MOTIVE INTERNATIONAL

FEBRUARY 2023

ISSUE PAPER

1250 Connecticut Ave, Suite 700 Washington, DC 20036 +1 (202) 261-3587 www.motiveinternational.com

Countering Adversary Efforts to Divert Sensitive Technologies

Top: Automated Delivery Robot (stock photo)
Bottom: US Army Titan Robot with Protector Javelin (QinetiQ file photo)

About Motive

Motive International is a Washington, DC-based social enterprise with a mission to mitigate conflict and enhance global stability and sustainability. We advance our mission through client programs and self-funded impact initiatives.

Visit www.motiveinternational.com to learn more and read case studies.

Summary

Malign actors have recently increased their efforts to gain access to strategic and sensitive technologies that can provide an advantage on the battlefield, a threat that requires urgent understanding and response. This threat is particularly acute in the Baltic states, which face a unique set of circumstances in the control of strategic goods. The Baltics are home to some of the EU's most vibrant innovation ecosystems, which excel in the development of technologies most desired by malign actors seeking to develop advanced weapons, including autonomous weapons. [1] Baltic industry and academia produce world-class artificial intelligence/machine learning (AI/ML), sensor technology, blockchain encryption, machine vision, robotics, and other emerging and disruptive technologies (EDTs). Russia's invasion of Ukraine has increased Kremlin demand for these military-relevant technologies and intensified malign efforts to acquire them from nearby Baltic states. Our extensive engagement culminated in tabletop exercises (TTXs) hosted by Motive International in late 2022 that simulated malign actor diversion tactics against government and industry in the Baltics and illuminated regulatory and capability gaps and opportunities to strengthen policy and practice. Recommendations include specific changes in how industry, government, and multi-lateral organizations identify threats and collaborate to counter them.

The Innovators Next Door Project

In 2021, Motive International, funded by the U.S. Department of State's Export Control and Related Border Security (EXBS) Program, launched the Innovators Next Door Project in partnership Lithuania's and Latvia's Ministries of Foreign Affairs (MFA) and industry partners in Estonia. In the Project's first year, Motive meticulously mapped each country's stakeholder and threat landscape, carried out expert analysis of national and Baltic-wide technology diversion dynamics, and engaged extensively with hundreds of representatives from industry, academia, civil society, national governments, and the European Commission.

Tabletop exercise materials from the Innovators Next Door Project event in Vilnius, Lithuania in October 2022. (Motive photo)

These activities informed in-person tabletop exercises (TTX) in Vilnius and Riga in October 2022. The TTXs presented government and industry stakeholders with simulated diversion threat scenarios, prompting them to respond through interactive gameplay. Motive facilitated and scored the game based on how well participants were able to recognize and mitigate diversion risks. Following the exercise, national policy leaders, legal experts, and industry executives led workshops to discuss gaps revealed in the exercise and identify concrete options to strengthen counter-diversion policy, practice, and cross-sector coordination. Project findings and recommendations are presented below.

> Most governments around the world have sub-optimal mechanisms to coordinate with the entities whose technologies face the greatest risk for diversion.

Gaps in Prevailing Policy and Practice

Transatlantic alignment and coordination on sanctions, export control regimes, and investment screening is robust, yet significant policy and practice gaps remain. Several categories or sub-categories of dual-use technology (e.g., some quantum, biotechnology, advanced material, and software) are not subject to licensing or reporting requirements under EU regimes. Furthermore, U.S. and EU export controls lack the ability or authority to regulate certain intangible technology transfers (ITT). Many European governments lack adequate foreign investment screening regulations or treat foreign investment separately from strategic goods control.

In addition to regulatory gaps, most governments around the world have sub-optimal mechanisms to coordinate with the entities whose technologies face the greatest risk for diversion, namely industry and academic institutions that handle EDTs. The lack of familiarity and trust between government and industry, bandwidth constraints, and absence of formal mandates for governments to conduct industry outreach contribute to sub-optimal coordination. The uptick in diversion attempts by Kremlin actors has magnified this shortcoming. This is particularly true in industry segments such as autonomy-enabling AI/ML algorithms, sensor integration software, and cloud data platforms, which are largely ungoverned by export control regimes and where government-to-industry connections are most nascent.

