, BRAYMAN and LIVSHITS discussed sending items to Russia through Germany “by hook or by crook.” In another communication on May 10, 2022, BRAYMAN asked LIVSHITS if he needed a “certificate of origin.” LIVSHITS responded, “You have to get rid of this.” BRAYMAN confirmed, “I’m throwing it out.” More recently, in an August 29, 2022 message, LIVSHITS asked BRAYMAN to forge a signature on an invoice, saying “you have to write Tate Olsen and a squiggle, as if it’s a signature.”

39. The defendant VADIM KONOSHCHENOK, while acting under the direction of the defendant BORIS LIVSHITS, shipped or physically smuggled U.S.-origin items from Estonia to Russia, including dual-use electronics and other export-controlled items. For example, on September 21, 2022, the defendant ALEXEY BRAYMAN sent a package from the New Hampshire Residence to “Vadim Konoshchenok” at an address in Tallinn, Estonia. The invoice described the contents as a “Prototype Development Board with Case,” manufactured by a software company in Texas and controlled by the DOC under ECCN 3A992.a.

VI. Financial Transactions in Furtherance of the Scheme

40. The defendant BORIS LIVSHITS established and managed numerous shell companies in the United States, including entities in the Eastern District of New York. Specifically, LIVSHITS used agents and nominees to create fictitious corporate entities and obtain corresponding Employer Identification Numbers (“EIN”) from the Internal Revenue Service (“IRS”). In this manner, LIVSHITS created the following entities, several of which

were incorporated with addresses in the Eastern District of New York: Advanced Web Services LLC; Crossgate LLC; Crosswell LLC; Divatek Trading Inc.; Fennica Networks LLC; FF Networks LLC; JJ Networks LLC; Palmira Networks LLC; Palmira Systems LLC; Speedray Solutions LLC; Strand Networks LLC; Strandaway LLC; Streen LLC; Trailgate Systems LLC; WebForce Communications LLC; and Windwire Technologies LLC.

41. The defendant BORIS LIVSHITS paid agents and nominees to open bank accounts at U.S. financial institutions in the names of these shell companies (the "U.S. Bank Accounts"), including in the Eastern District of New York. LIVSHITS retained control over the shell entities and the corresponding U.S. Bank Accounts for use in the Serniya Network.

42. The defendant VADIM YERMOLENKO obtained EINs and opened numerous U.S. Bank Accounts for multiple shell companies. YERMOLENKO managed the accounts at the direction of the defendant BORIS LIVSHITS, including the following ways:

(a) In or about 2019, YERMOLENKO provided LIVSHITS with YERMOLENKO's spouse's signature to use on IRS documents for company applications and applications to open U.S. Bank Accounts.

(b) In an August 1, 2019 email to LIVSHITS, YERMOLENKO stated, "[W]e need docs for all companies, tomorrow I'm going to open accounts." LIVSHITS responded by sending a list of IRS, state and other official documents for four shell entities, including Strand Networks LLC and Trailgate Systems LLC.

(c) In an email on August 5, 2019, YERMOLENKO provided LIVSHITS with the account names, electronic logins, passwords and answers to the security questions for the bank accounts of five different shell companies, including Strand Networks

LLC and Trailgate Systems LLC. Notably, several invoices exchanged between the defendant YEVGENIY GRININ and other members of the Serniya Network listed Strand Networks LLC as the beneficiary.

(d) In a series of April 2022 emails, LIVSHITS instructed YERMOLENKO as follows: “Here is the document of the new NJ LLC and EIN. You can open an account. Let’s start with [a major U.S. financial institution, hereinafter “Bank 1,” an entity the identity of which is known to the Grand Jury]. If they open an account there, then ask them if it is possible to have an account with access to their CEO Portal, where wire functionality and double custody with 2 RSA tokens . . . and wire limits to at least \$50k/wire and \$200-300k/months.” On April 26, 2022, YERMOLENKO opened an account in the name of “JJ Networks LLC” at a Bank 1 branch in New Jersey. The following day, YERMOLENKO deposited a check for \$44,400.84, and immediately transferred \$9,353 to Strandway LLC, and \$34,000 to Trailgate Systems, LLC—two front companies created and controlled by LIVSHITS—and withdrew the rest of the balance in cash.

(e) In an April 29, 2022 email, LIVSHITS instructed YERMOLENKO, “You need to call, or, which would be better, go to [the bank] – you need to find out why they won’t send the outgoing wire transfer to Iceland from Strand Networks LLC . . . if the bank asks what the payment is for – for bicycle spare parts, sporting goods and textile products.” The email attached an invoice describing the cargo as deep-sea navigation and communications equipment.

(f) In a June 15, 2022 message exchange, LIVSHITS asked the defendant ALEXEY BRAYMAN, “Is it possible for you to send my Wells Fargo token via Fedex to Vadik [YERMOLENKO] in NJ?” After BRAYMAN confirmed, saying “yes, I

can send it. No problem,” LIVSHITS sent YERMOLENKO’s home address and asked BRAYMAN to “send it today.”

43. Another agent (“Co-Conspirator 1”), an individual whose identity is known to the Grand Jury, obtained an EIN from the IRS and opened an account at a bank located in Sheepshead Bay, Brooklyn (“Bank 2”), a financial institution the identity of which is known to the Grand Jury, in the name of Strandway LLC (“the Strandway LLC Account”). The Strandway LLC Account was initially funded by a payment from Advanced Web Services, another entity controlled by the defendant BORIS LIVSHITS. LIVSHITS used funds from the U.S. Bank Accounts to pay for items purchased from the U.S. Companies, as well as other expenses associated with the transactions.

44. The defendants and their co-conspirators used the U.S. Bank Accounts, including the Strandway LLC Account, to receive funding from accounts in various foreign jurisdictions in the names of shell companies used in the Serniya Network, including Majory LLP, Invention Bridge SL and Photon Pro LLP, all of which were added to the SDN List pursuant to OFAC’s March 31, 2022 designation. Funds transferred from accounts in the names of Majory LLP, Invention Bridge SL and Photon Pro LLP into the Strandway LLC Account were often forwarded to and disbursed soon after their receipt—sometimes on the same day—indicating that the defendant BORIS LIVSHITS was acting as an intermediary to disguise the audit trail and obfuscate the origin, purpose and identities of Russian end users. The following transactions involving the Strandway LLC Account at Bank 2 were in furtherance of the scheme:

(a) On September 13, 2018, the Strandway LLC Account received \$43,900 from Majory LLP. Within five days, \$43,295 was disbursed to five different individuals and entities, including other accounts in the defendant BORIS LIVSHITS' name.

(b) On January 4, 2019, the Strandway LLC Account received \$18,300 from Majory LLP. By January 7, 2019, \$18,158 had been disbursed, with one payment to a Florida-based spectroscopy company, and two payments totaling \$8,450 to LIVSHITS. Spectroscopy equipment was heavily regulated by the U.S. government to Russia and other countries due to its potential use in nuclear weapons development.

(c) On July 1, 2019, the Strandway LLC Account received \$39,900 from Majory LLP. Within two days, \$39,650 had been disbursed, with \$26,500 to a technology company specializing in dual-use sonar and hydrophone equipment used for sea navigation and avionics.

(d) On July 31, 2019, the Strandway LLC Account received \$18,550 from Majory LLP. That same day, LIVSHITS sent \$18,500 to a Colorado-based technology and research development company ("U.S. Company 3"), an entity the identity of which is known to the Grand Jury.

(e) On October 6, 2020, Photon Pro LLP sent \$19,810 to LIVSHITS at the Strandway LLC Account.

(f) On October 25, 2019, the Strandway LLC Account received \$67,445 from an Invention Bridge SL account. By November 13, 2019, \$66,700 had been disbursed to various entities, including Web Force Communications, Advanced Web Services LLC and other accounts in the names of LIVSHITS and his agents and nominees.

45. The defendants and their co-conspirators used the U.S. Bank Accounts, including the Strandway LLC Account, to make numerous purchases of dual-use technologies from the U.S. Companies, including payments for oscilloscopes, signal generators, spectroscopy equipment, navigation and avionics components, and other items controlled under the EAR and other U.S. export control regulations. For example, on or about December 12, 2020, the defendant BORIS LIVSHITS initiated a \$9,900 payment from an account held at a U.S. financial technology company in the name of LIVSHITS and the front company Advanced Web Services. According to a supporting document, the payment was for a dual-use oscilloscope controlled by the DOC under ECCN 3A992.a for reasons of anti-terrorism. No export license was applied for or granted for this purchase. Moreover, oscilloscopes typically cost far more than \$9,900. Notably, the IRS maintained a transaction reporting requirement providing that any person who, during trade or business, received more than \$10,000 in a single transaction was required report the transaction to the IRS.

VII. Falsified and Illicit Shipments Through the New Hampshire Residence

46. In furtherance of transactions on behalf of the Serniya Network, the defendant BORIS LIVSHITS and the defendant ALEXEY BRAYMAN repeatedly used the New Hampshire Residence as a transshipment point for repackaging sensitive military-grade and export-controlled items and forwarding them to intermediate locations in Europe and Asia, from where they were transhipped to Russia. In doing so, LIVSHITS and BRAYMAN used the New Hampshire Residence as an address of record for Strandway LLC, and falsely listed Strandway LLC and the New Hampshire Residence as the end users of export-controlled items.

47. For example, on October 22, 2019, the defendant BORIS LIVSHITS emailed the defendant ALEXEY BRAYMAN: “[T]wo large boxes need to be sent . . . to Germany . . . It is necessary to cut off all old labels and remove all invoices and packing lists from the boxes that came with them originally. Leave manuals and other technical documentation.” LIVSHITS attached shipping labels for a freight company in Hamburg, Germany, as well as numerous falsified invoices and end use statements. One invoice documented that U.S. Company 3 purportedly sent a “Low Noise Cesium Frequency Synthesizer,” valued at \$44,965, to “Strandway LLC Attn: David Wetsky” at the New Hampshire Residence. The “End Use Statement” listed “Strandway LLC,” the New Hampshire Residence, the contact name “David Wetsky,” and a contact email address “david.wetzky[[@](mailto:david.wetzky@awsresearch.net)]awsresearch.net,” along with the advisory, “[e]xport of these products is subject to the United States Government Export Administration Regulations (EAR).” As described above, Strandway LLC and Advanced Web Services LLC were front companies used by LIVSHITS and the Serniya Network, and “David Wetsky” was a pseudonym used by LIVSHITS in furtherance of the scheme.

48. In July 2022, the defendant BORIS LIVSHITS attempted to purchase for \$15,564 a 3 GHz signal generator, controlled by the DOC under ECCN 3A992.a for reasons of anti-terrorism, from an Illinois-based test equipment company (“U.S. Company 4”), an entity the identity of which is known to the Grand Jury. In an email dated July 25, 2022, LIVSHITS requested that an employee at U.S. Company 4 “please ship the generator to our NH address” for “Strandway LLC,” and provided the address of the New Hampshire Residence. LIVSHITS also provided U.S. Company 4 with a pro forma invoice and a Form BIS-711 (“Statement by Ultimate Consignee and Purchaser”)—an end use statement filed

with the DOC—falsely listing Strandway LLC at the New Hampshire Residence as the “ultimate consignee and purchaser.” The BIS-711 was signed by the defendant VADIM YERMOLENKO, who was listed as the “Director” of Strandway LLC, and certified that the signal generator would not be “reexported or incorporated into an end product.”

49. The defendant ALEXEY BRAYMAN made at least four shipments of sensitive electronic test equipment and other dual-use items from the New Hampshire Residence to Russia after March 31, 2022, after Sertal, Serniya and the defendant YEVGENIY GRININ were added to the SDN list. These deliveries contained oscilloscopes, signal generators and multimeters, and included the manufacturer and part number information, which reflected that they were all controlled by the DOC under ECCN 3A992.a. The shipments from the New Hampshire Address to a transshipment location in Hamburg, Germany used by the Serniya Network were as follows:

- (a) A multimeter on or about April 15, 2022;
- (b) An oscilloscope probe on or about April 15, 2022;
- (c) An oscilloscope on or about on May 6, 2022; and
- (d) A signal generator on or about May 10, 2022.

VIII. The Purchase of Sensitive Testing Equipment

50. In or about and between September 2019 and December 2020, the defendants YEVGENIY GRININ, ALEKSEY IPPOLITOV, BORIS LIVSHITS and SVETLANA SKVORTSOVA unlawfully purchased sophisticated testing equipment from a California-based laboratory device and components manufacturer (“U.S. Company 5”), an entity the identity of which is known to the Grand Jury. The defendants ultimately delivered

the items to a Russian end user, using the defendant ALEXEY BRAYMAN to transship the items through the New Hampshire Residence.

51. On or about September 4, 2019, the defendant ALEXEY IPPOLITOV emailed the defendant YEVGENIY GRININ and another Serniya employee “urgently” requesting prices for several military-grade U.S.-origin items, including an analog signal generator, a spectrum analyzer, an electromagnetic simulation solver and spectral and pulse measurement devices. GRININ then sent an email to the defendant SVETLANA SKVORTSOVA, with the message “let’s break it down into parts” and suggested finding specific prices for each item.

52. In or about July 2020, the defendant SVETLANA SKVORTSOVA sent an email to the defendant BORIS LIVSHITS requesting certain parts from U.S. Company 5. After LIVSHITS provided price quotes, SKVORTSOVA forwarded the quotes to the defendant YEVGENIY GRININ. On September 20, 2020, SKVORTSOVA instructed LIVSHITS to bill the front company Photon Pro LLP for the items.

53. Packages pertaining to this shipment were then sent from U.S. Company 5 to the defendant ALEXEY BRAYMAN at the New Hampshire Residence, with shipping forms for each package falsely reflecting merchandise valued only at \$2,640. However, the purchase prices each exceeded \$15,000. These packages were then forwarded by BRAYMAN to a transshipping point in Germany.

