



Baltics - Belgium - Finland - France - Germany - Italy

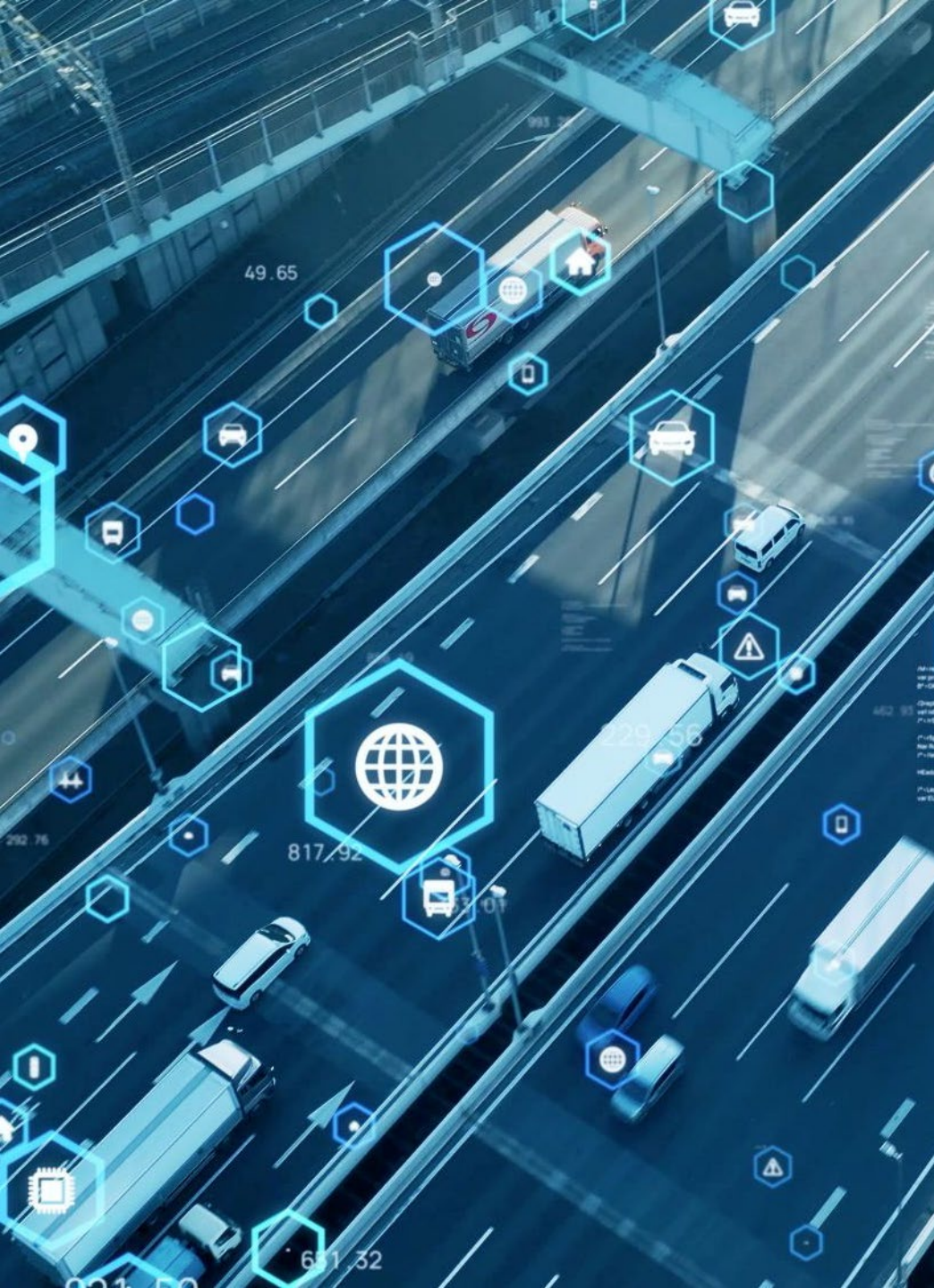
Netherlands - Norway - Poland - Spain - Switzerland - United Kingdom

Illicit Acquisition and Russia

European Sanctions and Export Control Society

info@europeansanctionssociety.org





Agenda

World of Illicit Acquisition

Foreign Direct Investment

Cyber Threats

Intelligence Collection

Illicit Procurement

Order

Payment

Shipping

Case Studies

Prevention and Risk Mitigation



Baltics - Belgium - Finland - France - Germany - Italy

Netherlands - Norway - Poland - Spain - Switzerland - United Kingdom

Illicit Acquisition

World of Illicit Acquisition and Counterproliferation



Above the Surface Overt Activities



- Outreaches
- Subpoenas
- Procurement
- Press Releases
- Export Controls

COMPANY A

COMPANY B

COMPANY C

- Methods of Order
- Listings
- Trade Restrictions
- Is Informed Letters
- End-Use Checks

- Regulations
- Criminal and Admin Investigations
- Methods of Shipping
- Methods of Payment
- Sanctions