Mounting evidence shows these are precisely the segments of greatest interest to military and intelligence apparatuses of Russia, China, and others, underscoring the need for improved coordination as an important counter-diversion safeguard. [2]

Recent diversion incidents offer evidence of this need. In 2018, Russian operatives targeted an unsuspecting cloud computing company in Lithuania to divert software and data for use in Kremlin missile launching systems. [3] Despite working in a sensitive domain, the Lithuanian firm had not considered the possible military applications of their technology and therefore lacked basic safeguards to prevent nefarious acquisition of their data or software. While the Lithuanian government used its investment screening mechanisms to stop a Kremlin-backed company from investing in the Lithuanian firm, this example demonstrates that, absent government outreach, firms and institutions that transact largely in the commercial, non-security sector, remain unaware of the dual-use nature of their innovations, much less of policies and practices related to strategic goods control.

An export license or investment denial made by one competent authority does not guarantee a neighboring EU state will make the same decision for the identical transaction. Divergent national regulation incentivizes both licit and illicit actors to seek out more lenient states in which to operate.

Key Findings

By deeply examining and simulating the dynamics described above with regional stakeholders, Motive's Innovators Next Door Project identified the following gaps and conditions as key contributing factors to unmitigated diversion risk in the Baltic tech sector:

Export Control Loopholes: Existing national export control regimes in the region do not adequately address "grey zone" items and situations. For example, export control lists maintained in EU framework law (Regulation (EU) 2021/821) that correspond with national regulations exclude entire categories of dual-use EDTs (e.g., most software and some advanced hardware), leaving sensitive technologies outside the jurisdiction of most regulatory controls. Moreover, myriad situations involving intangible technology transfers (ITT) are not subject to export licensing or reporting requirements.

Latvian government officials collaborate with EXBS representatives and Motive implementers during the Project TTX in Riga in October 2022. (Motive photo)

Divergent National Regulations: Although the EU's export control regime falls under EU common trade policy, individual member states have discretion to implement frameworks with wide latitude and have minimal obligations to enforce or honor determinations made by other member states. This means an export license or investment denial made by one competent authority does not guarantee a neighboring EU state will make the same decision for the identical transaction. In other words, the denial of an export license in one member state is not binding on other member states. Rules surrounding government obligations to report or share information or rationale on license denials is voluntary and can be inconsistent, limiting the effectiveness of systems intended to harmonize export controls across the EU. Divergent national regulation undermines the idea of a common application of export controls and incentivizes both licit and illicit actors to seek out more lenient states in which to operate.

Oversight Blind Spots: Although transactions for items not on the EU export control list can be denied by national authorities under "catch all" authority, this rarely occurs because authorities are not generally aware of transactions involving "unlisted" items. In other words, regulators cannot regulate what they are not aware of. Compounding blind spots is a general hesitation among officials to exercise catch all denial authority, if and when they do identify a suspicious transaction.

Unique Aspects of Non-Traditional Exports: There is uncertainty at the EU and national levels about jurisdiction over strategic goods transactions that take place entirely in the cyber domain, such as software transfers, and those that involve transfer of items to foreign entities or individuals physically present in the EU – a situation referred to as "deemed" exports in the U.S. context. These kinds of transactions remain largely ungoverned, allowing malign actors to acquire sensitive items and know-how lawfully simply by transacting while physically present in the EU or on digital platforms that lack clear national jurisdiction.

Foreign Investment Vulnerabilities: Many countries have procedures for export control and foreign investment screening, but the two are often applied separately, with the latter not routinely viewed through the lens of strategic goods control. As a result, a nefarious actor may gain access to sensitive EDTs by becoming a beneficiary of a firm in an industry segment not routinely subject to foreign investment screening. Furthermore, most foreign investment restrictions only apply when the total value or beneficiary share is above a certain threshold, allowing foreign access to sensitive technologies or IP through small-scale investments.

Lack of Integration with Business Promotion Arms of Government: Government investment and innovation promotion agencies tend not to be meaningfully engaged in strategic goods control within their own governments, which both misses opportunities for inter-ministerial information exchange and may create risk. Business promotion agencies have unique insights on market dynamics that could enrich the government's threat picture or provide actionable information on specific licensing or investment cases if they were better integrated in strategic goods regulation. Moreover, more integration could reduce the risk of business promotion agencies inadvertently enabling nefarious foreign investments or cross-border collaborations.