54. On November 10, 2020, the defendant YEVGENIY GRININ emailed the defendant ALEKSEY IPPOLITOV the invoice for the order, along with shipping labels reflecting the packages’ transshipment from Germany to GRININ in Russia. On or about December 9, 2020, the defendant SVETLANA SKVORTSOVA emailed GRININ and

informed him that the items had been received in Russia by the end user, a major Russian university and scientific research facility that collaborated with Russia's defense sector on research and development projects.

IX. The Purchase of a Military-Grade Spectrum Analyzer

55. In or about and between February 2022 and April 2022, the defendants YEVGENIY GRININ, ALEKSEY IPPOLITOV, BORIS LIVSHITS and SVETLANA SKVORTSOVA unlawfully purchased a military-grade spectrum analyzer from a Florida-based electronics company ("U.S. Company 6"), an entity the identity of which is known to the Grand Jury.

56. On February 18, 2022, the defendant BORIS LIVSHITS emailed an account executive at U.S. Company 6 and inquired about purchasing a military-grade spectrum analyzer, which could be used to measure electromagnetic signals on the battlefield or for countersurveillance operations and that was controlled by the DOC under ECCN 3A992.a for reasons of anti-terrorism. LIVSHITS purchased the item for \$14,065 and it was shipped to Strandway LLC and the defendant ALEXEY BRAYMAN at the New Hampshire Residence.

57. In an email exchange occurring on or about March 6, 2022 and March 7, 2022, the defendant BORIS LIVSHITS attempted to have a Hong Kong-based freight forwarder send the item to Russia, saying, "I have a logistics task. I need to ship [the spectrum analyzer] with DHL from US to Hong Kong to any company, which can receive it and then ship it via Emirate or Turkish air cargo to Russia – St. Petersburg or Moscow. Can you do this?" The freight forwarder refused LIVSHITS' request, citing the portfolio of international sanctions imposed on Russia after the invasion of Ukraine.

58. On March 9, 2022, the defendant BORIS LIVSHITS sent the defendant ALEXEY BRAYMAN shipping labels and other documents, directing that the spectrum analyzer be sent from the New Hampshire Residence to a location in Hamburg, Germany used by the Serniya Network as a transshipment point. Notably, the certificate of origin falsely claimed that the item originated in Malaysia, rather than in the United States.

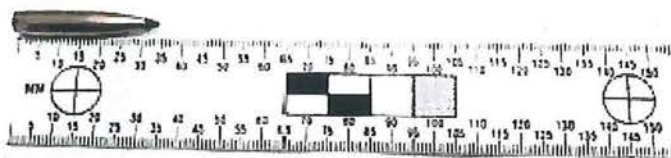
59. In an email exchange between the defendant BORIS LIVSHITS and an employee of U.S. Company 6 occurring on or about and between April 25, 2022 and April 27, 2022, LIVSHITS acknowledged that the spectrum analyzer was ultimately shipped to Russia—"I've finally received the [spectrum analyzer] I purchased from you in February, here in Russia"—and then complained that the device was not properly calibrated. The U.S. Company 6 employee responded, "because of the sanctions and restrictions and our position in this industry and our contracts, I have been strongly cautioned not to speak with you anymore or have any dealings with your associates in the US." LIVSHITS replied, "regarding sanctions, I've purchased this unit from you not as myself, but as a US company, with US shipping address. Hence this transaction has nothing to do with Russian-related sanctions."

X. The Attempts to Smuggle Electronics and Ammunition from Estonia

60. On October 27, 2022, the defendant VADIM KONOSHCHENOK was stopped by police and border guard officers in Narva, Estonia, where he was attempting to cross from Estonia into Russia. Inside of KONOSHCHENOK's vehicle were approximately 35 different types of semiconductors and other electronic components, several of which were of U.S.-origin and controlled by the DOC under ECCN 3A992.a for

reasons of anti-terrorism. One of the items had been purchased by the defendant BORIS LIVSHITS and shipped to KONOSHCHENOK on October 18, 2022.

61. Also secreted in KONOSHCHENOK's vehicle were thousands of 6.5mm bullets manufactured by a Nebraska-based firearms components and manufacturing company. The bullets were suitable for a sniper rifle and controlled under ECCN 0A505.x. According to the Form BIS-711 documents filed with the DOC in accordance with the export of the sniper rounds, these bullets had ostensibly been sold to Germany, Finland, Luxembourg and Latvia but did not disclose their ultimate re-export to Russia. Photographs depicting some of the seized bullets are below:



62. On November 24, 2022, the defendant VADIM KONOSHCHENOK was again stopped by police and border guard officers in Narva, Estonia, where he was attempting to cross from Estonia into Russia. Inside of KONOSHCHENOK's vehicle were approximately twenty cases of U.S.-origin bullets controlled under ECCN 0A505.x, including tactical bullets and .338 military sniper rounds.

COUNT ONE

(Conspiracy to Defraud the United States)

63. The allegations contained in paragraphs one through 62 are realleged and incorporated as if fully set forth in this paragraph.

64. In or about and between January 2017 and December 2022, both dates being approximate and inclusive, within the Eastern District of New York and elsewhere, the defendants YEVGENIY GRININ, ALEKSEY IPPOLITOV, BORIS LIVSHITS SVETLANA SKVORTSOVA, VADIM KONOSHCHENOK, ALEXEY BRAYMAN and VADIM YERMOLENKO, together with others, did knowingly and intentionally conspire to defraud the United States by impairing, impeding, obstructing and defeating, through deceitful and dishonest means, the lawful functions of OFAC and BIS, both agencies of the United States, in the enforcement of economic sanctions laws and regulations, and the issuance of licenses relating to export of goods and the provision of financial services.

65. In furtherance of the conspiracy and to affect its objects, within the Eastern District of New York and elsewhere, the defendants YEVGENIY GRININ, ALEKSEY IPPOLITOV, BORIS LIVSHITS, SVETLANA SKVORTSOVA, VADIM KONOSHCHENOK, ALEXEY BRAYMAN and VADIM YERMOLENKO, together with others, committed and caused to be committed, among others, the following:

OVERT ACTS

(a) On or about May 25, 2018, IPPOLITOV emailed GRININ a list of items to be procured for the National Research Nuclear University of the Moscow Engineering Physics Institute.

(b) On or about September 4, 2019, IPPOLITOV emailed GRININ about obtaining a “chip set” of 45 advanced semiconductors and other items from U.S. Company 1.

(c) On or about September 6, 2019, GRININ and SKVORTSOVA contacted LIVSHITS and requested a price quote for semiconductors and other comparable items from U.S. Company 1 and other U.S. Companies.

(d) On or about July 20, 2020, IPPOLITOV, GRININ and SKVORTSOVA received an email from an SVR official regarding an order.

(e) On or about September 20, 2020, SKVORTSOVA instructed LIVSHITS to bill Photon Pro LLP, a company controlled by GRININ, for items to be purchased from U.S. Company 5.

(f) On or about October 6, 2020, Photon Pro LLP, a company controlled by GRININ, sent \$19,810 to the Strandway LLC Account, controlled by LIVSHITS.

(g) On or about November 10, 2020, GRININ emailed IPPOLITOV invoices and shipping labels.

(h) On or about December 12, 2020, LIVSHITS initiated a \$9,900 payment from the Strandway LLC Account for an oscilloscope controlled under ECCN 3A992.a for reasons of anti-terrorism.

(i) On or about February 8, 2022, LIVSHITS purchased a spectrum analyzer from U.S. Company 6 for \$14,065.

(j) On or about March 9, 2022, LIVSHITS sent BRAYMAN shipping labels, a certificate of origin and other falsified documents regarding a spectrum analyzer from U.S. Company 6 and directed BRAYMAN to send the spectrum analyzer to a location in Hamburg, Germany.

(k) On or about April 26, 2022, YERMOLENKO opened an account in the name of "JJ Networks LLC" at a Bank 1 branch in New Jersey.

(l) On or about April 27, 2022, YERMOLENKO deposited a check for \$44,400.84 into an account in the name of "JJ Networks LLC" at a Bank 1 branch in New Jersey and immediately thereafter transferred \$9,353 to Strandway LLC and \$34,000 to Trailgate Systems, LLC, before withdrawing of the remaining balance in cash.

(m) On or about July 26, 2022, LIVSHITS provided a pro forma invoice and a Form BIS-711 containing false information to U.S. Company 4.

(n) On or about September 21, 2022, BRAYMAN sent a "Prototype Development Board with Case," which was controlled under ECCN 3A992.a, to KONOSHCHENOK in Estonia.

(o) On or about October 27, 2022, KONOSHCHENOK attempted to transport U.S.-origin electronic components controlled under ECCN 3A992.a and bullets controlled under ECCN 0A505.x from Estonia to Russia.

(Title 18, United States Code, Sections 371 and 3551 et seq.)

COUNT TWO
(Conspiracy to Violate IEEPA)

66. The allegations contained in paragraphs one through 62 are realleged and incorporated as if fully set forth in this paragraph.

67. On or about and between March 31, 2022 and December 2022, both dates being approximate and inclusive, within the Eastern District of New York and elsewhere, the defendants YEVGENIY GRININ, ALEKSEY IPPOLITOV, BORIS LIVSHITS and SVETLANA SKVORTSOVA, together with others, did knowingly and willfully conspire to violate the IEEPA, contrary to 50 U.S.C. § 1705, Executive Order 13848 and 31 C.F.R. §§ 579.203-204.

68. It was a part and an object of the conspiracy that the defendants YEVGENIY GRININ, ALEKSEY IPPOLITOV, BORIS LIVSHITS and SVETLANA SKVORTSOVA, together with others, knowingly and willfully violated the IEEPA, and the regulations promulgated thereunder, to wit: GRININ, IPPOLITOV, LIVSHITS, SKVORTSOVA, and their co-conspirators knowingly and willfully caused U.S. persons, entities and financial institutions to provide funds, goods and services to and for the benefit of Serniya and Sertal, and caused U.S. persons, entities and financial institutions to receive funds, goods and services from Serniya and Sertal without first obtaining the required approval of OFAC, contrary to Executive Order 13692 and 31 C.F.R. §§ 591.101, 591.201-591.202.

(Title 50, United States Code, Sections 1705(a) and 1705(c); Title 18, United States Code, Sections 3551 et seq.)

COUNT THREE
(Bank Fraud Conspiracy)

69. The allegations contained in paragraphs one through 62 are realleged and incorporated as if fully set forth in this paragraph.

70. In or about and between January 2017 and September 2022, both dates being approximate and inclusive, within the Eastern District of New York and elsewhere, the defendants YEVGENIY GRININ, ALEKSEY IPPOLITOV, BORIS LIVSHITS, SVETLANA SKVORTSOVA, ALEXEY BRAYMAN and VADIM YERMOLENKO, together with others, did knowingly and intentionally conspire to execute a scheme and artifice to defraud one or more financial institutions, to wit: Bank 1, Bank 2, Bank 3 and Bank 4, entities the identities of which are known to the Grand Jury, contrary to Title 18, United States Code, Section 1344(1).

(Title 18, United States Code, Sections 1349 and 3551 et seq.)

COUNT FOUR
(Wire Fraud Conspiracy)

71. The allegations contained in paragraphs one through 62 are realleged and incorporated as if fully set forth in this paragraph.

72. In or about and between January 2017 and December 2022, both dates being approximate and inclusive, within the Eastern District of New York and elsewhere, the defendants YEVGENIY GRININ, ALEKSEY IPPOLITOV, BORIS LIVSHITS, SVETLANA SKVORTSOVA, ALEXEY BRAYMAN and VADIM YERMOLENKO, together with others, did knowingly and intentionally conspire to devise a scheme and artifice to defraud one or more U.S. companies, to wit: U.S. Company 1, U.S. Company 2, U.S. Company 3, U.S. Company 4, U.S. Company 5 and U.S. Company 6, by means of one

or more materially false and fraudulent pretenses, representations and promises, and for the purpose of executing such scheme and artifice, to transmit and cause to be transmitted by means of wire communication in interstate and foreign commerce, writings, signs, signals, pictures and sounds, to wit: electronic communications, emails and other online communications and monetary transfers in and through the Eastern District of New York and elsewhere, contrary to Title 18, United States Code, Section 1343.

(Title 18, United States Code, Sections 1349 and 3551 et seq.)

COUNTS FIVE THROUGH EIGHT

(Wire Fraud)

73. The allegations contained in paragraphs one through 62 are realleged and incorporated as if fully set forth in this paragraph.

74. On or about the dates set forth below, all dates being approximate and inclusive, within the Eastern District of New York and elsewhere, the defendants YEVGENIY GRININ, ALEKSEY IPPOLITOV, BORIS LIVSHITS and SVETLANA SKVORTSOVA, together with others, did knowingly and intentionally devise a scheme and artifice to defraud one or more U.S. companies to wit: U.S. Company 1, U.S. Company 2, U.S. Company 3, U.S. Company 4, U.S. Company 5 and U.S. Company 6, and to obtain money and property from said companies and financial institutions by means of materially false and fraudulent pretenses, representations and promises, and, for the purpose of executing such scheme and artifice, transmitted and caused to be transmitted one or more writings, signs, signals, pictures and sounds by means of wire communication in interstate and foreign commerce, to wit: the wire transmissions set forth below:

Count	Approximate Date of Wire Transmission	Description of Wire Transmission
FIVE	September 13, 2018	\$43,900 wire transfer from a Majory LLP account in the United Kingdom to the Strandway LLC Account in the Eastern District of New York
SIX	July 1, 2019	\$39,900 wire transfer from a Majory LLP account in the United Kingdom to the Strandway LLC Account in the Eastern District of New York
SEVEN	October 16, 2019	\$12,830 wire transfer from the Strandway LLC account in the Eastern District of New York to U.S. Company 3
EIGHT	October 7, 2020	\$14,344 wire transfer from the Strandway LLC account in the Eastern District of New York to U.S. Company 5

(Title 18, United States Code, Sections 1343 and 3551 et seq.)