Below the Surface Covert Activities

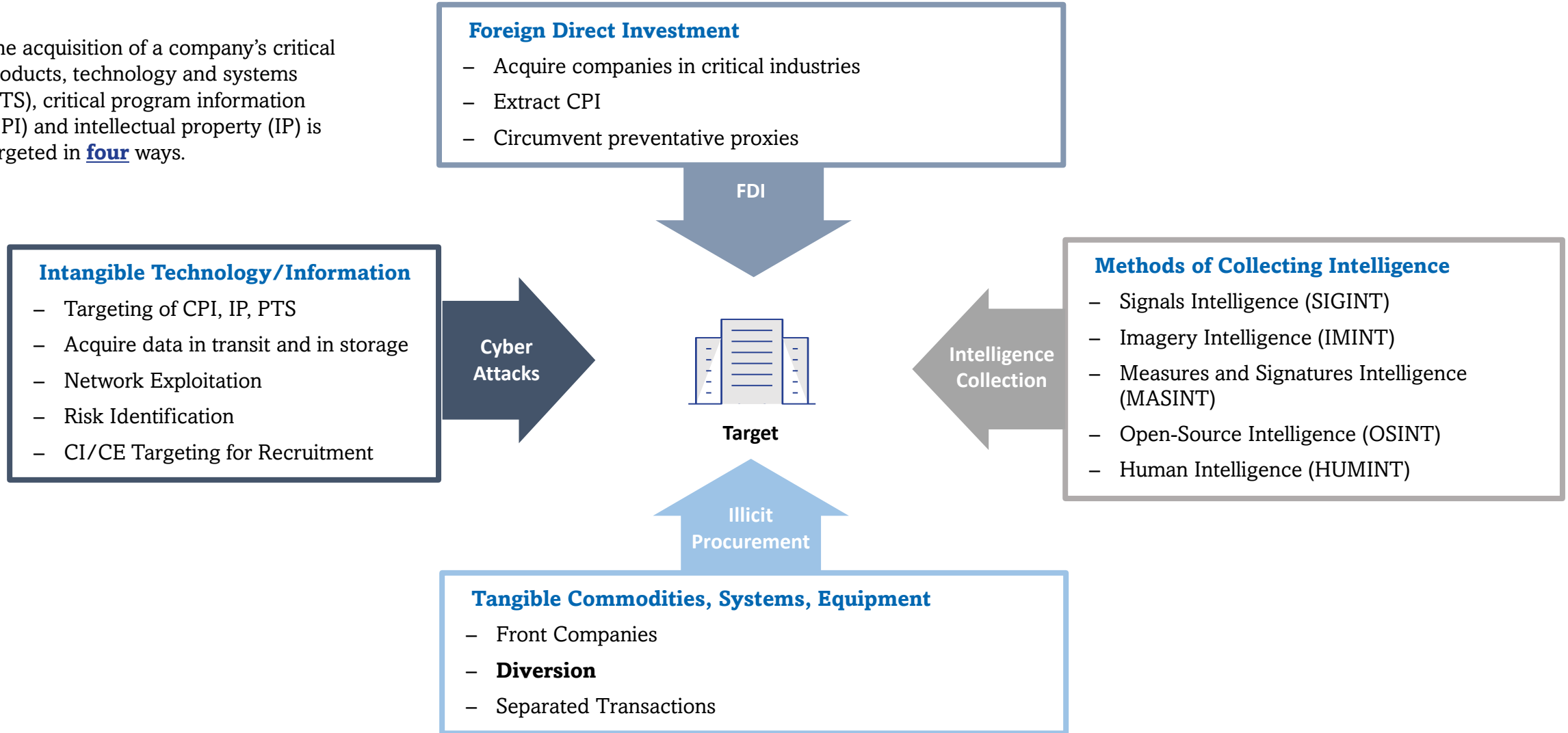
- Intelligence Collection
- Measure and Signatures Intelligence (MASINT)
- Signals Intelligence (SIGINT)
- Human Intelligence (HUMINT)
- Open-Source Intelligence (OSINT)
- Imagery Intelligence (IMINT)

- Inter-Agency Cooperation
- Cyber Intrusions
- Covert Enforcement Operations
- Undercover Operations
- Counterintelligence Operations
- Targeting of Critical Program Information
- Multilateral Approaches to Licensing Reviews
- Government Sharing of Information
- Outbound Inspections
- Monitoring
- Tracking Shipments

- Espionage
- Theft of Trade Secrets
- Recruiting of Witting and Unwitting Sources
- Sabotage
- Exploitation
- Disruption
- Diversion
- IP Theft

Multi-Pronged Approach to Illicit Acquisition

- The acquisition of a company's critical products, technology and systems (PTS), critical program information (CPI) and intellectual property (IP) is targeted in **four** ways.



What is Critical Program Information?

Critical Program Information, or CPI, can be defined as a company's elements that contribute to technical competitive advantage, and that, if compromised, could undermine a company's **current and future market share and profitability**.

Critical Program Information

The protection of a company's Critical Program Information (CPI) is a three-part process including enhanced cyber security, foreign threat protection and a robust export control and sanctions program.





Baltics - Belgium - Finland - France - Germany - Italy

Netherlands - Norway - Poland - Spain - Switzerland - United Kingdom

Foreign Direct Investment



Foreign Direct Investment

- Directly acquire companies in prominent industries
- Establish companies in foreign countries to build and grow, then buy out other companies
- List on the stock exchange to gain capital from the U.S.
- Government subsidizing in certain industries, in certain regions of the world, to gain market share for intelligence and revenue generation reasons.



FDI Case Study – Momentum and Stable Road

- The U.S. Securities and Exchange Commission said the companies and Stable Road Acquisition Company Chief Executive Brian Kabot agreed to pay \$8 million to resolve allegations they misled investors about Momentum Inc.'s technology and national security risks associated with its former CEO Mikhail Kokorich.
 - U.S. concerns with Kokorich's connections to Russian government.
 - Momentum sought to merge with Stable Road.
 - Became publicly traded to obtain capital.
 - Fined for violations to cover for national security risks.
 - New CEO assigned.