Minimal Government-Industry Collaboration: Last, but perhaps our most significant and addressable finding, is the lack of effective mechanisms for strategic goods regulators to interact with the industry actors at greatest risk of having their technologies targeted for diversion. Few channels exist for officials to educate industry about threats or for the two sectors to exchange information on issues of concern. This prevents the two sides from enhancing their collective threat picture, results in industry being uninformed of current policies, and forecloses opportunities to craft policy that protects national security and business interests. It also limits government visibility and understanding of "grey zone" transactions and trends described above. In some cases, lack of cross-sector interaction stems from distrust or wariness of government, with firms routinely finding ways to operate just below the threshold of regulatory reach to reduce compliance burdens, minimize delays, or simply to avoid interacting with government. While firms that serve the defense and broader government sector often interact with strategic goods regulators, EDT developers that engage purely in commercial transactions or academic research are often unaware of the dual use potential of their technology and even less aware of policies and best practices to safeguard it. This leaves unsuspecting firms – often in the segments of greatest interest to malign actors -- highly vulnerable to diversion tactics.

A Way Forward: A Capability-Based Approach

While current conditions allow weapons-relevant technologies to proliferate, opportunities to reduce risk abound. The Innovators Next Door Project articulated core government and industry capabilities that can significantly reduce diversion risks and safeguard strategic goods (Table 1.) The Project's simulation-based learning and cross-sector dialogue helped reveal and address capability shortfalls and demonstrated the extent to which risk can be reduced when stakeholders are proficient in these knowledge and skill areas.

Table 1. Core Capabilities for Reducing Diversion Risks

For Government	For Industry
Ability to apply and adjust policies and procedures in response to dynamic events and trends.	Ability to recognize and manage risk in export situations, including "deemed" exports.
Ability to detect and deny diversion attempts in coordination with industry, and with other partner governments.	Ability to manage risks in non-export situations/domestic/internal activities.
Ability to discern and govern higher-risk dual-use but non-controlled/non-listed items.	Ability to identify and manage risk in known/likely military end-use situations.
Ability to discern and govern dual-use export controlled/listed items.	Ability to safeguard potential dual-use but non-controlled/non-listed items.
Ability to discern and govern sanctions-controlled items.	Ability to safeguard dual-use export controlled/listed items.
Ability to identify and govern industry entities of interest.	Ability to safeguard sanctions-controlled items.
Ability to detect and deny transactions with sanctioned entities.	Ability to avoid transactions with sanctioned entities.
Ability to govern transactions with non-sanctioned entities.	Ability to manage risk in transactions with non-sanctioned entities.

Within and far beyond the Baltics, this capability-based framework has broad geographic relevance and could set the stage for a new international paradigm for strategic goods control. Such a paradigm expands the frame beyond an "export control" issue, rethinks prevailing policy and practice, prioritizes coordination within and beyond governments, and is guided by the following principles:

- *Understanding* that government strategic goods control structures and processes must be inter-disciplinary, agile, proactive, and adaptive;
- *Appreciating* that industry has a wide range of vital, often voluntary, tools to mitigate diversion risks and should be treated by governments as partners in detecting and managing threats; and;
- *Accepting* that formal regulations, even when they incorporate "deemed" exports and "catch-all" concepts, cannot cover every possible scenario, item, or entity involved in diversion risks; and
- *Recognizing* that controls come with trade-offs in innovation and must be carefully balanced.

Recommendations

In response to the findings above, and consistent with the strategic goods control paradigm above, Motive and our Project stakeholders developed the following recommended actions for industry and government consideration:

Sharpen Government Roles & Responsibilities: Governments could designate a single national focal point with the mandate and stature to engage at a whole of government scale and serve as a single point of entry for industry and academia when it comes to strategic goods control. Inter-ministerial commissions and cooperation frameworks are a start, but often lack sufficient aperture or authority to overcome intra-government silos or lack the mandate to proactively engage with non-governmental stakeholders. We recommend that outreach to industry and academia be an explicit function - on par with licensing, investment screening, policy formulation, and threat monitoring - of national focal point entities.

Re-Imagine Government-Industry Collaboration: Those who develop and trade in dual use technologies have a vested interest in preventing diversion and nefarious use of these goods both as a matter of protecting proprietary innovations and market-wide reputations. For this reason, we encourage policy and regulatory officials to view industry and academia as partners in strategic goods control and to pro-actively set-up mechanisms that facilitate cross-sector collaboration. These might include:

- Channels for government to disseminate threat and regulatory updates directly to industry or through industry association or cluster entity nodes, especially those active in high-risk EDT segments.

- Portals that allow industry to submit inquiries to government – potentially anonymously - and receive timely responses related to compliance, specific transactions, or the risk landscape.