COUNT NINE

(Money Laundering Conspiracy)

75. The allegations contained in paragraphs one through 62 are realleged and incorporated as if fully set forth in this paragraph.

76. In or about and between January 2017 and December 2022, both dates being approximate and inclusive, within the Eastern District of New York and elsewhere, the defendants YEVGENIY GRININ, ALEKSEY IPPOLITOV, BORIS LIVSHITS, SVETLANA SKVORTSOVA, ALEXEY BRAYMAN and VADIM YERMOLENKO, together with others, did knowingly and intentionally conspire to:

(a) transport, transmit and transfer monetary instruments and funds from one or more places in the United States to and through one or more places outside the United States and to one or more places in the United States from and through one or more places outside the United States, (i) with the intent to promote the carrying on of one or more specified unlawful activities, to wit: conspiracy to violate IEEPA, conspiracy to commit wire

fraud and wire fraud as charged in Counts Two and Four through Eight, all contrary to Title 18, United States Code, Section 1956(a)(2)(A); and (ii) which transactions in fact involved the proceeds of unlawful activity, to wit: conspiracy to violate IEEPA, conspiracy to commit wire fraud and wire fraud as charged in Counts Two and Four through Eight, knowing that the monetary instruments and funds involved in the transportation, transmission and transfer represented the proceeds of said unlawful activity, and knowing that such transportation, transmission and transfer was designed in whole and in part to conceal and disguise the nature, the location, the source, the ownership and the control of the proceeds of said specified unlawful activity, all contrary to Title 18, United States Code, Section 1956(a)(2)(B)(i); and

(b) engage in one or more monetary transactions within the United States in criminally derived property of a value greater than \$10,000 that was derived from one or more specified unlawful activities, to wit: conspiracy to violate IEEPA, conspiracy to commit wire fraud, and wire fraud as charged in Counts Two and Four through Eight, all contrary to Title 18, United States Code, Section 1957(a).

(Title 18, United States Code, Sections 1956(h) and 3551 et seq.)

COUNTS TEN THROUGH THIRTEEN
(Money Laundering)

77. The allegations contained in paragraphs one through 62 are realleged and incorporated as if fully set forth in this paragraph.

78. On or about and between the dates set forth below, all dates being approximate and inclusive, within the Eastern District of New York and elsewhere, the defendants YEVGENIY GRININ, ALEKSEY IPPOLITOV, BORIS LIVSHITS and

SVETLANA SKVORTSOVA, together with others, did knowingly and intentionally engage in monetary transactions, in and affecting interstate and foreign commerce, in criminally derived property that was of a value greater than \$10,000, in the approximate amounts set forth below, and that was derived from one or more specified unlawful activities, to wit: conspiracy to violate IEEPA, conspiracy to commit wire fraud and wire fraud as charged in Counts Two and Four through Eight:

Count	Approximate Date	Description of Wire Transmission
TEN	January 4, 2019	\$18,300 wire transfer from a Majory LLP account in the United Kingdom to the Strandway LLC Account in the Eastern District of New York
ELEVEN	July 31, 2019	\$18,550 wire transfer from a Majory LLP account in the United Kingdom to the Strandway LLC Account in the Eastern District of New York
TWELVE	October 25, 2019	\$67,445 wire transfer from an Invention Bridge SL account in Spain to the Strandway LLC Account in the Eastern District of New York
THIRTEEN	October 6, 2020	\$22,632 wire transfer from a Photon Pro LLP account in Austria to the Strandway LLC Account in the Eastern District of New York

(Title 18, United States Code, Sections 1957(a), 1957(b), 1957(d)(1), 2 and 3551 et seq.)

COUNT FOURTEEN
(Conspiracy to Violate ECRA)

79. The allegations contained in paragraphs one through 62 are realleged and incorporated as if fully set forth in this paragraph.

80. In or about and between August 13, 2018 and December 2022, both dates being approximate and inclusive, within the Eastern District of New York and elsewhere, the defendants YEVGENIY GRININ, ALEKSEY IPPOLITOV, BORIS

LIVSHITS, SVETLANA SKVORTSOVA, VADIM KONOSHCHENOK, ALEXEY BRAYMAN and VADIM YERMOLENKO, together with others, did knowingly and willfully conspire to violate and to cause one or more violations of licenses, orders, regulations and prohibitions issued under the Export Control Reform Act.

81. It was a part and an object of the conspiracy that the defendants YEVGENIY GRININ, ALEKSEY IPPOLITOV, BORIS LIVSHITS, SVETLANA SKVORTSOVA, VADIM KONOSHCHENOK, ALEXEY BRAYMAN and VADIM YERMOLENKO together with others, would and did agree to export and cause to be exported from the United States to Russia items on the Commerce Control List set forth in Title 15, Code of Federal Regulations, part 774, Supplement Number 1, without having first obtained a license for such export from the U.S. Department of Commerce.

(Title 50, United States Code, Sections 4819(a)(1), 4819(a)(2)(A)-(G) and 4819(b); and Title 15, Code of Federal Regulations, Sections 736.2(b)(1) and 746.8(a)(1))

COUNT FIFTEEN

(Smuggling Goods from the United States)

82. The allegations contained in paragraphs one through 62 are realleged and incorporated as if fully set forth in this paragraph.

83. In or about and between January 2017 and December 2022, both dates being approximate and inclusive, within the Eastern District of New York and elsewhere, the defendants YEVGENIY GRININ, ALEKSEY IPPOLITOV, BORIS LIVSHITS, SVETLANA SKVORTSOVA, VADIM KONOSHCHENOK, ALEXEY BRAYMAN and VADIM YERMOLENKO, together with others, did knowingly and fraudulently export and send from the United States, merchandise, articles and objects, to wit: items on the

Commerce Control List set forth in Title 15, Code of Federal Regulations, part 774, Supplement Number 1, contrary to United States laws and regulations, to wit: Title 50, United States Code, Section 4819(a)(1), 4819(a)(2)(A)-(G) and 4819(b) and Title 15, C.F.R. §§ 736.2 and 746.8(a)(1), and did fraudulently and knowingly receive, conceal and facilitate the transportation and concealment of such merchandise, articles and objects, prior to exportation, knowing the same to be intended for exportation contrary to such United States laws and regulations.

(Title 18, United States Code, Section 554(a), 2 and 3551 et seq.)

COUNT SIXTEEN

(Failure to File Electronic Export Information)

84. The allegations contained in paragraphs one through 62 are realleged and incorporated as if fully set forth in this paragraph.

85. In or about and between January 2017 and December 2022, both dates being approximate and inclusive, within the Eastern District of New York and elsewhere, the defendants YEVGENIY GRININ, ALEKSEY IPPOLITOV, BORIS LIVSHITS and SVETLANA SKVORTSOVA, together with others, did knowingly and willfully fail to file and cause the failure to file electronic export information through the Automated Export System relating to the transportation of electronic items and devices that had a value of more than \$2,500 from the United States to the Russian Federation.

(Title 13, United States Code, Section 305(a)(1); Title 18, United States Code, Sections 2 and 3551 et seq.)

CRIMINAL FORFEITURE ALLEGATION
AS TO COUNTS TWO AND FIFTEEN

86. The United States hereby gives notice to the defendants that, upon their conviction of either of the offenses charged in Counts Two and Fifteen, the government will seek forfeiture in accordance with Title 18, United States Code, Section 981(a)(1)(C) and Title 28, United States Code, Section 2461(c), which require any person convicted of such offenses to forfeit any property, real or personal, constituting, or derived from, proceeds traceable to such offenses.

87. If any of the above-described forfeitable property, as a result of any act or omission of the defendants:

- (a) cannot be located upon the exercise of due diligence;
- (b) has been transferred or sold to, or deposited with, a third party;
- (c) has been placed beyond the jurisdiction of the court;
- (d) has been substantially diminished in value; or
- (e) has been commingled with other property which cannot be divided without difficulty;

it is the intent of the United States, pursuant to Title 21, United States Code, Section 853(p), to seek forfeiture of any other property of the defendants up to the value of the forfeitable property described in this forfeiture allegation.

(Title 18, United States Code, Section 981(a)(1)(C); Title 21, United States Code, Section 853(p); Title 28, United States Code, Section 2461(c))

CRIMINAL FORFEITURE ALLEGATION
AS TO COUNTS THREE THROUGH EIGHT

88. The United States hereby gives notice to the defendants that, upon their conviction of any of the offenses charged in Counts Three through Eight, the government will seek forfeiture in accordance with: (a) Title 18, United States Code, Section 981(a)(1)(C) and Title 28, United States Code, Section 2461(c), which require any person convicted of such offense to forfeit any property, real or personal, which constitutes or is derived from proceeds traceable to such offenses; and/or (b) Title 18, United States Code, Section 982(a)(2), which requires any person convicted of such offenses to forfeit any property constituting, or derived from, proceeds obtained directly or indirectly as a result of such offenses.

89. If any of the above-described forfeitable property, as a result of any act or omission of the defendants:

- (a) cannot be located upon the exercise of due diligence;
- (b) has been transferred or sold to, or deposited with, a third party;
- (c) has been placed beyond the jurisdiction of the court;
- (d) has been substantially diminished in value; or
- (e) has been commingled with other property which cannot be divided without difficulty;

it is the intent of the United States, pursuant to Title 21, United States Code, Section 853(p),

to seek forfeiture of any other property of the defendants up to the value of the forfeitable property described in this forfeiture allegation.

(Title 18, United States Code, Sections 981(a)(1)(C) and 982(a)(2); Title 21, United States Code, Section 853(p); Title 28, United States Code, Section 2461(c))

**CRIMINAL FORFEITURE ALLEGATION
AS TO COUNTS NINE THROUGH THIRTEEN**

90. The United States hereby gives notice to the defendants that, upon their conviction of any of the offenses charged in Counts Nine through Thirteen, the government will seek forfeiture in accordance with Title 18, United States Code, Section 982(a)(1), which requires any person convicted of such offenses to forfeit any property, real or personal, involved in such offenses, or any property traceable to such property.

91. If any of the above-described forfeitable property, as a result of any act or omission of the defendants:

- (a) cannot be located upon the exercise of due diligence;
- (b) has been transferred or sold to, or deposited with, a third party;
- (c) has been placed beyond the jurisdiction of the court;
- (d) has been substantially diminished in value; or
- (e) has been commingled with other property which cannot be

divided without difficulty;

it is the intent of the United States, pursuant to Title 21, United States Code, Section 853(p), as incorporated by Title 18, United States Code, Section 982(b)(1), to seek forfeiture of any

other property of the defendants up to the value of the forfeitable property described in this forfeiture allegation.

(Title 18, United States Code, Sections 982(a)(1) and 982(b)(1); Title 21, United States Code, Section 853(p))

CRIMINAL FORFEITURE ALLEGATION
AS TO COUNT FOURTEEN

92. The United States hereby gives notice to the defendants that, upon their conviction of the offense charged in Count Fourteen, the government will seek forfeiture in accordance with Title 50, United States Code, Section 4819(d)(1), which requires any person convicted of such offense to forfeit any of the person's property (a) used or intended to be used, in any manner, to commit or facilitate the offense; (b) constituting or traceable to the gross proceeds taken, obtained or retained, in connection with or as a result of the offense; and/or (c) constituting an item or technology that was exported or intended to be exported in violation of the Export Control Reform Act.

93. If any of the above-described forfeitable property, as a result of any act or omission of the defendants:

- (a) cannot be located upon the exercise of due diligence;
- (b) has been transferred or sold to, or deposited with, a third party;
- (c) has been placed beyond the jurisdiction of the court;
- (d) has been substantially diminished in value; or
- (e) has been commingled with other property which cannot be divided without difficulty;

it is the intent of the United States, pursuant to Title 21, United States Code, Section 853(p), as incorporated by Title 50, United States Code, Section 4819(d)(2), to seek forfeiture of any other property of the defendants up to the value of the forfeitable property described in this forfeiture allegation.

(Title 50, United States Code, Sections 4819(d)(1) and 4819(d)(2); Title 21, United States Code, Section 853(p))

CRIMINAL FORFEITURE ALLEGATION
AS TO COUNT SIXTEEN

94. The United States hereby gives notice to the defendants that, upon their conviction of the offense charged in Count Sixteen, the government will seek forfeiture in accordance with Title 13, United States Code, Section 305, which requires any person convicted of such offense to forfeit any of the person's (a) interest in, security of, claim against, or property or contractual rights of any kind in the goods or tangible items that were the subject of the violation; (b) interest in, security of, claim against, or property or contractual rights of any kind in tangible property that was used in the export or attempt to export that was the subject of the violation; and/or (c) property constituting, or derived from, any proceeds obtained directly or indirectly as a result of the violation.

95. If any of the above-described forfeitable property, as a result of any act or omission of the defendants:


- (a) cannot be located upon the exercise of due diligence;
- (b) has been transferred or sold to, or deposited with, a third party;
- (c) has been placed beyond the jurisdiction of the court;
- (d) has been substantially diminished in value; or

(e) has been commingled with other property which cannot be divided without difficulty;
it is the intent of the United States, pursuant to Title 21, United States Code, Section 853(p), to seek forfeiture of any other property of the defendants up to the value of the forfeitable property described in this forfeiture allegation.

(Title 13, United States Code, Section 305; Title 21, United States Code, Section 853(p))

A TRUE BILL


FOREPERSON


BREON PEACE
UNITED STATES ATTORNEY
EASTERN DISTRICT OF NEW YORK

No. 22-CR-409 (S-1) (HG)

UNITED STATES DISTRICT COURT

EASTERN *District of* NEW YORK

CRIMINAL DIVISION

THE UNITED STATES OF AMERICA

vs.