Baltics - Belgium - Finland - France - Germany - Italy

Netherlands - Norway - Poland - Spain - Switzerland - United Kingdom

Intelligence Collection



5 Intelligence Disciplines



Signals Intelligence (SIGINT)



Open-Source Intelligence (OSINT)



Imagery Intelligence (IMINT)



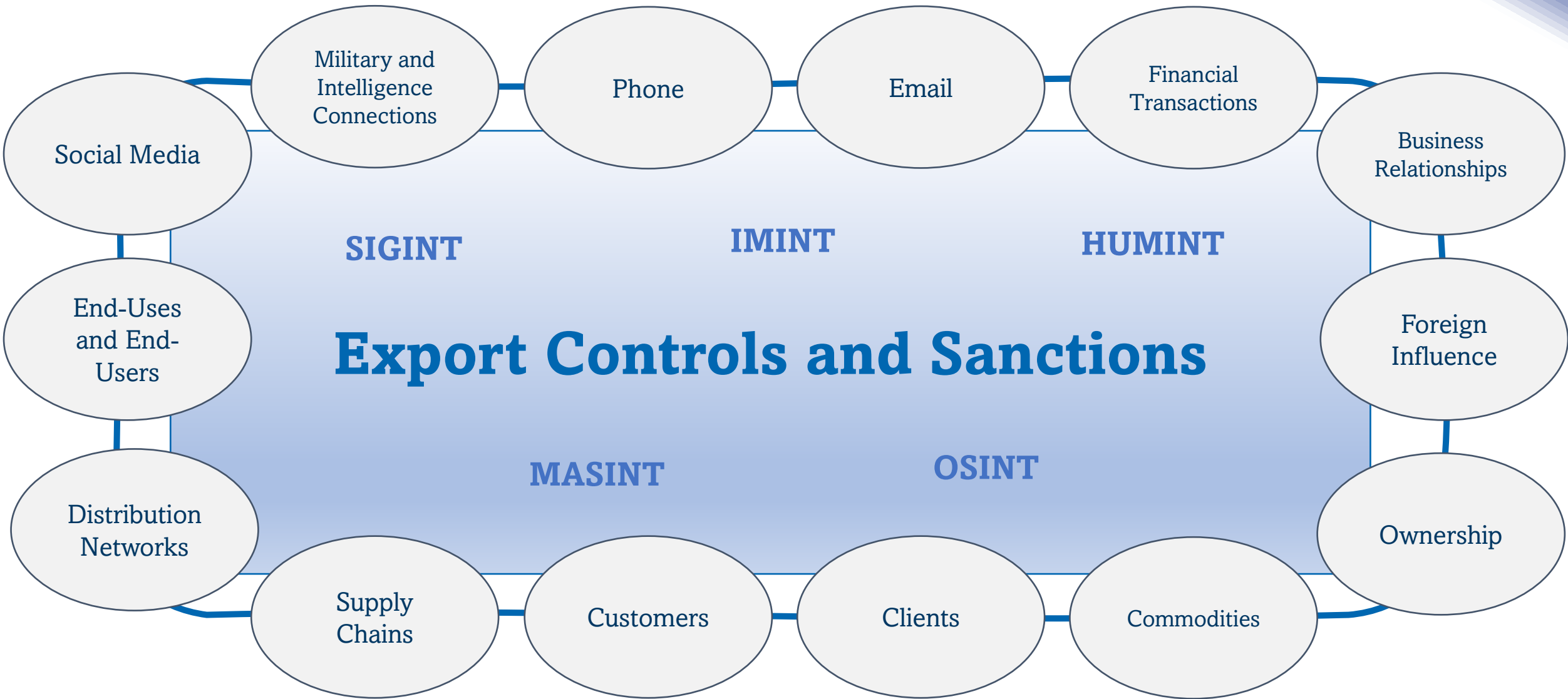
Human Intelligence (HUMINT)



Measures and Signatures Intelligence (MASINT)



Intelligence Collection



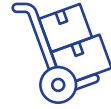
Intelligence Officers and Industry



Attaches



Distributors



Logistics companies



Professors



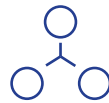
Research Students



Shipping Companies



Front Companies



Trade Associations



Businessmen
(Recruited vs. Implanted)





