



**World Customs  
Organization**

**STUDY REPORT**

# **Unlocking the Value of Open-Source Intelligence (OSINT) for Customs Enforcement**

**JULY 2024**



Study Report

# Unlocking the Value of Open-Source Intelligence (OSINT) for Customs Enforcement

July 2024

# Table of Contents

<b>Foreword</b> .....	<b>5</b>
<b>List of abbreviations</b> .....	<b>6</b>
<b>Executive summary</b> .....	<b>7</b>
<b>Introduction</b> .....	<b>9</b>
<b>I. The Evolving OSINT Landscape</b> .....	<b>13</b>
1. Defining what OSINT is and is not.....	13
2. Brief history and evolution of OSINT .....	16
<b>II. Application of OSINT in Customs</b> .....	<b>19</b>
1. Threat identification and risk assessment .....	19
2. Trade compliance and fraud detection.....	20
3. Smuggling and trafficking detection .....	20
4. Border security .....	20
<b>III. Special Focus: OSINT in Strategic Trade Control Enforcement</b> .....	<b>22</b>
<b>IV. Implementing OSINT</b> .....	<b>28</b>
1. Analysing challenges and identifying success factors .....	28
2. Avoiding pitfalls.....	31
3. Addressing training and capacity building .....	33
<b>Conclusion</b> .....	<b>35</b>
<b>Additional resources for further reading</b> .....	<b>37</b>
<b>Glossary of terms</b> .....	<b>39</b>
<b>Bibliography</b> .....	<b>40</b>

## Foreword

This Study Report aims to provide a thorough review of how Open-Source Intelligence (OSINT) can be leveraged by the World Customs Organization (WCO) Member administrations. Over the past few years, digital investigation techniques making use of Publicly Available Information (PAI) have proven highly effective. This Report offers a comprehensive understanding of OSINT, its limitations, and its applicability to Customs enforcement processes. It also suggests different strategies to address potential challenges in implementing OSINT.

The origins of this Study Report trace back to the Fragile Borders Action Plan adopted by the WCO Members at the 2023 Council Sessions. Recognizing the potential to leverage OSINT in fragile and conflict-affected situations in particular, the Action Plan included a set of deliverables related to the development of OSINT in Customs enforcement.

From the operational perspective, the first productive discussions on OSINT were held in February 2024, in a closed-door exploratory workshop with WCO staff and selected Member administrations. An awareness-raising panel discussion exploring the use of OSINT in Customs was subsequently organized during the March 2024 Enforcement Committee Meeting. These engagements underscored the critical role of OSINT in modern enforcement strategies, highlighting its potential to significantly bolster Customs enforcement efforts. Building on these insights, a pilot training workshop was held in Antwerp, Belgium in June 2024. The training focused on the practical application of OSINT in the domain of Strategic Trade Controls. Its success, and the valuable feedback received, reinforced the necessity of this comprehensive Study Report.

The WCO wishes to thank Global Affairs Canada (GAC) for its generous support of the OSINT project that included the commissioning of this Study Report.

## List of abbreviations

AI	Artificial Intelligence
API	Advance Passenger Information
Aoi	Area of Interest
CoP	Community of Practice
FBIS	U.S. Foreign Broadcast Information Service
GAC	Global Affairs Canada
GEOINT	Geospatial Intelligence
GIS	Geographic Information System
GPS	Global Positioning System
HUMINT	Human Intelligence
IAEA	International Atomic Energy Agency
ICT	Information and Communication Technologies
OCU	Operational Coordination Unit
OPCW	Organisation for the Prohibition of Chemical Weapons
OPSEC	Operational Security
OSINT	Open-Source Intelligence
OSS	U.S. Office of Strategic Services
PAI	Publicly Available Information
PNR	Passenger Name Record
SALW	Small Arms and Light Weapons
SOCMINT	Social Media Intelligence
SOP	Standard Operating Procedure
STCE	Strategic Trade Control Enforcement
SWOT	Strengths-weaknesses-opportunities-threats
TBML	Trade-Based Money Laundering
UNODA	United Nations Office on Disarmament Affairs
UNODC	United Nations Office on Drugs and Crime
WCO	World Customs Organization
WMD	Weapons of Mass Destruction

## Executive summary

Open-Source Intelligence (OSINT) is the process of collecting, analysing, and utilizing information that is publicly and commercially available to support intelligence and decision-making processes. It has become increasingly popular in recent years. Deriving from the Publicly Available Information (PAI) that is accessible to anyone with a few clicks of a mouse on the Internet, OSINT has become a preferred method in various sectors, ranging from national security and intelligence to competitive analysis and investigative journalism. OSINT allows its users to gather insights and make informed decisions without necessarily relying on sensitive or classified data.