YEVGENIY GRININ, ALEKSEY IPPOLITOV, BORIS LIVSHITS, SVETLANA SKVORTSOVA, VADIM
KONOSHCHENOK, ALEXEY BRAYMAN and VADIM YERMOLENKO.

Defendants.

SUPERSEDING INDICTMENT

(T. 13, U.S.C., § 305(a)(1); T. 18, U.S.C., §§ 371, 554, 981(a)(1)(C), 982(a)(1), 982(a)(2), 982(b)(1), 1343, 1349, 1956(h),
1957(a), 1957(b), 1957(d)(1), 2 and 3551 et seq.; T. 21, U.S.C., § 853(p); T. 28, U.S.C., § 2461(c); T. 50, U.S.C., §§
4819(a)(1), 4819(a)(2)(A)-(G), 4819(b), 4819(d)(1), 4819(d)(2), 1705(a) and 1705(c); T. 15, C.F.R., §§ 736.2(b)(1) and
746.8(a)(1))

A true bill.

Foreperson

Filed in open court this _____ day,

of _____ A.D. 20 _____

Clerk

Bail, \$ _____

Artie McConnell, Assistant U.S. Attorney (718) 254-7150

DMP:JAM/CRH/MS/SAC
F. #2019R01707

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK

----- X

UNITED STATES OF AMERICA

- against -

ILYA KAHN,

Defendant.

----- X

AFFIDAVIT AND
COMPLAINT IN SUPPORT
OF AN APPLICATION FOR
AN ARREST WARRANT

(T. 50, U.S.C., §§ 4819(a)(1),
4819(a)(2)(A)-(G) and 4819(b); T. 15,
C.F.R., §§ 736.2(b)(1), 736.2(b)(5),
744.10(a) and 746.8(a)(1))

No. 23-MJ-1133

EASTERN DISTRICT OF NEW YORK, SS:

Nicholas Milan, being duly sworn, deposes and states that he is a Special Agent with the Federal Bureau of Investigation, duly appointed according to law and acting as such:

Conspiracy to Violate the Export Control Reform Act

In or about and between March 2018 and December 2023, both dates being approximate and inclusive, within the Eastern District of New York and elsewhere, the defendant ILYA KAHN, together with others, did knowingly and willfully conspire to violate and to cause one or more violations of licenses, orders, regulations and prohibitions issued under the Export Control Reform Act, Title 50, United States Code, Section 4811 et seq., to wit: (a) KAHN, together with others, did agree to export and reexport and cause to be exported and reexported from the United States to Russia, including through Hong Kong and other locations, items on the Commerce Control List set forth in Title 15, Code of Federal Regulations, Part 774, Supplement Number 1, without having first obtained a license for such export from the U.S. Department of Commerce,

and (b) KAHN, together with others, did agree to export and reexport and cause to be exported and reexported from the United States to a prohibited end user, Joint Stock Company Research and Development Center ELVEES, which was added to the Entity List, set forth in Title 15, Code of Federal Regulations, Part 774, Supplement Number 4, on or about March 9, 2022, items subject to the Export Administration Regulations, without having first obtained a license for such export from the U.S. Department of Commerce.

(Title 50, United States Code, Sections 4819(a)(1), 4819(a)(2)(A)-(G) and 4819(b); and Title 15, Code of Federal Regulations, Sections 736.2(b)(1), 736.2(b)(5), 744.10(a) and 746.8(a)(1))

The source of your deponent's information and the grounds for his belief are as follows:¹

INTRODUCTION AND AGENT BACKGROUND

1. I am a Special Agent with the Federal Bureau of Investigation ("FBI"), and have been since 2018. I am currently assigned to investigate export control violations and espionage by foreign governments and related criminal and counterintelligence activity. Through my training, education and experience, I am familiar with the techniques and methods of operation used by individuals involved in intelligence and criminal activities to conceal their behavior from detection by law enforcement authorities. I have participated in numerous investigations, during the course of which I have conducted physical and electronic surveillance, interviewed witnesses, examined

¹ Because the purpose of this complaint is to set forth only those facts necessary to establish probable cause to arrest, I have not described all the relevant facts and circumstances of which I am aware.

financial records, executed court-authorized search warrants and used other techniques to secure relevant information.

2. I am familiar with facts and circumstances set forth below from my participation in the investigation, from my review of documents obtained pursuant to the investigation and from reports of other law enforcement officers involved in the investigation. When I rely on statements made by others, such statements are set forth only in part and in substance unless otherwise indicated. All translations in this affidavit are preliminary drafts and subject to revision.

RELEVANT STATUTORY AND REGULATORY BACKGROUND

3. The Export Administration Regulations (“EAR”), 15 C.F.R. Parts 730-774, were promulgated by the U.S. Department of Commerce (“DOC”), Bureau of Industry and Security (“BIS”), to regulate the export of goods, technology and software from the United States. Under the Export Control Reform Act (“ECRA”), it is a crime to violate, attempt to violate, conspire to violate or cause a violation of any regulation, order, license or authorization issued pursuant to the statute, including the EAR. See 50 U.S.C. § 4819(a)(1). Willful violations of the EAR constitute criminal offenses under the ECRA. See 50 U.S.C. § 4819(b).

4. Through the EAR, the BIS reviews and controls the export of certain U.S. items from the United States to foreign destinations. See 15 C.F.R. §§ 734.2-734.3. In particular, the BIS has placed restrictions on the export and reexport of items that it has determined could make a significant contribution to the military potential or nuclear proliferation of other nations or that could be detrimental to the foreign policy or national security of the United States. Under the EAR, such restrictions depend on several factors, including the technical characteristics of the item, the destination country, the end user and the end use.

5. The most sensitive items subject to the EAR controls are identified on the Commerce Control List (“CCL”), set forth in Title 15, Code of Federal Regulations, Part 774, Supplement Number 1. Items listed on the CCL are categorized by Export Control Classification Number (“ECCN”), each of which is subject to export control requirements depending on destination, end use and end user.

6. In response to Russia’s invasion of Ukraine on February 24, 2022, the DOC imposed new license requirements on exports to Russia. As of February 24, 2022, any item classified under any ECCN in Categories 3 through 9 of the CCL requires a license to be exported to Russia. See 87 Fed. Reg. 12226 (Mar. 3, 2022). As of April 8, 2022, all items on the CCL require a license to export to Russia. See 87 Fed. Reg. 22130 (Apr. 14, 2022). These rules were codified in Title 15, Code of Federal Regulations, Section 746.8, which states, in relevant part, “a license is required, excluding deemed exports and deemed reexports, to export, reexport, or transfer (in-country) to or within Russia or Belarus any item subject to the EAR and specified in any Export Control Classification Number (ECCN) on the CCL.”

7. The BIS publishes the names of certain foreign entities – including businesses, research institutions, government and private organizations, individuals, and other types of legal persons – that are subject to specific license requirements for the export, reexport and/or transfer (in-country) of specified items. These entities comprise the Entity List, which is found at Title 15, Code of Federal Regulations, Part 774, Supplement Number 4. The entities on the Entity List are subject to individual licensing requirements and policies supplemental to those found elsewhere in the EAR, due to a determination that such entities have engaged in activities contrary to U.S. national security and/or foreign policy interests. As relevant here, applications to export, reexport

or transfer (in-country) items subject to the EAR to Russian entities on the Entity List are subject to a presumption of denial, and no license exceptions apply. See 15 C.F.R. § 744.10.

PROBABLE CAUSE

I. Introduction and Summary of Probable Cause

8. U.S. law enforcement, including the FBI, is conducting a criminal investigation of an international network of individuals and entities responsible for the illegal procurement of sensitive technology for the benefit of the Russian government, including its military and intelligence services.

9. As discussed further below, the evidence gathered pursuant to this investigation has revealed that KAHN engaged in a years-long scheme to secure and export sensitive technology from the United States for the benefit of Joint Stock Company Research and Development Center ELVEES (hereinafter “Elvees”)², a Russian semiconductor manufacturer whose clients include elements of the Russian Ministry of Defense and the Federal Security Service (“FSB”), the main successor agency to the Soviet Union’s KGB. Elvees was sanctioned by the U.S. government in 2022 because of its critical role in facilitating Russia’s military and its invasion of Ukraine. Since at least 2017, and continuing after Elvees was sanctioned, KAHN acquired and exported sensitive and sophisticated electronics from the United States to Russia without securing the appropriate licenses. KAHN also facilitated the manufacturing of Elvees-designed microelectronics by a company in Taiwan. Following Russia’s invasion of Ukraine, after which the company in Taiwan

² Elvees has been identified by the Department of Commerce as “Electronic Computing and Information Systems (ELVIS), a.k.a. Joint Stock Company Research and Development Center ELVEES; and Scientific Production Center Elvis” and by the Department of Treasury as “Elvees Research and Development Center JSC, a.k.a. Elvees R and D Center JSC; a.k.a. Elvees R&D Center JSC; a.k.a. Joint Stock Company Scientific and Production Center Electronic Computing and Information Systems; a.k.a. JSC SPC Elvis.”

would no longer ship the technology to Russia, KAHN arranged for the technology to be sent to the United States. KAHN then re-exported the technology to Elvees in Russia through Hong Kong and other transshipment points in violation of export regulations. KAHN has engaged in substantial fraudulent conduct to obscure his involvement with a sanctioned Russian entity and to evade U.S. export regulations.

II. Background on KAHN and Elvees

10. KAHN is a dual U.S.-Israeli citizen who resides primarily in Israel and occasionally travels to the United States. KAHN is the president and sole owner of Senesys Incorporated (“Senesys”), which is described in California state filings as a “security software development” business. The company lists an address in California as its address of record. The Senesys website states that the company includes “AI and video analytics developers, security experts, and network specialists” and uses a “drone-based surveillance system.”

11. KAHN is also the owner of Sensor Design Association (“SDA”), which is identified in various business records as being located at the same California address as Senesys.³ According to its website, SDA describes itself as a “leading American company in the international market testing of silicon wafers” and that it provides services to “Military / Avionics / Space OEM users.” The SDA website lists an address in Brooklyn, New York as the contact address, which is a residential apartment. In a voluntary phone interview conducted on or about May 29, 2019, a member of KAHN’s family (hereinafter “Family Member-1”) advised law enforcement that SDA and Senesys were the same company.

³ The same California address is also listed as KAHN’s residence in public and government databases, and appears to be a residential address. Other government documents list a different residential address in California as KAHN’s residence.

12. Elvees is a Russian semiconductor manufacturer with close ties to the Russian government. According to an Elvees website, www.elveesneotek.ru/en, Elvees was established with the support of JSC Rusnano, a Russian nanotechnology company. The website claims that Elvees has done hundreds of projects with major Russian, European and Asian companies, as well as international airports, sea trade ports and hydroelectric power plants. Some of the Russian entities Elvees lists as clients include sanctioned Russian energy companies such as Gazprom and Transneft,⁴ as well as Russia's National Defense Control Center, which is the senior command and control center of the Russian Ministry of Defense and the Russian Armed Forces. On the website's "corporate information" page, it states that Elvees has had a procurement license with the FSB since April 28, 2023. The FSB is also sanctioned by the U.S. government.

13. On or about March 9, 2022, Elvees was added to the Entity List by the DOC.⁵ In addition, on or about September 15, 2022, the U.S. Department of the Treasury's Office of Foreign Asset Controls ("OFAC") added Elvees to the Specially Designated Nationals and Blocked Persons List (the "SDN List"),⁶ which is published on OFAC's website. In a press release on or about September 15, 2022, in connection with the designation to the SDN List, the Department of State described Elvees as "a Russian electronics company involved in developing electronics components . . . [and] also produc[ing] a radar system for detecting and tracking airborne, ground,

⁴ See OFAC website, "U.S. Treasury Announces Unprecedented & Expansive Sanctions Against Russia, Imposing Swift and Severe Economic Costs," available at <https://home.treasury.gov/news/press-releases/jy0608> (last visited Dec. 10, 2023) (identifying Gazprom and Transneft as sanctioned entities).

⁵ See 87 Fed. Reg. 13,141 (Mar. 9, 2022).

⁶ See OFAC website, "Russia-related Designations . . . ," available at <https://ofac.treasury.gov/recent-actions/20220915> (last visited Dec. 12, 2023).

and surface targets.”⁷ Accordingly, as of March 9, 2022, goods may not be exported or reexported from the United States to Elvees without a license from DOC. And, as of September 15, 2022, U.S. persons—including KAHN, SDA and Senesys—are prohibited from engaging in any transactions with or for the benefit of Elvees absent authorization from OFAC.⁸

14. Since at least 2011, KAHN used SDA and Senesys to engage in the export of microelectronics and other sophisticated technology from the United States. According to records gathered as part of this investigation, more than 290,000 microelectronics and other items were shipped out of the United States by SDA and Senesys between 2017 and 2023 alone.

15. KAHN’s export activity for the specific benefit of Elvees dates to at least 2012, and KAHN has derived a substantial amount of revenue from his relationship with Elvees. According to financial records, SDA received more than \$37 million from Elvees and related entities between 2012 and 2022, including more than \$2.1 million from Elvees between 2021 and 2022.

III. KAHN’s Knowledge of U.S. Export Regulations

16. KAHN has substantial knowledge about the laws and regulations that govern the export of goods from the United States.

17. For example, KAHN maintained a spreadsheet in his records, which includes an entry from on or about January 25, 2011, that mentions the EAR, links to the then-existing DOC

⁷ See State Dept. website, “Targeting Russia’s Senior Officials, Defense Industrial Base, and Human Rights Abusers,” available at <https://www.state.gov/targeting-russias-senior-officials-defense-industrial-base-and-human-rights-abusers/> (last visited Dec. 11, 2023).