Baltics - Belgium - Finland - France - Germany - Italy

Netherlands - Norway - Poland - Spain - Switzerland - United Kingdom

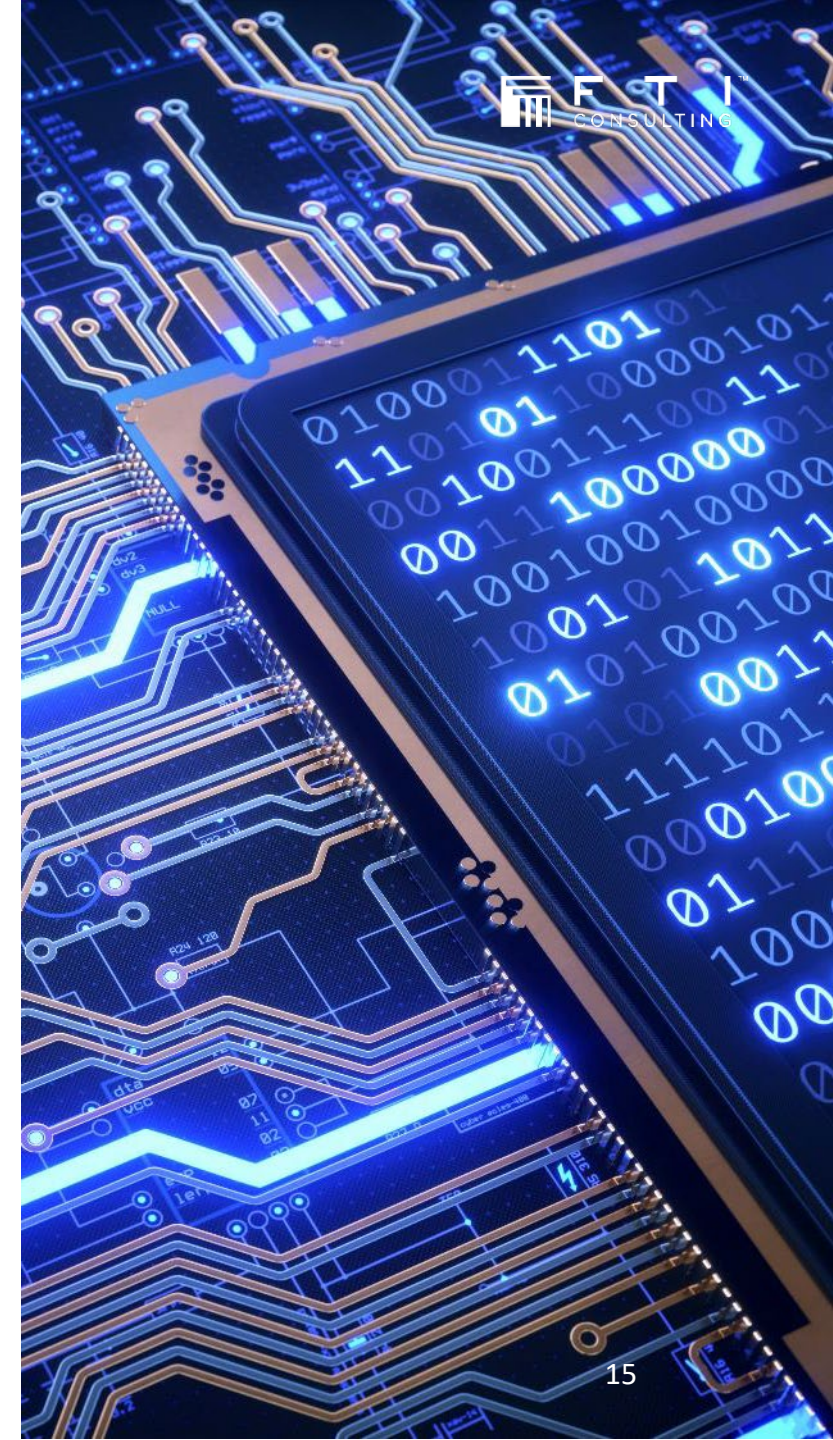
Cyber Threats

Historic Examples

- Presidential Election Hacking (GRU)
- U.S. Defense Contractors (Hacker groups)
- Global Energy Sector (FSB)
- Oil and Gas (Triton malware)
- Satellites
- DDOS attack on Topeka 501 District

Methods

- Selling computer networking equipment
- Selling software, back door updates
- FSB and encryption
- Development of apps
- Social media
- Ransomware



Attempted Acquisition of Technology

- Critical Program Information (CPI)
- Information regarding equipment
- Diagrams
- Schematics
- Plans
- Spec sheets
- User Manuals

Collection and Exploitation

- Targeting for recruitment
- Sabotage
- Disruption
- Military modernization
- Collecting intelligence information
- Extraction of data





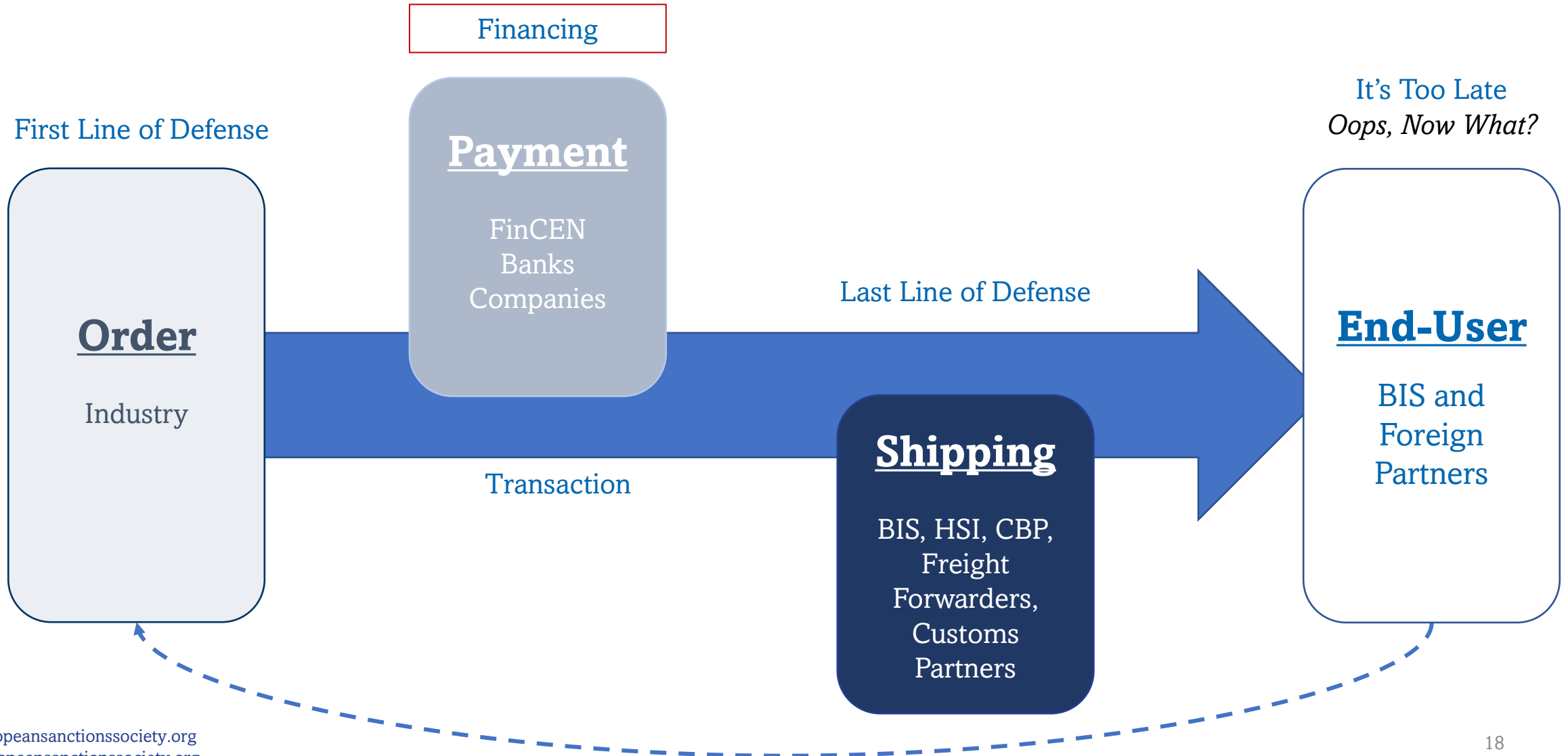
Baltics - Belgium - Finland - France - Germany - Italy