- Mechanisms that enable government officials to easily access industry experts for case-specific consultations or for inputs to new policies or strategies.

- Collaborative efforts to map and maintain updated listings of firms and institutes that develop or trade in certain EDTs, with mutual agreement on how this list will/will not be used or disclosed, such as for outreach in the spirit of partnership not enforcement or oversight.

- Co-created standards and frameworks for determining dual use applications of commercial EDTs and for identifying technologies at highest risk of diversion.

- Forums that bring together industry, strategic goods officials, and business promotion agency representatives to discuss emerging trends and align standards and strategies.

- Specific mandates for industry associations or cluster entities to take on a coordination role between government and industry and/or to serve as an advisory body to government on strategic goods control matters that impact their constituents.

- Webinars, online resources, or events organized by government that help industry adopt Know Your Customer (KYC) and related due diligence best practices, Internal Compliance Programs (ICPs) tailored for EDT segments and entities of various sizes/stages, and other safeguards.

- On-demand consults with government or self-help resources that allow firms to create an index of the items they handle, cross-referenced with the relevant export controls, sanctions, investment screening requirements, or reporting that is either required or recommended for each item.

Improve Multilateral Alignment: The EU and EU member states, along with the United States and other leading innovating economies could work toward developing a "Common Operating Picture" of technology diversion vulnerabilities and set new standards for strategic goods control best practices. This could start with the adoption of the core capabilities framework presented above and a commitment to achieving proficiency in each area. Additionally, we recommend the following options for specific key institutions:

- The EU's Working Party on Dual-Use Goods could document and share best practices from across member states of industry outreach mechanisms, work to harmonize member state export control lists and investment screening regimes, and application of catch-all authorities.

- NATO could establish a Centre of Excellence on Sensitive Dual-Use Technologies that develops a training curriculum on strategic goods control best practices for governments and industry in member states; NATO could also ensure the forthcoming Defense Innovation Accelerator for the North Atlantic (DIANA) requires participating entities to demonstrate best practices for protecting their technologies from diversion, such as having ICPs tailored to their organization.

- A G7 Working Group on Strategic Trade Controls could coordinate G7 counter-diversion policies and practices as a complement to the work of G7 Foreign and Trade Ministers on Russia sanctions, global trade flows, and supply chain resiliency.

- A dialogue with key partners in Asia could be established to examine and share information about the diversion tactics and techniques used by the PRC and their state-aligned entities, then proactively educate industry in the region and encourage them to embrace capabilities and best practices described in this paper.

The EU's Working Party on Dual-Use Goods could document and share best practices from across member states of industry outreach mechanisms, work to harmonize member state export control lists and investment screening regimes, and application of catch-all authorities.

Conclusion

Countries with vibrant EDT ecosystems and proximity to adversaries are particularly vulnerable to the threat of technology diversion. The Baltic states offer illustrative examples. The region's relatively small number of affected industry entities, and capable, open governments create conditions for targeted policy reforms and intimate cross-sector collaboration. That said, we believe the Innovators Next Door Project approach and findings have relevance well beyond the Baltics to national and regional context across the globe. We believe a capability-based framework and partnership-oriented mindset between government and industry - no matter the geography – are key to thwart diversion of sensitive technologies while balancing national security imperatives with diverse stakeholder interests.

A Latvian tech executive exchanges ideas with a NATO official who attended the October 2022 Project event. (Motive photo)

Participants at the Innovators Next Door event in Vilnius, pictured above, included representatives from the domestic tech industry, academia, civil society, NATO, the U.S. State Department, inter-ministerial officials from the Lithuanian government, and others. (Motive Photo)

[1] Technologies covered include robotics, machine vision, artificial intelligence/machine learning, blockchain, encryption, sensors and IT networking.
[2] https://www.rusi.org/explore-our-research/publications/special-resources/silicon-lifeline-western-electronics-heart-russias-war-machine
[3] Lithuanian Ministry of Defence, National Threat Assessment, 2019. https://www.vsd.lt/wp-content/uploads/2019/02/2019-Gresmes-internetui-EN.pdf

Motive International is a Washington, D.C. based social enterprise with a mission to mitigate conflict and enhance stability in fragile global environments. We advance our mission by delivering specialized consulting and advising services to government, military, civil society and private-sector clients and through mission-driven impact initiatives.

Visit www.motiveinternational.com to read timely, content-rich articles and analysis on regional and thematic topics related to our mission.