⁸ It is a violation of the International Emergency Economic Powers Act (“IEEPA”), 50 U.S.C. § 1701 *et seq.*, for U.S. persons to transact with entities whose property and interests in property are blocked pursuant to Executive Order 14024. See also 31 C.F.R. § 587.201.

website pages associated with export licensing requirements,⁹ and references particular ECCNs for microelectronics of the type that KAHN often exported from the United States.

18. As another example, in 2018, KAHN and Family Member-1 discussed the need for an end-use certificate (i.e., a written certification about the identity and location of the user of the item) when Family Member-1 attempted to purchase microelectronics associated with radar equipment from a U.S. company.

19. Additionally, and as discussed further below, KAHN received and completed numerous requests from U.S. companies for end-user information, which typically included warnings and information about U.S. export regulations.

20. After Elvees was sanctioned in 2022, KAHN repeatedly indicated in written communications that he was not permitted to engage in business with certain customers in Russia, and even wrote a letter in April 2022 stating that he “cannot continue [sic] business with Elvees,” though he did, in fact, continue doing business with and for Elvees.

21. Despite this knowledge, KAHN repeatedly exported controlled goods from the United States to Russia and other countries, including goods controlled for national security reasons, without securing the proper licenses.

22. Additionally, after Elvees was added to the Entity List in March 2022, and to the SDN List in September 2022, KAHN continued to cause exports for which Elvees was the ultimate end user, and to engage in other transactions for Elvees’s benefit, in violation of U.S. export

⁹ The URLs to the website pages in the document are no longer active but, based on my training and experience and discussions with DOC employees, I know that the URL previously linked to information related to export licensing requirements.

regulations and sanctions. As discussed below, he did so through a complex series of transactions designed to obscure his illegal activity.

IV. KAHN's Fraudulent Scheme to Violate ECRA and Export Regulations

A. Illegal Export of U.S.-Origin Microcontroller to Russia

23. On or about March 29, 2018, KAHN received a letter from Elvees directing him to purchase five units of a specific low power microcontroller ("U.S. Microcontroller-1") manufactured by a U.S. company ("U.S. Company-1"). Depicted below is the header of the letter, which contains the Elvees name in Russian as well as a distinctive circular logo associated with Elvees.



24. U.S. Microcontroller-1 is controlled by the DOC under ECCN 3A001.a.2.c for national security reasons. A license was required to export this item from the United States to Russia in 2018 and thereafter.

25. According to order confirmation records found in the Senesys email account associated with KAHN, on or about August 24, 2019, Senesys purchased five units of the U.S. Microcontroller-1 from U.S. Company-1. The delivery address was an address in New Hampshire identified as being associated at the time with SDA and Family Member-1.

26. On or about August 30, 2019, SDA issued a commercial invoice to Elvees for the shipment of five units of the U.S. Microcontroller-1 to an address associated with Elvees in Moscow, Russia.

27. According to a license history check performed by BIS, KAHN did not obtain a license to export these or any other goods to Russia.

B. Illegal Export of Multiple U.S.-Origin Microelectronics to Sanctioned Russian Entity Through Hong Kong Shipper

28. According to email records, on or about and between March 16, 2022 and March 18, 2022, after Russia's invasion of Ukraine on February 24, 2022, KAHN exchanged a series of communications with a representative of a Hong Kong shipping company (the "Hong Kong Shipper"). In sum and substance, the communications reveal a scheme to falsely portray the Hong Kong Shipper as the purchaser and end user of items exported from the United States to conceal the fact that the items were ultimately destined for Elvees in Russia. Specifically, on behalf of Elvees, KAHN indicated that he would purchase a quantity of specific U.S.-origin network interface controllers (the "U.S. Network Hardware") from a U.S. supplier and requested that the Hong Kong Shipper purchase those goods from him. KAHN also requested the Hong Kong Shipper to purchase a radiofrequency transmitter (the "U.S. RF Transmitter") directly from a U.S. company.

29. KAHN indicated to the Hong Kong Shipper that a person he identified by name ("Named Employee-1") was directing the acquisition of these goods. According to other records found in KAHN's business records for SDA and Senesys, Named Employee-1 is an Elvees employee. For example, on December 6, 2018, KAHN received a request from Elvees employees to purchase technology from a U.S.-based business. A person with the same name as Named Employee-1 with an "@elvees.com" email address was cc'd on this email thread.

30. Additionally, on or about March 16, 2022, another person with an "@elvees.com" email address ("Named Employee-2") emailed KAHN an invoice reflecting "prepayment" for the

shipment of quantities of the U.S. RF Transmitter and U.S. Network Hardware. The invoice sent by Named Employee-2 was drafted to appear to be from the Hong Kong Shipper, indicated that the items were to be shipped to Russia to the attention of Named Employee-1, but billed to a different company than Elvees. On or about that same date, March 16, 2022, KAHN sent what appears to be the same invoice to the Hong Kong Shipper, indicating that it was an “invoice sample,” but that the “money will be the same as in the invoice” once the transaction to acquire the U.S. RF Transmitter and U.S. Network Hardware was completed.

31. As noted above, as of March 9, 2022, prior to these communications, Elvees was placed on the Entity List, and therefore KAHN and the U.S. businesses that he operated were prohibited from exporting or reexporting any goods to Elvees without a license.

32. Additionally, according to DOC records, the U.S. Network Hardware was controlled under ECCN 5A002.a, for reasons of national security, and could not be shipped to Russia or Hong Kong without a license during the relevant time period. The U.S. RF Transmitter was controlled under ECCN 5A991.b, for reasons of anti-terrorism, and could not be shipped to Russia without a license during the relevant time period.

33. According to purchase order information found in KAHN’s business records, on or about March 22, 2022, May 18, 2022, and May 24, 2022, KAHN purchased four units of the U.S. Network Hardware from a U.S.-based company. KAHN requested that the items be shipped to SDA in California. On or about March 29, 2022 and May 3, 2022, KAHN purchased five units of the U.S. RF Transmitter from a U.S.-based company. KAHN likewise requested that the items be shipped to SDA in California.

34. KAHN was advised by the suppliers that exporting these products might be illegal without a proper license. Invoices for the U.S. Network Hardware sent to KAHN state that the

U.S. Network Hardware is subject to the EAR and cannot be shipped without proper license.

Similarly, invoices for the U.S. RF Transmitter expressly stated:

THESE ITEMS ARE CONTROLLED BY THE U.S. GOVERNMENT AND AUTHORIZED FOR EXPORT ONLY TO THE COUNTRY OF ULTIMATE DESTINATION FOR USE BY THE ULTIMATE CONSIGNEE OR END-USER(S) HEREIN IDENTIFIED. THEY MAY NOT BE RESOLD, TRANSFERRED, OR OTHERWISE DISPOSED OF, TO ANY OTHER COUNTRY OR TO ANY PERSON OTHER THAN THE AUTHORIZED ULTIMATE CONSIGNEE OR END-USER(S), EITHER IN THEIR ORIGINAL FORM OR AFTER BEING INCORPORATED INTO OTHER ITEMS WITHOUT FIRST OBTAINING APPROVAL FROM THE U.S. GOVERNMENT OR AS OTHERWISE AUTHORIZED BY U.S. LAW AND REGULATIONS.

(Capitalization in original).

35. KAHN was also told by an employee of the Hong Kong Shipper that export of the technology from the United States was not permitted without appropriate permissions. Specifically, on or about March 16, 2022, the employee told KAHN that U.S. Network Hardware “is forbidden to be sold to China(including HK),” a reference to Hong Kong, and that “if you ship this time from USA to me, it will be a problem.” On or about March 17, 2022, KAHN received another email from the representative of the Hong Kong Shipper, stating that the U.S. RF Transmitter also could not be shipped “to China” and that it was likely “because it has military use.”

36. Notwithstanding these warnings, KAHN proceeded with the transaction and export of the goods. According to emails and other records, on or about June 13, 2022, KAHN received confirmation from a New York-based shipping company that it had shipped items to an address in Hong Kong associated with Hong Kong Shipper by way of John F. Kennedy International Airport (“JFK Airport”). Included in the materials was an SDA commercial invoice, signed by KAHN,

which indicated that he shipped the four units of the U.S. Network Hardware and five units of the U.S. RF Transmitter to Hong Kong.

37. According to a license history check performed by BIS, KAHN did not obtain a license to export these or any other goods to Russia or Hong Kong. Additionally, as discussed above, Elvees was directing the acquisition of these goods, and as a result of Elvees being placed on the Entity List, a specific license was required to export any items for which Elvees was the ultimate end user. KAHN did not obtain such a license to export to Elvees.

C. The Scheme to Illegally Manufacture and Ship Semiconductors Designed by Elvees

38. KAHN also assisted Elvees with the manufacture of semiconductors in Taiwan that were designed by Elvees and the shipment of those semiconductors from Taiwan to Russia. Following Russia's invasion of Ukraine in February 2022, KAHN often caused the shipment of quantities of the microelectronics from Taiwan to the United States before reexporting them to Russia, including through the People's Republic of China (the "PRC"), South Korea and Hong Kong, using the same Hong Kong shipping company described above. The export or reexport of these items from the United States to Russia required a license, which KAHN did not obtain.

39. According to publicly available Russian news reporting, since at least 2012 Elvees has designed and caused the manufacture of a series of semiconductors¹⁰ known as "NVCOM."

¹⁰ Semiconductors are sometimes also called microchips or integrated circuits.

Depicted below is an image from the reporting of an example of an NVCOM semiconductor, which includes the distinctive Elvees logo, as well as the model number “1892BM10R.”¹¹



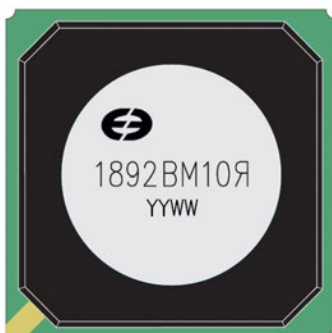
40. NVCOM semiconductors were typically fabricated by a company located in Taiwan (the “Taiwan Manufacturer”). KAHN, through SDA and Senesys, facilitated the production and shipment of the NVCOM semiconductors for the benefit of Elvees. For example, on or about January 27, 2017, KAHN, using his Senesys email account, discussed with an Elvees employee issues related to the testing of certain NVCOM semiconductors. Subsequently, on or about October 12, 2017, a shipping invoice in KAHN’s records from SDA reflects that SDA shipped 20,655 units of “Microchip 1892BM10R” (i.e., the same model number on the NVCOM microchip depicted above) from Taiwan to an entity in Russia at a total cost of more than \$248,000. Notably, subsequent records in KAHN’s possession reflect that the company the NVCOM microchips were sent to in Russia is a buyer for Elvees.

41. As discussed above, Elvees was added to the Entity List on March 9, 2022. The following month, on April 11, 2022, KAHN appeared to express his awareness of the fact that due to Russia’s invasion of Ukraine the U.S. government was increasingly imposing export restrictions and sanctions on Russia and Russian entities, including Elvees, writing a letter to a senior Elvees

¹¹ The “R” in the model number is reversed, reflecting a Russian-language Cyrillic character that does not exist in the Roman alphabet.

employee that stated, “Dew [sic] current political situation I cannot continue business with ELVEES.”

42. Nevertheless, KAHN continued to engage in transactions with Elvees. For example, on May 19, 2022, KAHN emailed the Taiwan Manufacturer and gave directions about the NVCOM semiconductor. The design KAHN sent to the manufacturer continued to reflect the Elvees logo, indicating that KAHN was still working for the benefit of Elvees. Depicted below is the design sent by KAHN, which is materially identical to the picture of the NVCOM microprocessor in paragraph 39:



43. KAHN was made aware that continued transactions with Elvees was a problem for the Taiwan Manufacturer. On August 17, 2022, KAHN signed a “Form of Reasonable Inquiry of Export Control Compliance” that was requested by the Taiwan Manufacturer, certifying that KAHN would not “engage in any export, re-export or transfer of [semiconductor products] posing potential risk exposure to violations of U.S. Export Administration Regulations.” KAHN certified that semiconductors manufactured by Taiwan Manufacturer would not “be destined, directly or indirectly, to any entity or individuals located in the territory of Russia and/or Belarus.”

44. Additionally, on or about August 19, 2022, KAHN was asked to provide information about the end user and application of the NVCOM semiconductor and another microchip model. KAHN responded asking if he could “put Awadji [a location in Kyrgyzstan] as

the end user?” The manufacturer representative said he could not because “Our Legal doesn’t allow us to ship to Awaji as they suspect the parts might eventually go to Russia.”

45. Subsequent to the Taiwan Manufacturer’s rejection of Awadji as an appropriate shipping location, KAHN sought to ship NVCOM semiconductors into the United States. On or about September 16, 2022 – one day after Elvees was sanctioned by OFAC and placed on the SDN List – KAHN completed a “written assurance of end uses” from the Taiwan Manufacturer, which indicated that he was shipping 50,667 units of NVCOM semiconductors to SDA’s address in California, by way of JFK Airport in New York.

46. According to DOC records, the NVCOM semiconductors are controlled by the DOC under ECCN 3A001.a.2.c for national security and anti-terrorism reasons and require a license to be shipped to Russia and Hong Kong during this time period. Thus, once KAHN shipped these items into the United States, he was required to obtain an export license if he wanted to export them to Russia or Hong Kong. Additionally, as a result of Elvees being placed on the Entity List, a specific license was required to export any items for which Elvees was the ultimate end user, and after Elvees was placed on the SDN List, KAHN and his businesses were prohibited from engaging in any transaction or providing any services for Elvees’s benefit.

47. According to records from KAHN’s Senesys email account, on or about November 4, 2022, KAHN engaged in a series of emails with the Hong Kong Shipper about the shipment of NVCOM semiconductors to entities outside the United States, including in the Republic of Korea (“South Korea”) and Krygyzstan.