Netherlands - Norway - Poland - Spain - Switzerland - United Kingdom

Illicit Procurement



Illicit Procurement





Most Frequently Targeted Commodities

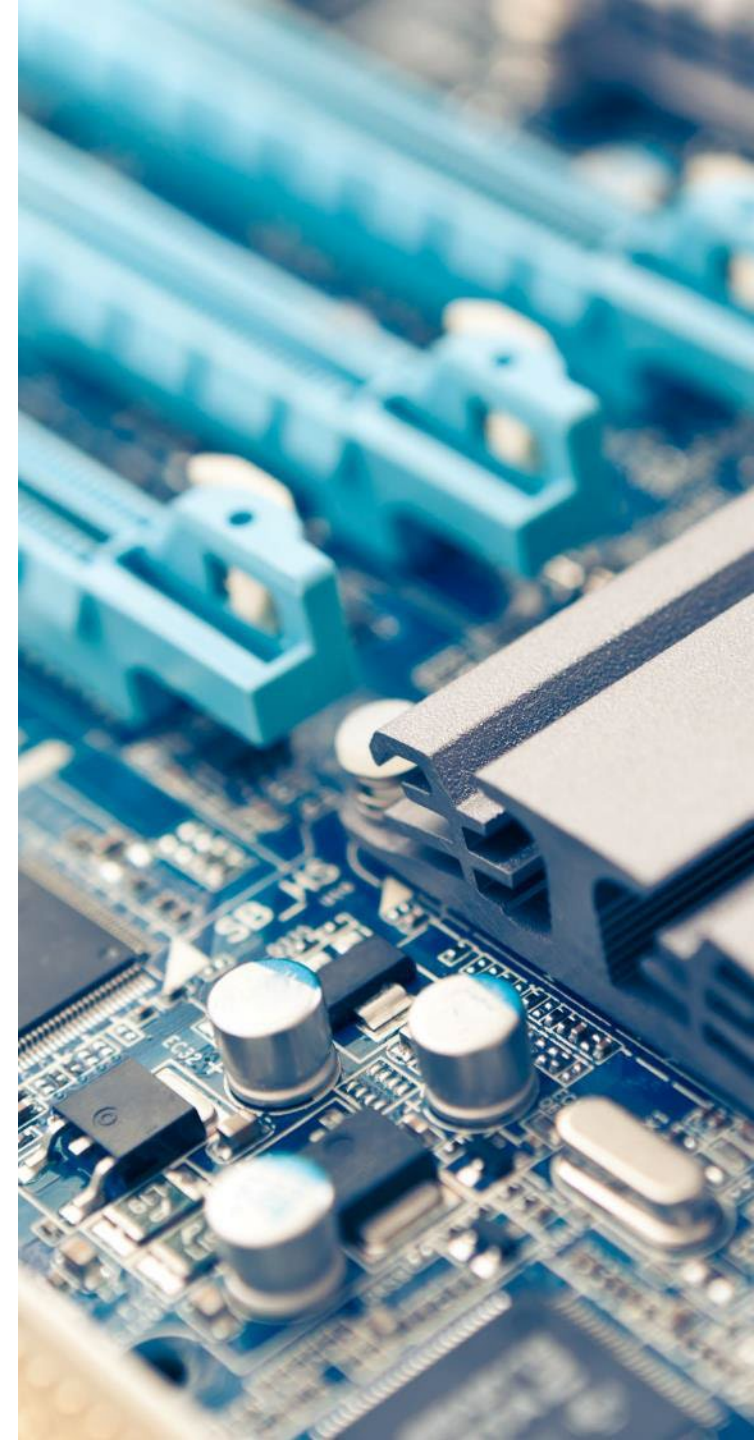
(Historically)

Commodities:

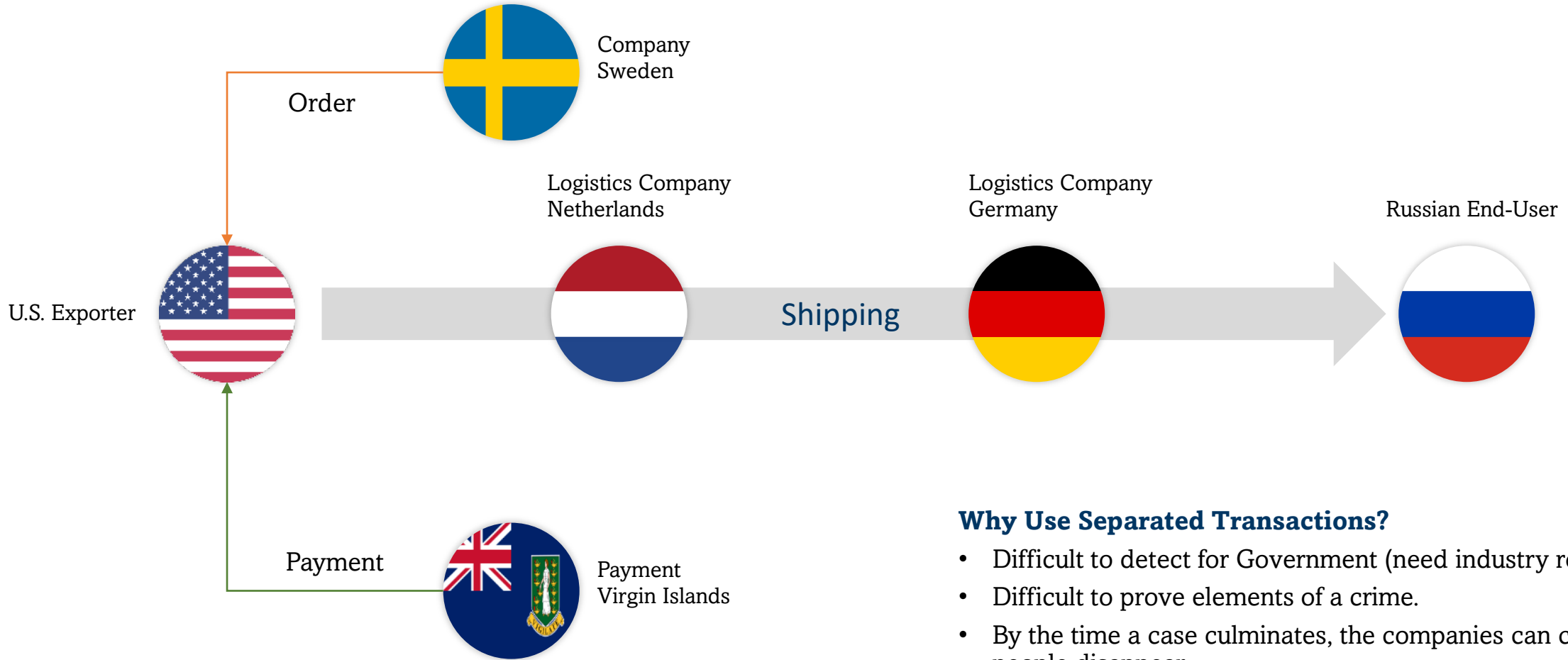
- Microelectronics
- Semiconductors
- Semiconductor manufacturing equipment
- Night vision
- Thermal vision
- Scopes
- Aircraft parts
- Computer networking devices
- Encryption
- Deep sea submersible equipment
- Underwater communication equipment