This Study Report is aimed at senior management in Customs administrations who are interested in examining the possibility of introducing OSINT into their enforcement practices. Its objective is to provide a comprehensive review of how WCO Member Customs administrations can unlock the value of OSINT. Since OSINT is a very young discipline, and relatively few Customs administrations have started leveraging its value, this Study Report should be considered as a step towards laying the foundation of OSINT in Customs enforcement.

The Study Report demonstrates the benefits of OSINT for Customs administrations, offering critical information for implementing OSINT practices within Customs operations by answering three key questions:

- I. Why OSINT matters for Customs administrations, and what value added it offers;
- II. How Customs administrations can leverage OSINT, and
- III. How OSINT can be implemented within the administration, and how to address certain challenges arising from this process.

To address these questions, the Study Report is divided into four chapters. The first chapter examines the notion of OSINT and its evolution over time. The second chapter provides information on the applications of OSINT in different functional areas of Customs enforcement. The third chapter is dedicated to the use case related to the implementation of OSINT in Strategic Trade Controls, while the final chapter suggests an analysis of OSINT implementation with the use of SWOT (strengths-weaknesses-opportunities-threats) methodology, the identification of key success factors, and proposed strategies to address challenges and limitations arising from OSINT implementation.

The findings of this Study Report reveal that the accessibility and cost-effectiveness of OSINT, when compared with obtaining classified or proprietary information, along with its low barriers to entry and the timeliness of the information it provides compared to the often outdated information derived from classified sources, offer immense opportunities for Customs administrations. OSINT can also serve as a catalyst in enhancing other forms of intelligence (such as the human intelligence that is widely used in Customs enforcement) by providing additional context and insights that allow more comprehensive conclusions to be drawn. At the same time, due to its constantly evolving and collaborative nature, OSINT can serve as a stepping stone to promote and support ongoing developments in the adoption of the latest information and communications technology (ICT), international and inter-agency cooperation, as well as continuous learning.

The Study Report identifies several functional areas that could benefit from the use of OSINT, namely: threat identification and risk management, trade compliance and fraud detection, smuggling and trafficking prevention, and border security.

The Strategic Trade Controls use case allows readers to examine the subject more closely by delving deeper in the OSINT techniques that can be incorporated into the export controls domain, ranging from risk analysis and threat detection to investigation. The Study Report also suggests how OSINT can be leveraged to enhance inter-agency and international operations by providing the example of the WCO's Operations Cosmo, which focused on countering the illicit trafficking of strategic goods.

Finally, the Study Report also provides a SWOT analysis of OSINT implementation. It makes a number of recommendations regarding how to address some of the threats and weaknesses. The recommendations cover multiple areas, ranging from broader strategies that apply to any major project implementation in a Customs administration (for example, getting a political buy-in, securing the necessary financial and human resources, and providing an adequate legal and regulatory framework) to more specific areas (such as addressing ethical considerations arising from the use of OSINT or ensuring access to continuous training, given the evolving nature of the discipline).

Reaping the benefits of OSINT can help Customs administrations to better contribute to safety and security at both the national and international levels. Bearing in mind the struggle for resources and dwindling budgets that are conditions found frequently in any governmental agency, this Study Report does not offer a panacea. Rather, it provides food for thought on how to unlock the potential of OSINT in the context of Customs enforcement activities.

## Introduction

Customs authorities have traditionally been responsible for implementing a wide range of border management policies, often on behalf of other government agencies. These responsibilities encompass diverse areas, including revenue collection, trade facilitation, compliance and enforcement, such as countering illicit trade in prohibited and restricted commodities and substances, enforcement of intellectual property laws, as well as an enhanced role in security, to name just a few. In many developing countries import duties and related taxes constitute a significant portion of national revenue. Nevertheless, while revenue collection is the primary focus for the majority of Customs authorities, there has been a growing understanding that revenue collection is heavily impacted in fragile and conflict-affected environments, thus leading to the need to bolster the security function of Customs administrations across the globe. Notably, the role of Customs in the security context was addressed in the WCO Policy Commission's Punta Cana Resolution<sup>1</sup> in 2015. It was further developed through the WCO's work on the role of Customs in fragile and conflict-affected situations,<sup>2</sup> which culminated in the adoption of the WCO Fragile Borders Action Plan at the June 2023 Council Sessions.<sup>3</sup>

Customs administrations were among the first government agencies to adopt Information and Communication Technologies (ICT) in their operations on a wide scale. This included harmonizing regulations, reducing face-to-face interactions, tracking transactions and data to fight corruption, transforming paper-based processes into paperless systems, eliminating discretionary human intervention, and enhancing accountability for decisions. However, the adoption of ICT has been uneven among Customs administrations and has evolved through different stages. Initially, this evolution involved digitization, or going paperless, followed by digitalization, which entails the integration of digital systems. Despite progress, challenges persist, such as underutilization of ICT<sup>4</sup> to support management decision-making, the continuation of manual procedures, a silo mentality, and a difficulty in building agile and innovative solutions because of legacy systems.