48. According to email communications and other records, on or about November 11, 2022, KAHN, through SDA, directed a New York-based shipper to ship 28,800 units of

NVCOM01 microchips to the Hong Kong Shipper, which according to an SDA invoice were valued at \$72,000.

49. According to emails and other records found in KAHN's Senesys email account, on or about and between November 22, 2022 and January 12, 2023, KAHN shipped 7,200 units of NVCOM semiconductors, by way of a New York-based shipper, first to the Hong Kong Shipper, and eventually to an entity in the PRC. Notably, on or about November 25, 2022, KAHN emailed the Hong Kong Shipper, indicating that he received a "call from Russia" about the entity in the PRC to which he had shipped NVCOM semiconductors, which I believe to be a reference to the fact that the semiconductors were, in reality, destined for Russia and Elvees.

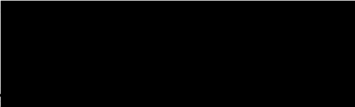
50. Subsequently, on or about May 19, 2023, a Senesys invoice reflects that 7133 units of NVCOM semiconductors were shipped to a company in South Korea. The invoice was signed by Family Member-1.

51. According to government records, KAHN never obtained a license to export NVCOM semiconductors from the United States to Russia, South Korea or Hong Kong, nor did he obtain a license to export any goods to Elvees as the end user.


WHEREFORE, your deponent respectfully requests that an arrest warrant be issued for the defendant ILYA KAHN, so that he may be dealt with according to law.

IT IS FURTHER REQUESTED that this Court issue an order sealing, until further order of the Court, all papers submitted in support of this application, including this Affidavit and any arrest warrants issued, with the exception that the complaint and arrest warrant can be unsealed for the limited purpose of disclosing the existence of, or disseminating, the complaint and/or arrest warrant to relevant United States, foreign or intergovernmental authorities, at the discretion of the United States and in connection with efforts to prosecute the defendant or to secure the defendant's

arrest, extradition or expulsion. Based on my training and experience, I have learned that criminals actively search for criminal affidavits on the Internet and disseminate them to other criminals as they deem appropriate, such as by posting them publicly through online forums. Premature disclosure of the contents of this Affidavit and related documents will seriously jeopardize the investigation, including by giving targets an opportunity to flee or continue flight from prosecution, destroy or tamper with evidence, change patterns of behavior and notify confederates.


Nicholas Milan
Special Agent
Federal Bureau of Investigation

Sworn to before me this
22th day of December, 2023 by telephone



THE HONORABLE PEGGY KUO
UNITED STATES MAGISTRATE JUDGE
EASTERN DISTRICT OF NEW YORK

Approved:


MATTHEW J.C. HELLMAN / KEVIN SULLIVAN
Assistant United States Attorneys

Before:

THE HONORABLE GABRIEL W. GORENSTEIN
United States Magistrate Judge
Southern District of New York

23 MAG 6023

UNITED STATES OF AMERICA

-v.-

ARTHUR PETROV,

Defendant.

SEALED COMPLAINT

Violations of 50 U.S.C. § 4819; and 18
U.S.C. §§ 2, 371, 554, 1349, and 1956

COUNTY OF OFFENSE:
NEW YORK

SOUTHERN DISTRICT OF NEW YORK, ss.:

BRIAN SMITH, being duly sworn, deposes and says that he is a Special Agent with the Federal Bureau of Investigation (“FBI”), and charges as follows:

COUNT ONE
(Conspiracy to Defraud the United States)

1. From at least in or about February 2022, up to and including in or about August 2023, in the Southern District of New York, Cyprus, Russia, and elsewhere, and in an offense begun and committed out of the jurisdiction of any particular State or district of the United States, ARTHUR PETROV, the defendant, and others known and unknown, at least one of whom is expected to be first brought to and arrested in the Southern District of New York, knowingly and intentionally combined, conspired, confederated, and agreed together and with each other to defraud the United States and agencies thereof, by impairing, impeding, obstructing, and defeating, through deceitful and dishonest means, the lawful functions of the U.S. Department of Commerce, an agency of the United States, in the enforcement and issuance of licenses relating to the export of goods.

2. In furtherance of the conspiracy and to effect the illegal object thereof, ARTHUR PETROV, the defendant, and others known and unknown, committed the overt acts set forth in paragraphs 19(p) through 19(oo) of this Complaint, among others.

(Title 18, United States Code, Sections 371 and 3238.)

COUNT TWO
(Conspiracy to Violate ECRA)

3. From at least in or about February 2022, up to and including in or about August 2023, in the Southern District of New York, Cyprus, Russia, and elsewhere, and in an offense

begun and committed out of the jurisdiction of any particular State or district of the United States, ARTHUR PETROV, the defendant, and others known and unknown, at least one of whom is expected to be first brought to and arrested in the Southern District of New York, knowingly and willfully combined, conspired, confederated, and agreed together and with each other to violate, and to cause a violation of, licenses, orders, regulations, and prohibitions issued under the Export Control Reform Act.

4. It was a part and an object of the conspiracy that ARTHUR PETROV, the defendant, and others known and unknown, would and did export and cause to be exported from the United States to Russia items controlled under Subchapter I of the Export Control Reform Act, to wit, electronics components on the Commerce Control List set forth in Title 15, Code of Federal Regulations, Part 774, Supplement Number 1, without having first obtained a license for such export from the U.S. Department of Commerce, in violation of Title 50, United States Code, Section 4819(a)(2)(A), (B), (C), (D), (E), (F), and (G), and Title 15, Code of Federal Regulations, Sections 736.2(b)(1), 746.8(a)(1), and 764.2.

(Title 50, United States Code, Sections 4819(a)(1), 4819(a)(2)(A)-(G), and 4819(b); Title 15, Code of Federal Regulations, Sections 736.2(b)(1), 746.8(a)(1), and 764.2; and Title 18, United States Code, Section 3238.)

COUNT THREE
(Violation of ECRA – Export #1)

5. From at least in or about April 2022, up to and including in or about October 2022, in the Southern District of New York, Cyprus, Russia, and elsewhere, and in an offense begun and committed out of the jurisdiction of any particular State or district of the United States, ARTHUR PETROV, the defendant, and others known and unknown, at least one of whom is expected to be first brought to and arrested in the Southern District of New York, knowingly and willfully exported and caused to be exported, and attempted to export and cause to be exported, from the United States to Russia items controlled under Subchapter I of the Export Control Reform Act, to wit, microcontrollers on the Commerce Control List set forth in Title 15, Code of Federal Regulations, Part 774, Supplement Number 1, controlled under Export Control Classification Number 3A991.a.2, without having first obtained a license for such export from the U.S. Department of Commerce, and aided and abetted the same.

(Title 50, United States Code, Sections 4819(a)(1), 4819(a)(2)(A)-(G), and 4819(b); Title 15, Code of Federal Regulations, Sections 736.2(b)(1), 746.8(a)(1), and 764.2; and Title 18, United States Code, Sections 2 and 3238.)

COUNT FOUR
(Violation of ECRA – Export #2)

6. From at least in or about July 2022, up to and including in or about October 2022, in the Southern District of New York, Cyprus, Russia, and elsewhere, and in an offense begun and committed out of the jurisdiction of any particular State or district of the United States, ARTHUR PETROV, the defendant, and others known and unknown, at least one of whom is expected to be first brought to and arrested in the Southern District of New York, knowingly and willfully exported and caused to be exported, and attempted to export and cause to be exported, from the

United States to Russia items controlled under Subchapter I of the Export Control Reform Act, to wit, integrated circuits on the Commerce Control List set forth in Title 15, Code of Federal Regulations, Part 774, Supplement Number 1, controlled under Export Control Classification Number 3A991.b.1.a, without having first obtained a license for such export from the U.S. Department of Commerce, and aided and abetted the same.

(Title 50, United States Code, Sections 4819(a)(1), 4819(a)(2)(A)-(G), and 4819(b); Title 15, Code of Federal Regulations, Sections 736.2(b)(1), 746.8(a)(1), and 764.2; and Title 18, United States Code, Sections 2 and 3238.)

COUNT FIVE
(Violation of ECRA – Export #3)

7. From at least in or about April 2022, up to and including in or about March 2023, in the Southern District of New York, Cyprus, Russia, and elsewhere, and in an offense begun and committed out of the jurisdiction of any particular State or district of the United States, ARTHUR PETROV, the defendant, and others known and unknown, at least one of whom is expected to be first brought to and arrested in the Southern District of New York, knowingly and willfully exported and caused to be exported, and attempted to export and cause to be exported, from the United States to Russia items controlled under Subchapter I of the Export Control Reform Act, to wit, microcontrollers on the Commerce Control List set forth in Title 15, Code of Federal Regulations, Part 774, Supplement Number 1, controlled under Export Control Classification Number 3A991.a.2, without having first obtained a license for such export from the U.S. Department of Commerce, and aided and abetted the same.

(Title 50, United States Code, Sections 4819(a)(1), 4819(a)(2)(A)-(G), and 4819(b); Title 15, Code of Federal Regulations, Sections 736.2(b)(1), 746.8(a)(1), and 764.2; and Title 18, United States Code, Sections 2 and 3238.)

COUNT SIX
(Conspiracy to Smuggle Goods from the United States)

8. From at least in or about February 2022, up to and including in or about August 2023, in the Southern District of New York, Cyprus, Russia, and elsewhere, and in an offense begun and committed out of the jurisdiction of any particular State or district of the United States, ARTHUR PETROV, the defendant, and others known and unknown, at least one of whom is expected to be first brought to and arrested in the Southern District of New York, knowingly and intentionally combined, conspired, confederated, and agreed together and with each other to commit an offense against the United States, to wit, smuggling goods from the United States in violation of Title 18, United States Code, Section 554.

9. It was a part and an object of the conspiracy that ARTHUR PETROV, the defendant, and others known and unknown, would and did fraudulently and knowingly export and send from the United States, attempt to export and send from the United States, and cause to be exported and sent from the United States, merchandise, articles, and objects, to wit, items controlled under Subchapter I of the Export Control Reform Act, namely, electronics components on the Commerce Control List set forth in Title 15, Code of Federal Regulations, Part 774, Supplement Number 1, contrary to laws and regulations of the United States, to wit, the Export

Control Reform Act and associated regulations, Title 50, United States Code, Sections 4819(a)(1), 4819(a)(2)(A)-(G), and 4819(b), and Title 15, Code of Federal Regulations, Sections 736.2(b)(1), 746.8(a)(1), and 764.2, and fraudulently and knowingly receive, conceal, buy, sell, and in any manner facilitate the transportation, concealment, and sale of such merchandise, articles, and objects, prior to exportation, knowing the same to be intended for exportation contrary to such laws and regulations of the United States.

10. In furtherance of the conspiracy and to effect the illegal objects thereof, ARTHUR PETROV, the defendant, and others known and unknown, committed the overt acts set forth in paragraphs 19(p) through 19(oo) of this Complaint, among others.

(Title 18, United States Code, Sections 371 and 3238.)

COUNT SEVEN
(Smuggling Goods from the United States – Export #1)

11. From at least in or about April 2022, up to and including in or about October 2022, in the Southern District of New York, Cyprus, Russia, and elsewhere, and in an offense begun and committed out of the jurisdiction of any particular State or district of the United States, ARTHUR PETROV, the defendant, and others known and unknown, at least one of whom is expected to be first brought to and arrested in the Southern District of New York, fraudulently and knowingly exported and sent from the United States, attempted to export and send from the United States, and caused to be exported and sent from the United States, merchandise, articles, and objects, to wit, items controlled under Subchapter I of the Export Control Reform Act, namely, microcontrollers on the Commerce Control List set forth in Title 15, Code of Federal Regulations, Part 774, Supplement Number 1, controlled under Export Control Classification Number 3A991.a.2, contrary to laws and regulations of the United States, to wit, the Export Control Reform Act and associated regulations, Title 50, United States Code, Sections 4819(a)(1), 4819(a)(2)(A)-(G), and 4819(b), and Title 15, Code of Federal Regulations, Sections 736.2(b)(1), 746.8(a)(1), and 764.2, and fraudulently and knowingly received, concealed, bought, sold, and in any manner facilitated the transportation, concealment, and sale of such merchandise, articles, and objects, prior to exportation, knowing the same to be intended for exportation contrary to such laws and regulations of the United States.

(Title 18, United States Code, Sections 554(a), 2, and 3238.)

COUNT EIGHT
(Smuggling Goods from the United States – Export #2)

12. From at least in or about July 2022, up to and including in or about October 2022, in the Southern District of New York, Cyprus, Russia, and elsewhere, and in an offense begun and committed out of the jurisdiction of any particular State or district of the United States, ARTHUR PETROV, the defendant, and others known and unknown, at least one of whom is expected to be first brought to and arrested in the Southern District of New York, fraudulently and knowingly exported and sent from the United States, attempted to export and send from the United States, and caused to be exported and sent from the United States, merchandise, articles, and objects, to wit, items controlled under Subchapter I of the Export Control Reform Act, namely, integrated circuits on the Commerce Control List set forth in Title 15, Code of Federal Regulations, Part 774,

Supplement Number 1, controlled under Export Control Classification Number 3A991.b.1.a, contrary to laws and regulations of the United States, to wit, the Export Control Reform Act and associated regulations, Title 50, United States Code, Sections 4819(a)(1), 4819(a)(2)(A)-(G), and 4819(b), and Title 15, Code of Federal Regulations, Sections 736.2(b)(1), 746.8(a)(1), and 764.2, and fraudulently and knowingly received, concealed, bought, sold, and in any manner facilitated the transportation, concealment, and sale of such merchandise, articles, and objects, prior to exportation, knowing the same to be intended for exportation contrary to such laws and regulations of the United States.