Uses:

- Missiles
- Torpedoes
- Space program
- Special Forces
- Military modernization
- Underwater monitoring
- Secure communications
- Security services
- Chemical, Biological, Nuclear weapons



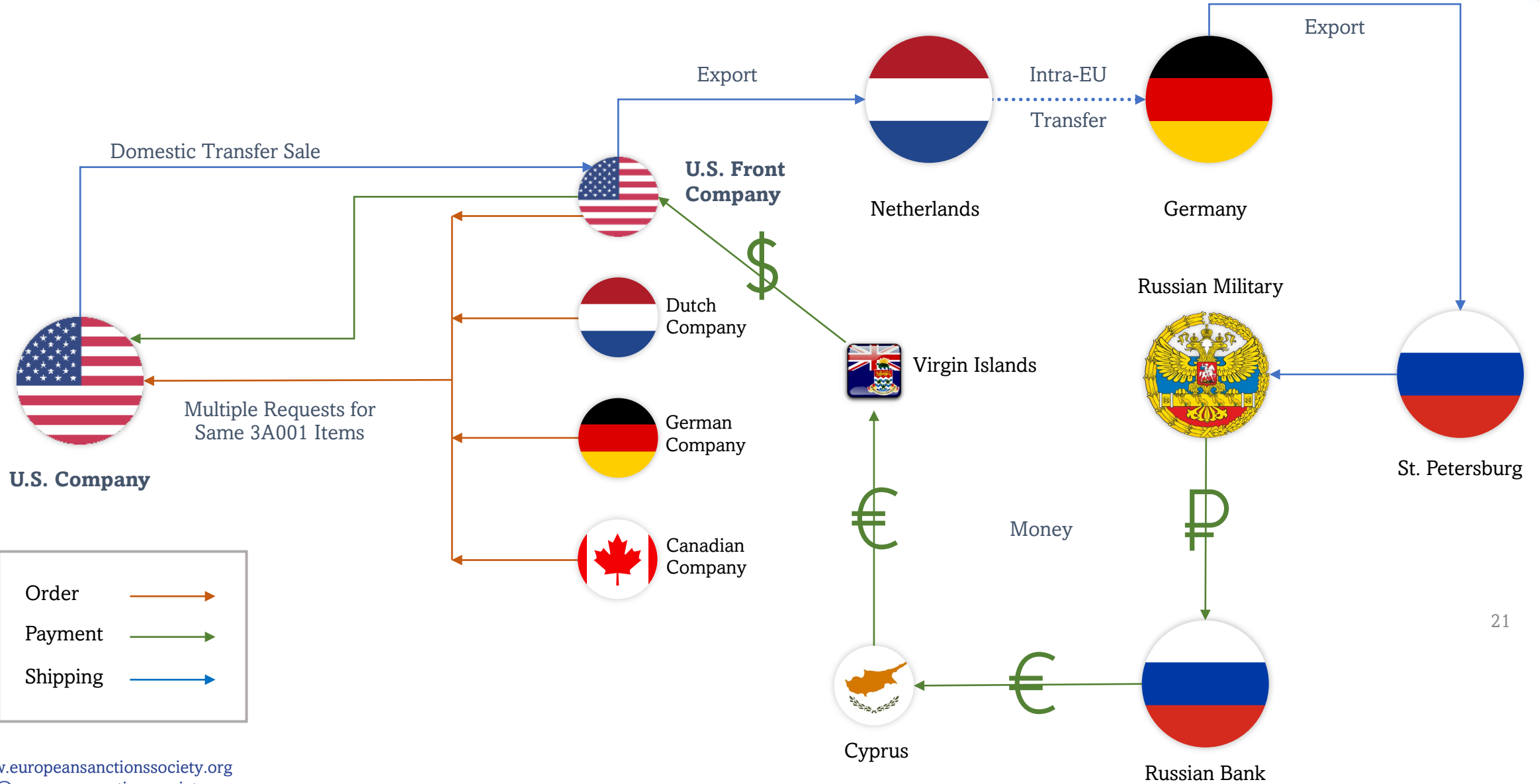
Separated Transactions



Why Use Separated Transactions?

- Difficult to detect for Government (need industry reporting).
- Difficult to prove elements of a crime.
- By the time a case culminates, the companies can close, and people disappear.

Procurement Attacks



Organized Crime, Oligarchs, Funding for Illicit Acquisition

- To fund illicit acquisition supporting military modernization and development, the Russian government uses a multipronged approach to raising money.
- Oligarchs and organized criminal syndicates make contributions to the Russian government directly through SOEs as well as certain companies under government influence. These contributions can provide capital to government sponsored procurement networks funding intelligence services, illicit acquisition, and military operations.



Oil and Gas



Defense Sales



Metals and Mineral



Iron and Steel



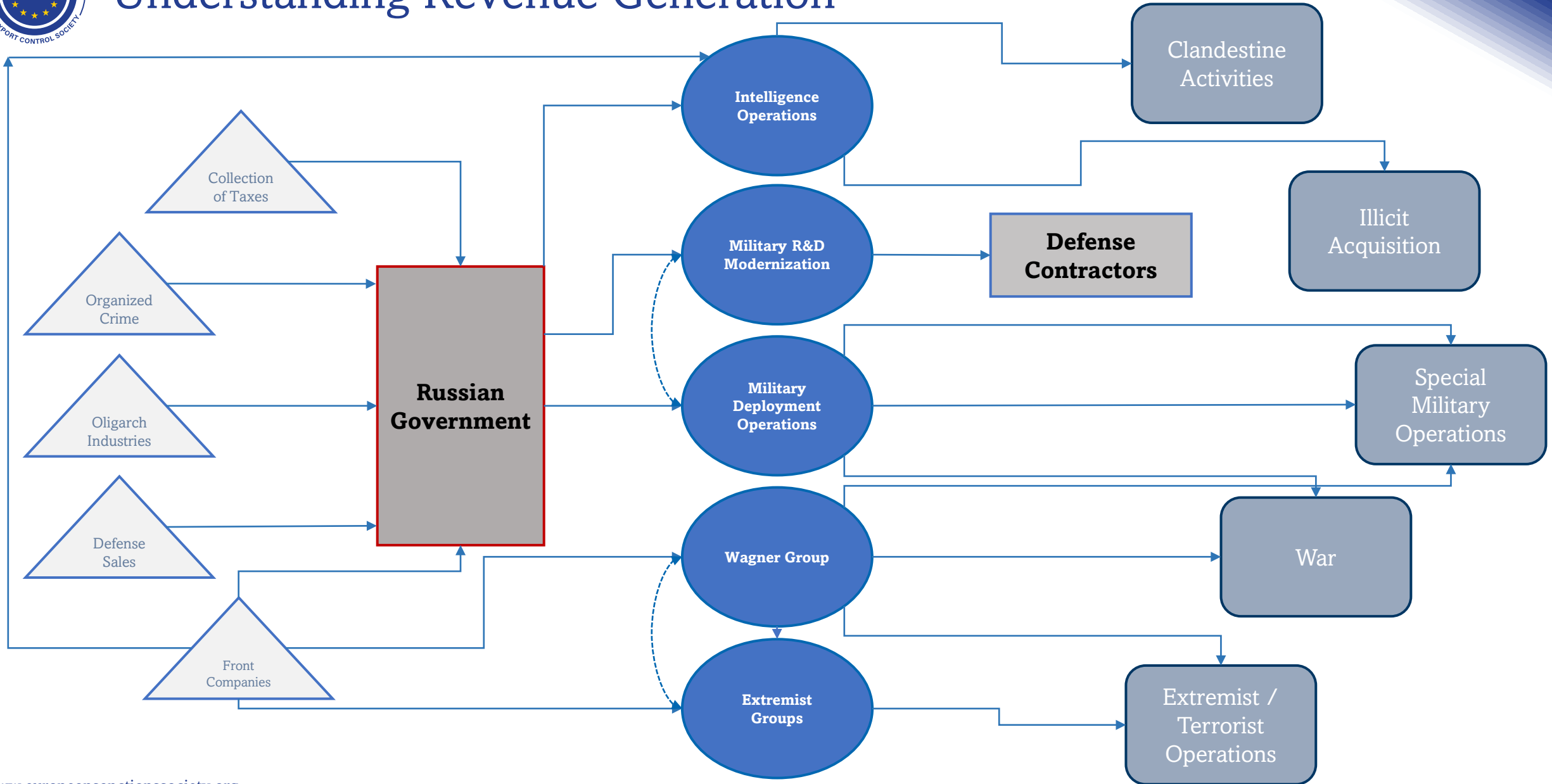
Railroads



Taxes



Understanding Revenue Generation





Baltics - Belgium - Finland - France - Germany - Italy

Netherlands - Norway - Poland - Spain - Switzerland - United Kingdom

Diversion Risks

Historic Russian Shipment Routes

Other Countries:

- Belarus
- Slovakia
- Hungary



Departure from the EU:

- Finland
- Latvia
- Lithuania
- Estonia
- Germany



Arrival to the EU:

- Netherlands
- Germany



Future Risk of Diversion

- **Building Partnerships with other Countries (Iran, China, NK, and others)**
- **Asian Networks Established**
- **Eurasian Customs Union (EACU) –**
 - **Armenia** – Included in Commerce Country Group D, with case-by-case license review policy for civil end users/uses. No license requirements at all for any exports of U.S.-origin items controlled only for AT reasons.
 - **Belarus** – Sanctioned (See Available License Exceptions)
 - **Kazakhstan** – Included in Commerce Country Group D, with case-by-case license review policy for civil end users/uses. No license requirements at all for any exports of U.S.-origin items controlled only for AT reasons.
 - **Kyrgyzstan** – Included in Commerce Country Group D, with case-by-case license review policy for civil end users/uses. No license requirements at all for any exports of U.S.-origin items controlled only for AT reasons.
 - **Russia** – Sanctioned (See Available License Exceptions)

***Board of Directors Remarks** – Items exported to these areas as ultimate consignees or end-users can be subject to diversion and sent to Russia and provided to sanctioned and/or listed entities with minimal insight from government and industry.*



Use of Third-Party Countries for License Exceptions

- The use of license exceptions to export certain commodities to authorized destinations can result in the risk of diversion.
- Whereas a policy of denial exists to send certain sensitive commodities to Russia, illicit acquisition networks can seek to obtain items from the U.S. using license exceptions to companies in Europe and Asia listed as ultimate consignees and then divert items directly or indirectly to Russia.