(Title 18, United States Code, Sections 554(a), 2, and 3238.)

COUNT NINE
(Smuggling Goods from the United States – Export #3)

13. From at least in or about April 2022, up to and including in or about March 2023, in the Southern District of New York, Cyprus, Russia, and elsewhere, and in an offense begun and committed out of the jurisdiction of any particular State or district of the United States, ARTHUR PETROV, the defendant, and others known and unknown, at least one of whom is expected to be first brought to and arrested in the Southern District of New York, fraudulently and knowingly exported and sent from the United States, attempted to export and send from the United States, and caused to be exported and sent from the United States, merchandise, articles, and objects, to wit, items controlled under Subchapter I of the Export Control Reform Act, namely, microcontrollers on the Commerce Control List set forth in Title 15, Code of Federal Regulations, Part 774, Supplement Number 1, controlled under Export Control Classification Number 3A991.a.2, contrary to laws and regulations of the United States, to wit, the Export Control Reform Act and associated regulations, Title 50, United States Code, Sections 4819(a)(1), 4819(a)(2)(A)-(G), and 4819(b), and Title 15, Code of Federal Regulations, Sections 736.2(b)(1), 746.8(a)(1), and 764.2, and fraudulently and knowingly received, concealed, bought, sold, and in any manner facilitated the transportation, concealment, and sale of such merchandise, articles, and objects, prior to exportation, knowing the same to be intended for exportation contrary to such laws and regulations of the United States.

(Title 18, United States Code, Sections 554(a), 2, and 3238.)

COUNT TEN
(Conspiracy to Commit Wire Fraud)

14. From at least in or about February 2022, up to and including in or about August 2023, in the Southern District of New York, Cyprus, Russia, and elsewhere, and in an offense begun and committed out of the jurisdiction of any particular State or district of the United States, ARTHUR PETROV, the defendant, and others known and unknown, at least one of whom is expected to be first brought to and arrested in the Southern District of New York, knowingly and willfully combined, conspired, confederated, and agreed together and with each other to commit wire fraud in violation of Title 18, United States Code, Section 1343.

15. It was a part and an object of the conspiracy that ARTHUR PETROV, the defendant, and others known and unknown, having devised and intending to devise a scheme and artifice to defraud, and for obtaining money and property by means of false and fraudulent

pretenses, representations, and promises, would and did transmit and cause to be transmitted by means of wire communication in interstate and foreign commerce, writings, signs, signals, pictures, and sounds for the purpose of executing such scheme and artifice, in violation of Title 18, United States Code, Section 1343.

(Title 18, United States Code, Sections 1349 and 3238.)

COUNT ELEVEN
(Conspiracy to Commit Money Laundering)

16. From at least in or about February 2022, up to and including in or about August 2023, in the Southern District of New York, Cyprus, Russia, and elsewhere, and in an offense begun and committed out of the jurisdiction of any particular State or district of the United States, ARTHUR PETROV, the defendant, and others known and unknown, at least one of whom is expected to be first brought to and arrested in the Southern District of New York, knowingly and intentionally combined, conspired, confederated, and agreed together and with each other commit money laundering in violation of Title 18, United States Code, Section 1956(a)(2)(A).

17. It was a part and an object of the conspiracy that ARTHUR PETROV, the defendant, and others known and unknown, would and did transport, transmit, and transfer, and attempt to transport, transmit, and transfer, monetary instruments and funds to places in the United States from and through places outside the United States, in amounts exceeding \$10,000, with the intent to promote the carrying on of specified unlawful activity, to wit, (a) smuggling goods from the United States, as charged in Counts Seven through Nine of this Complaint, and (b) wire fraud, in violation of Title 18, United States Code, Section 1343.

(Title 18, United States Code, Sections 1956(h), 1956(f), and 3238.)

The bases for my knowledge and for the foregoing charges are, in part, as follows:

18. I have been an FBI Special Agent since 2018. I am currently assigned to the Counterintelligence Division of the New York Field Office of the FBI, which focuses on cases involving, among other things, sanctions evasion, export control violations, counter-proliferation, wire fraud, bank fraud, and money laundering. During my time as an FBI Special Agent, I have become familiar with some of the ways in which criminal actors avoid export controls, evade sanctions, and smuggle goods and technology from the United States, and I have participated in numerous investigations involving sanctions evasion, export control violations, and smuggling. This affidavit is based upon my participation in the investigation of this matter, including my conversations with law enforcement agents and other individuals, my review of law enforcement reports and records, and my review of business records, photographs, email communications, and draft summaries and translations of such documents and communications. Because this affidavit is being submitted for the limited purpose of establishing probable cause, it does not include all the facts that I have learned during the course of my investigation. Where the contents of documents and the actions, statements, and conversations of others are reported herein, they are reported in substance and in part, except where otherwise indicated. Where figures, calculations, and dates are set forth herein, they are approximate, unless stated otherwise.

19. Based on my participation in this investigation, including my conversations with other law enforcement agents and other individuals, my conversations with law enforcement agents and other individuals, my review of law enforcement reports and records, and my review of business records, shipping and travel records, photographs, email communications obtained pursuant to judicially authorized search warrants, and draft summaries and translations of such documents and communications, I have learned the following, in substance and in part:

Overview

a. As set forth in greater detail below, the FBI and the Bureau of Industry and Security (“BIS”) of the U.S. Department of Commerce (“DOC”) are investigating a sophisticated international scheme to violate and evade U.S. export controls against Russia that began before and continued after Russia’s February 2022 invasion of Ukraine. PETROV and two co-conspirators (“CC-1” and “CC-2”), who are Russian nationals operating an illicit procurement network in Russia and elsewhere overseas, have fraudulently procured from U.S. distributors large quantities of micro-electronics subject to U.S. export controls on behalf of LLC Electrocom VPK (“Electrocom”), a Russia-based supplier of critical electronics components for manufacturers supplying weaponry and other equipment to the Russian military. To carry out the scheme, PETROV, CC-1, and CC-2 use shell companies and other deceptive means to conceal that the electronics components are destined for Russia. The technology that PETROV and his co-conspirators have procured in contravention of export controls during the course of the conspiracy have significant military applications, and include various types of electronics components that have been recovered in Russian military hardware on the battlefield in Ukraine, such as Russian guided missiles, drones, and electronic warfare and communications devices.

b. To perpetrate the scheme, PETROV first acquires the controlled micro-electronics from U.S.-based electronics exporters using a Cyprus-based shell company, Astraferos Technokosmos LTD (“Astraferos”). PETROV procures these sensitive electronics components by falsely representing to the U.S. exporters that Astraferos is purchasing the items for fire security systems, among other commercial uses, and that the ultimate end-users and destinations of the electronics are companies in Cyprus or one of two other countries (“Country-1” and “Country-2”) — when in fact the components are destined for Electrocom in Russia, which supplies manufacturers for the Russian military. The micro-electronics that PETROV has procured as part of the conspiracy include, among other things, microcontrollers and integrated circuits that are on the Commerce Control List (“CCL”) maintained by the DOC and cannot lawfully be exported or reexported to Russia without a license from the DOC. Invoices provided to PETROV by the U.S. distributors expressly noted that these microcontrollers and integrated circuits are subject to U.S. export controls. As noted, these types of micro-electronics have been recovered in Russian military equipment on the battlefield in Ukraine.

c. To evade these controls, PETROV, CC-1, and CC-2 work together to transship the controlled items using pass-through entities in third countries. In particular, after fraudulently procuring the electronics components from the U.S. distributors, PETROV ships the controlled items to a pass-through shipping company (“Company-1”) in Country-1 used by CC-1, or to a pass-through shipping company (“Company-2”) in Country-2 operated by CC-2. CC-1 and CC-2 then cause the items to be shipped, sometimes through yet another third country, to the ultimate destination: Electrocom in Saint Petersburg, Russia. At all times, PETROV, CC-1, and CC-2 conceal from the U.S. distributors that they are procuring the controlled electronics

components on behalf of Electrocom — a supplier for the Russian military industrial complex, as set forth above — and that the items are destined not for Cyprus, Country-1, or Country-2, but rather for Russia.

d. During the course of the conspiracy, PETROV, CC-1, and CC-2 have procured from U.S. distributors and shipped to Russia more than \$225,000 worth of controlled electronics components with military applications. None of these individuals, or the entities they use to perpetrate their scheme, have ever applied for an export license from the DOC.

The Defendant, CC-1, CC-2, and Relevant Entities

e. Electrocom is a Russia-based supplier of electronics to the Russian military, founded by CC-2 and two other Russian nationals. CC-2 is an executive at Electrocom, and PETROV and CC-1 are employees at Electrocom. On behalf of Electrocom, PETROV, CC-1, and CC-2 operate and use pass-through entities — Astraferos (in Cyprus), Company-1 (in Country-1), and Company-2 (in Country-2), respectively — to procure electronics from U.S.-based companies by misrepresenting the true destination and end-use of the electronics, and then cause those goods and technology to be shipped to Electrocom in Russia, in violation of U.S. export controls. The company’s official name — LLC Electrocom VPK — reflects its principal purpose as a supplier of components used by the Russian military: “VPK” is commonly used as an acronym in Russian for “Military Industrial Complex.” Consistent with its corporate name, Electrocom supplies dual-use electronics — that is, electronics with both civilian and military applications — to Russian military suppliers, including multiple companies that have been sanctioned by the U.S. Government. For example, in a draft letter dated March 10, 2023, which CC-1 received from an associate, and was addressed from Electrocom to TRV-Engineering — a U.S.-sanctioned Russian company affiliated with Tactical Missiles Corporation JSC, a U.S.-sanctioned Russian defense conglomerate that produces airborne weapons and weapon systems for Russia’s navy¹ — CC-2, the signatory to the letter identified as Electrocom’s “General Director,” described Electrocom as “specializ[ing]” in “the supply” and import to Russia of “hard-to-reach” and “high-tech electric components produced in the United States, Europe and Asia for domestic enterprises of both the civil sector and the military industrial complex.”

¹ On or about March 24, 2022, the U.S. Department of the Treasury’s Office of Foreign Assets Control (“OFAC”) designated Tactical Missiles Corporation JSC as a Specially Designated National (“SDN”) for “operating or having operated in the defense and related materiel sector of the Russian Federation economy and for being owned or controlled by, or having acted or purported to act for or on behalf of, directly or indirectly, the Government of the Russian Federation,” and OFAC designated TRV-Engineering (also known as TRV Auto Limited Liability Company) as an SDN for “being owned or controlled by, or having acted or purported to act for or on behalf of, directly or indirectly, [Tactical Missiles Corporation JSC].” On or about April 1, 2022, the DOC added “Tactical Missile Corporation, TRV Engineering” to the DOC’s Entity List — which identifies entities for which there is reasonable cause to believe the entities have been involved, are involved, or pose a significant risk of being or becoming involved in activities contrary to the national security or foreign policy interests of the United States — “for acquiring and attempting to acquire items subject to the [DOC’s Export Administration Regulations] in support of Russia’s military.”

f. PETROV, a Russian national who has resided in Cyprus and Russia, among other locations, has operated Astraferos, a shell company registered in Cyprus, to procure from U.S. distributors micro-electronics for transshipment to Russia. PETROV works for Electrocom and has used Astraferos as a front company, working together with CC-1 and CC-2, to procure from U.S. distributors hundreds of thousands of dollars' worth of controlled goods that they then transshipped to Electrocom in Russia. Based on a review of email communications, PETROV represents that he is "Head of Purchasings" for Astraferos. PETROV's public online profile state that he stopped working for Electrocom in February 2022 — and describe his role there as "Purchaser" and "Head [o]f Purchasing Department" in Russia" — yet his email signature blocks and the content of his email correspondence make clear that he is still working for Electrocom but doing so under the Astraferos name. For example, even after he began operating as the "Head of Purchasings" for Astraferos, PETROV sometimes even used an email address expressly associating him with Electrocom.

g. CC-1 is a Russian national residing in Russia who works for Electrocom and transships U.S.-sourced electronics to Electrocom in Russia through Company-1, a third-party distributor based in Country-1. CC-1 uses Company-1 as a pass-through for U.S.-sourced parts procured for Electrocom by PETROV through Astraferos in Cyprus. The website for Company-1 states that the company supplies "electronic components" and provides "supply and service in Russia."

h. CC-2 is a Russian national residing in Russia who is the co-founder and General Director of Electrocom. As part of the illicit procurement network with PETROV and CC-1, CC-2 operates Company-2, a shell company registered and based in Country-2, to transship U.S.-sourced electronics procured by PETROV and Astraferos in Cyprus, to Electrocom in Russia.

Background on Russia's Use of U.S.-Sourced Electronics in Ukraine

i. Russia is highly dependent on Western-sourced micro-electronics components for its military's hardware, including components manufactured or sold in the United States. Russia relies on third-party transshipment hubs and clandestine procurement networks, such as the network operated by PETROV to secure access to such U.S.-sourced electronics.

j. Russia's weapons systems and military platforms — including rocket systems, drones, ballistic missiles, tactical radios, and electronic warfare devices — contain a range of predominantly Western-sourced components and micro-electronics that are critical to their functions. Russia's war effort in Ukraine is particularly dependent on components sourced from the United States. An array of U.S.-sourced components have been found in Russian military hardware recovered in Ukraine since Russia's February 2022 invasion. As set forth below, many of these components are subject to export controls in the United States. Categories of electronics components found in Russian military hardware in Ukraine include, among other things, the types of microcontrollers and integrated circuits that PETROV, CC-1, and CC-2 have fraudulently procured from U.S. distributors and illicitly shipped to Electrocom in Russia.

Background on Applicable Export Regulations

k. On August 13, 2018, the President signed into law the National Defense Authorization Act of 2019, which included the Export Control Reform Act (“ECRA”). *See* 50 U.S.C. § 4801 *et seq.* ECRA provides permanent statutory authority for the Export Administration Regulations (“EAR”), Title 15, Code of Federal Regulations, Sections 730-774.

l. ECRA provides that “the national security and foreign policy of the United States require that the export, reexport, and in-country transfer of items, and specified activities of United States persons, wherever located, be controlled.” 50 U.S.C. § 4811. To that end, ECRA grants the President the authority to “(1) control the export, reexport, and in-country transfer of items subject to the jurisdiction of the United States, whether by United States persons or foreign persons; and (2) the activities of United States persons, wherever located, relating to” specific categories of items and information. 50 U.S.C. § 4812. ECRA grants to the Secretary of Commerce the authority to establish the applicable regulatory framework. 50 U.S.C. § 4813.

m. ECRA authorizes the DOC to review and control the export from the United States of certain items, including goods, software, and technologies. The EAR outline the regulatory framework as provided by ECRA. In particular, the EAR restrict the export of items that could contribute to the military potential of other nations or that could be detrimental to U.S. foreign policy or national security. The EAR impose licensing and other requirements for items subject to the EAR to be lawfully exported from the United States or lawfully reexported from one foreign destination to another.

n. Through the EAR, the BIS reviews and controls the export from the United States to foreign countries of certain items. In particular, the BIS has placed restrictions on the export and reexport of items that the BIS has determined could make a significant contribution to the military potential or nuclear proliferation of other nations or that could be detrimental to the foreign policy or national security of the United States. Under the EAR, such restrictions depend on several factors, including the technical characteristics of the item, the destination country, the end-user, and the end-use.

o. The most sensitive items subject to EAR controls are identified on the Commerce Control List, or CCL, set forth in Title 15, Code of Federal Regulations, Part 774, Supplement Number 1. Items listed on the CCL are categorized by Export Control Classification Number (“ECCN”), each of which have export control requirements depending on destination, end-use, and end-user. As of April 8, 2022, license requirements for export to Russia were expanded to cover all items on the CCL. *See* 87 Fed. Reg. 12226 (Mar. 3, 2022); 87 Fed. Reg. 22130 (Apr. 14, 2022); 15 C.F.R. § 746.8.

p. As detailed below, PETROV, CC-1, and CC-2 have procured items controlled on the CCL, for which an export license from the DOC is required for the export, or reexport, to Russia of these goods. None of PETROV, CC-1, or CC-2 — nor their affiliated entities — have applied for, or received, a license from the DOC to ship controlled items to Russia.

q. Under ECRA, it is a crime to willfully violate, attempt to violate, conspire to violate, or cause a violation of any regulation, order, license, or authorization issued pursuant to the statute, including the EAR. *See* 50 U.S.C. § 4819(a)(1).

The Scheme

r. As described above, PETROV, CC-1, and CC-2 have perpetrated a scheme to evade and violate U.S. export controls by procuring and shipping controlled electronics with military applications to Russia. PETROV negotiated the purchase and export of the electronics with U.S.-based suppliers. To procure the technology, PETROV misrepresented that the goods would be shipped to Cyprus, Country-1, or Country-2 — which were in fact the locations of pass-through shipping companies operated and used by PETROV and his co-conspirators to transship the components to Electrocom in Russia. In particular, CC-1 used Company-1 in Country-1, and CC-2 used Company-2 in Country-2, to ship to Russia the sensitive U.S.-sourced components initially procured by PETROV. As an essential part of the scheme, PETROV, CC-1, and CC-2 concealed at all times from the U.S. exporters that the goods were destined for Russia.

s. Set forth below are three examples of exports of controlled technology that PETROV and his co-conspirators executed as part of this illicit scheme (“Export #1,” “Export #2,” and “Export #3”).

Export #1

t. In or about April 2022, approximately six weeks after Russia’s invasion of Ukraine, PETROV began communicating with a U.S.-based electronics distributor (“U.S. Distributor-1”), to purchase an array of micro-electronics, including electronics subject to DOC export controls, as set forth below.

u. In his initial correspondence with U.S. Distributor-1 in or about April 2022, PETROV misrepresented that Astraferos in Cyprus was the end-user of the items, falsely claiming that Astraferos is a “fabless manufacturer (fire security systems sphere),” when in fact PETROV operates Astraferos as a pass-through freight-forwarder, on behalf of Electrocom and in coordination with CC-1 and CC-2.²

v. The electronics that PETROV procured as part of the conspiracy from U.S. Distributor-1 in Export #1 included microcontrollers that are controlled on the CCL for Anti-Terrorism reasons under ECCN 3A991.a.2, such that a license from the DOC was required for the export or reexport to Russia of this item at all times relevant to this Complaint.

w. On or about July 14, 2022, following the above-referenced misrepresentations by PETROV about the nature of Astraferos and the destination of the electronics he was seeking to purchase, U.S. Distributor-1 sold PETROV and Astraferos approximately 15 16-bit flash microcontrollers, controlled under ECCN 3A991.a.2, and shipped the microcontrollers on or about July 16, 2022 from the United States to PETROV at an address in Cyprus, where PETROV operates the shell company Astraferos. On the invoice for the order provided to PETROV, U.S. Distributor-1 expressly noted that the 15 microcontrollers are

² PETROV, CC-1, and CC-2 communicated primarily in Russian. Descriptions of those communications in this Complaint reflect draft English translations. Throughout this Complaint, all communications are described in substance and in part, and quoted text appears as in the original messages, including any typographical and grammatical errors, except where alterations are indicated.

controlled under ECCN 3A991.a.2 and stated that the export of the microcontrollers is controlled by the U.S. Government, authorized “only to the country of ultimate destination for use by the ultimate consignee or end-user(s) herein identified,” and that the items are prohibited from being “resold, transferred, or otherwise disposed of, to any other country or to any person other than the authorized ultimate consignee or end-user(s).”

x. On or about July 20, 2022, PETROV received the 15 controlled microcontrollers in Cyprus. On or about July 27, 2022, CC-1 emailed PETROV requesting a status update on the microcontrollers. On or about July 28, 2022, PETROV informed CC-1 via email that he would send CC-1 the microcontrollers imminently, along with other micro-electronics procured from U.S. Distributor-1.

y. On or about July 29, 2022, CC-1 sent a contract, which included the 15 controlled microcontrollers, to an employee of a Russia-based logistics company (“Logistics Company-1”) who was responsible for coordinating the transportation of the goods to Russia. PETROV and his co-conspirators use Logistics Company-1 to transship sensitive, controlled electronics components — after PETROV has procured the goods from U.S. distributors and the goods have been shipped to PETROV and Astraferos in Cyprus — to Electrocom in Russia. The contract explicitly stated that the buyer of the goods is Electrocom, and the resulting invoice from Logistics Company-1 stated that the goods will be shipped to Saint Petersburg, Russia.

z. On or about September 20, 2022, CC-1 emailed a contract to an employee of a Russian Radio Frequency Identification (“RFID”) company (“RFID Company-1”) reflecting the sale by Electrocom to RFID Company-1 of approximately 185 microcontrollers of the same make and model as the 15 microcontrollers that U.S. Distributor-1 exported to PETROV and Astraferos. The contract indicated that Electrocom was shipping the microcontrollers to RFID Company-1’s Moscow address. Russia is reliant on Western imports for its RFID chips, which have significant military applications, including for use in tagging military assets for tracking purposes.

aa. A review of DOC records determined that a DOC license was not applied for, or obtained, in connection with the export of the 15 controlled microcontrollers in Export #1.

Export #2

bb. In or about July 2022, PETROV began purchasing DOC-controlled electronics from another U.S.-based distributor (“U.S. Distributor-2”). On or about July 27, 2022, in order to procure the sensitive controlled goods, PETROV misrepresented the nature of Astraferos’s business to a U.S. Distributor-2 employee in an email, stating that the function of Astraferos is “design and production” — when in fact, as described above, PETROV operates Astraferos as a pass-through freight-forwarder, on behalf of Electrocom and in coordination with CC-1 and CC-2, to obtain electronics for Electrocom.

cc. Export #2 included integrated circuits that are controlled on the CCL under ECCN 3A991.b.1.a for Anti-Terrorism reasons, such that a license from the DOC was required for the export or reexport to Russia of this item at all times relevant to this Complaint.

dd. On or about August 18, 2022, U.S. Distributor-2 shipped an array of dual-use electronics to Astraferos’s address in Cyprus. In the shipping, billing, and end-use records

and correspondence, PETROV falsely represented to U.S. Distributor-2 that the “ultimate consignee” of the controlled items was Company-1 — that is, the third-party distributor used by CC-1 to perpetrate the scheme on behalf of Electrocom. The invoice that U.S. Distributor-2 provided to PETROV for Export #2 noted the ECCN numbers under which the goods are controlled and explicitly stated that “re-export[ation]” or further “ship[ment] to another destination” was prohibited under U.S. export controls.

ee. On or about August 22, 2022, PETROV emailed CC-1 informing CC-1 that Export #2 would be sent the following day. PETROV also emailed CC-1 a shipping label and an invoice for Export #2, reflecting the controlled micro-electronics that had been shipped by U.S. Distributor-2 to Astraferos in Cyprus.

ff. On or about August 31, 2022, CC-1 emailed an employee of Logistics Company-1, providing Logistics Company-1 with the weights for each of the items ordered, including the export-controlled integrated circuits. On or about September 2, 2022, CC-1 sent a contract for the order to Logistics Company-1. The contract set forth that the buyer of the goods was Electrocom, and the resulting invoice from Logistics Company-1 stated that the goods would be shipped to Saint Petersburg, Russia.

gg. A review of DOC records determined that a DOC license was not applied for, or obtained, in connection with the export of the integrated circuits in Export #2.

Export #3

hh. On or about July 15, 2022, PETROV ordered from U.S. Distributor-1, via email, 90 microcontrollers — specifically, 16-bit flash digital signal processors and controllers — based on his same April 2022 misrepresentations to U.S. Distributor-1 that Astraferos was the end-user of the goods purchased from U.S. Distributor-1 and that Cyprus was the final destination.

ii. The microcontrollers procured in Export #3 were controlled on the CCL under ECCN 3A991.a.2 for Anti-Terrorism reasons, such that a license from the DOC was required for the export or reexport to Russia of this item at all times relevant to this Complaint.

jj. On or about January 11, 2023, relying on the above-referenced misrepresentations by PETROV to U.S. Distributor-1 about the nature of Astraferos and the final destination of the goods, U.S. Distributor-1 shipped the 90 controlled microcontrollers from the United States to PETROV at Astraferos’s address in Cyprus. On the invoice for the order provided to PETROV, U.S. Distributor-1 expressly noted that the microcontrollers are controlled under ECCN 3A991.a.2 and that the export of the microcontrollers is controlled by the U.S. Government, authorized “only to the country of ultimate destination for use by the ultimate consignee or end-user(s) herein identified,” and that the items are prohibited from being “resold, transferred, or otherwise disposed of, to any other country or to any person other than the authorized ultimate consignee or end-user(s).”

kk. On or about January 31, 2023, PETROV shipped the 90 controlled microcontrollers to Company-2 in Country-2, and updated his superior at Electrocom, CC-2, about the status of the shipment. CC-1 participated in ensuring that the shipment reached Russia; among other things, CC-1 emailed CC-2 a contract between Electrocom and Company-2 for the

microcontrollers. The consignee on the contract, which was not provided to U.S. Distributor-1, is listed as Electrocom alongside its address in Saint Petersburg, Russia.

ll. Over the following weeks, CC-1 apprised CC-1's Electrocom colleagues, including CC-2, of the shipment of the 90 microcontrollers. For example, on or about February 8, 2023, CC-1 emailed CC-2 the shipping label for the shipment that included the microcontrollers. CC-1 was also tracking other Russia-bound shipments around this time. On or about February 27, 2023, CC-1 emailed an employee of Aviasystems, a Russian aerospace company and military supplier that focuses on aircraft navigational support, flight controls, and landing equipment, to advise that a shipment of goods had arrived at Russian customs, and a second shipment was on the border. CC-1 wrote, "Due to the fact that they are dual-use, we try to make certificates for them," an apparent reference to the military applications for the goods and CC-1's efforts around this time to facilitate shipment of such goods to Electrocom in Russia.

mm. On or about March 1, 2023, CC-2 sent a Company-2 employee two emails reflecting that Export #3 involved Cyprus, Country-2, and Russia. CC-2 attached "invoices from Cyprus to [City-1], as well as from [City-1] to Russia," referring to the city in Country-2 where Company-2 is based. CC-2 attached the Astraferos invoice that lists the 90 controlled microcontrollers, and indicated that Electrocom was buying the goods from Company-2. CC-2 added, "They have items that need to be left in a warehouse in [City-1]," and stated that "The remaining positions," which CC-2 made clear included the 90 controlled microcontrollers, "must be shipped to Russia on the provided invoice."

nn. In or about early March 2023, the Export #3 microcontrollers arrived at Electrocom's address in Saint Petersburg, Russia.

oo. A review of DOC records determined that a DOC license was not applied for, or obtained, in connection with the export of the microcontrollers in Export #3.

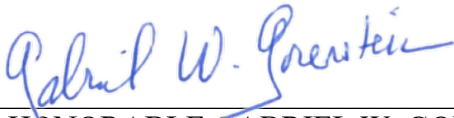
(continued on next page)

WHEREFORE, I respectfully request that a warrant be issued for the arrest of ARTHUR PETROV, the defendant, and that he be arrested, and imprisoned or bailed, as the case may be.

/s/ Brian Smith

BRIAN SMITH
Special Agent
Federal Bureau of Investigation

Sworn to me through the transmission of this Complaint by reliable electronic means, this 11th day of August 2023.



THE HONORABLE GABRIEL W. GORENSTEIN
United States Magistrate Judge
Southern District of New York