CIV – Civilian Use

APP – Computers

LVS – Limited Value Shipment

STA – Strategic Trade Authorization

GFT – Gift Parcels and Donations

APR – Additional Permissive Re-Exports

RPL – Replacement Parts and Equipment

AGR – Agricultural Commodities

TSR – Technology and Software Under Restriction



Baltics - Belgium - Finland - France - Germany - Italy

Netherlands - Norway - Poland - Spain - Switzerland - United Kingdom

Recent Case Studies




POLITICS

The Swedes: Russian couple arrested in Stockholm has ties to GRU and Swedish military intelligence, lives next door to Skripals' poisoner

28 November 2022



Baltics - Belgium - Finland - France - Germany - Italy

Netherlands - Norway - Poland - Spain - Switzerland - United Kingdom

What can we do?



Recommendations

- Think like a counterintelligence/counterespionage agent
- Develop a **risk-based** approach to a compliance program
- Display positive commitments to compliance
- Conduct business with members of trade associations, to include logistics/freight forwarders with displayed commitments to compliance
- Train employees on risk-based approaches
- Promote training for members of supply chains
- Identify and database **red flags**
- Report red flags and suspicious activities
- Conduct a 5 year look back – **VSDs**
- Identify critical areas to allocate limited resources – avoid over-compliance

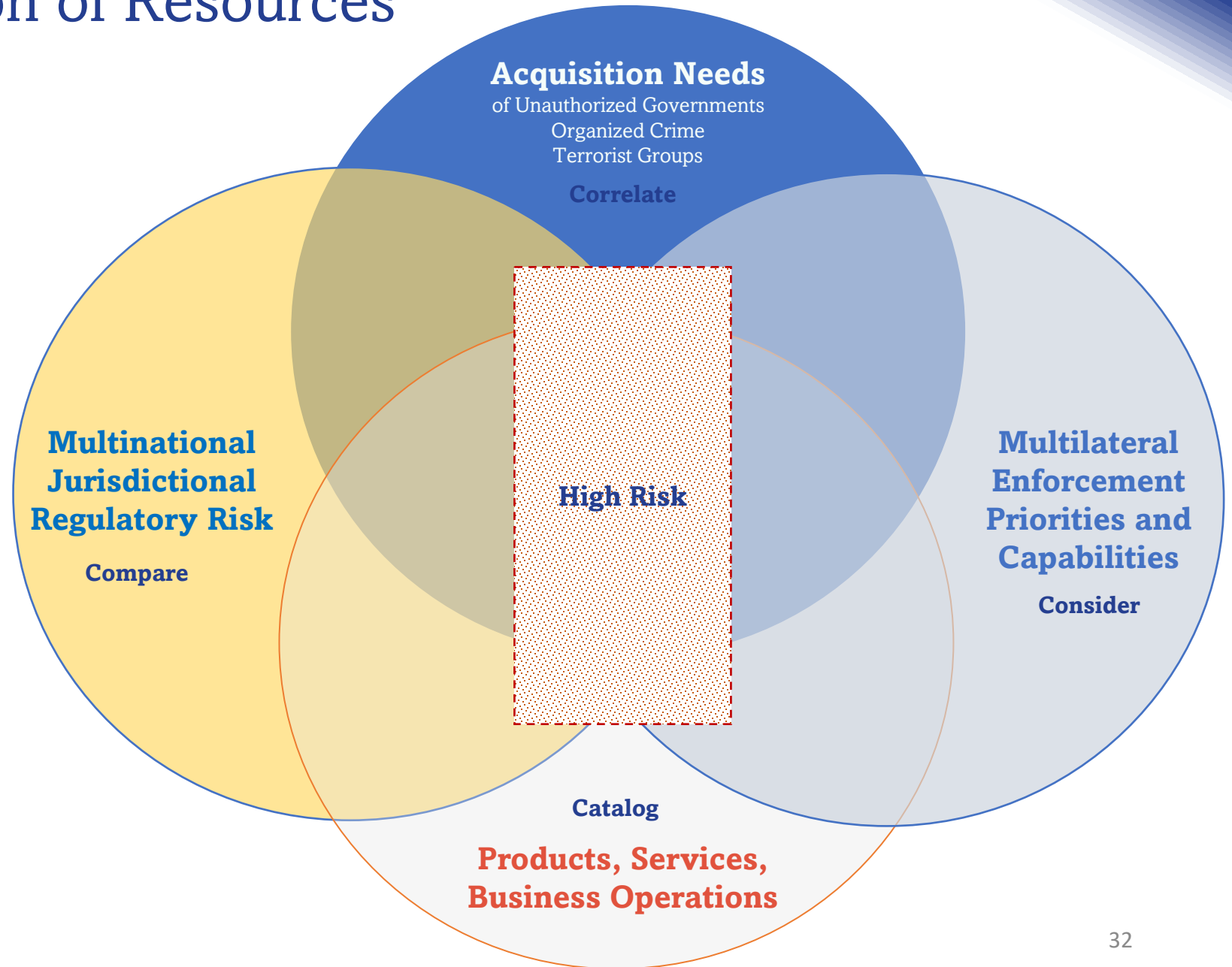
Efficient Allocation of Resources

Identifying Resource Focus

RESOURCE ALLOCATION (The 4 Cs)

- **C**atalog what products and services a company offers,
- **C**orrelate to the acquisition needs of nefarious entities,
- **C**ompare to multilateral regulations, and
- **C**onsider the priorities and capabilities of enforcement agencies.

Tip: Avoid over compliance





Baltics - Belgium - Finland - France - Germany - Italy

Netherlands - Norway - Poland - Spain - Switzerland - United Kingdom

Future Special Training Sessions

Illicit Acquisition and China

Illicit Acquisition and Iran

Diversion Case Studies

Intelligence and Export Controls and Sanctions Compliance

www.europeansanctionsociety.org



Baltics - Belgium - Finland - France - Germany - Italy

Netherlands - Norway - Poland - Spain - Switzerland - United Kingdom

Questions

European Sanctions and Export Control Society

info@europeansanctionssociety.org