---

<sup>1</sup> WCO (2015), *Punta Cana Resolution*, available at <https://www.wcoomd.org/-/media/wco/public/global/pdf/about-us/legal-instruments/resolutions/resolution-of-the-wco-policy-commission-on-the-role-of-customs-in-the-security-context.pdf?la=en>

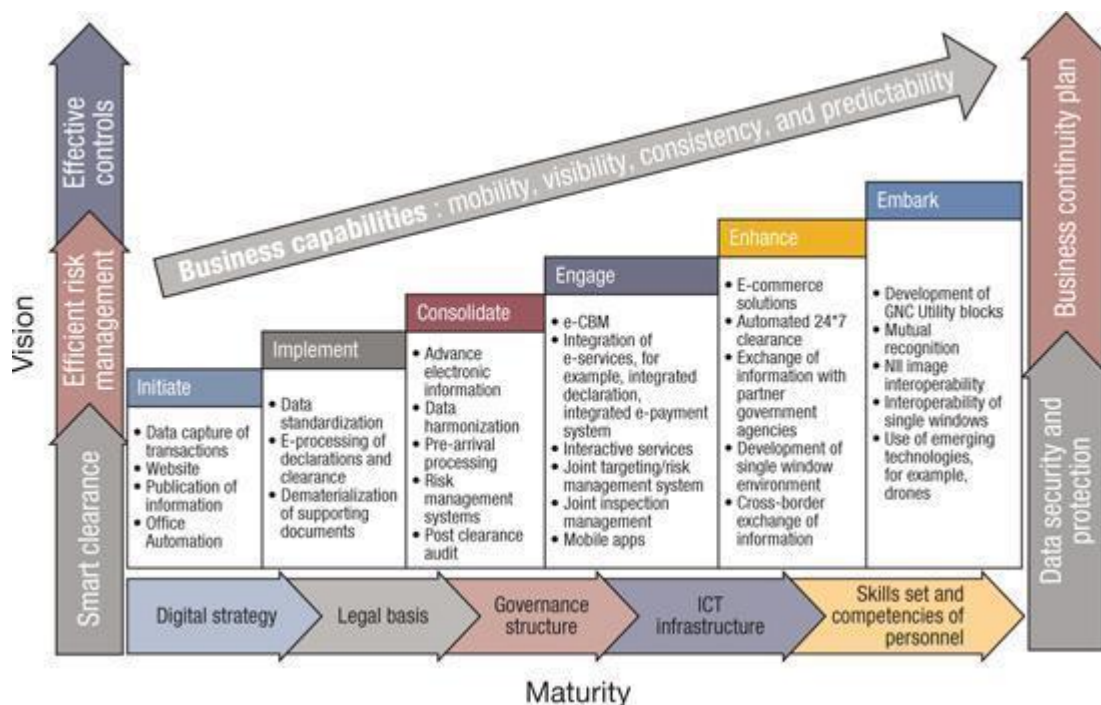
<sup>2</sup> WCO (2022), *Secretariat Note on the Role of Customs in Fragile and Conflict-Affected Situations*, available at in [https://www.wcoomd.org/-/media/wco/public/global/pdf/topics/research/report/fragility\\_secretariatnote\\_pc\\_council\\_2022\\_may19version\\_en.pdf?db=web](https://www.wcoomd.org/-/media/wco/public/global/pdf/topics/research/report/fragility_secretariatnote_pc_council_2022_may19version_en.pdf?db=web)

<sup>3</sup> WCO (2023), *Outcomes of the 2023 WCO Council Sessions: Election of a new WCO Secretary General and Chairperson of the WCO Council*, available at

<https://www.wcoomd.org/en/media/newsroom/2023/june/outcomes-of-the-2023-wco-council-sessions.aspx>

<sup>4</sup> See WCO/WTO (2022), *"The role of advanced technologies in cross-border trade: A customs perspective"*, available at <https://www.wcoomd.org/en/topics/facilitation/instrument-and-tools/tools/wco-wto-paper.aspx>

Graph 1. Digital Customs Maturity Model<sup>5</sup>



The Digital Customs Maturity Model shows the different steps that need to be taken by Customs administrations to enhance their digital capabilities. It also portrays how advancement through this process can enhance business capabilities, and improve controls.

The rise of violent non-state actors has also increased security requirements for international supply chains, necessitating more documentation, and collaboration among Customs administrations and other law enforcement agencies, while maintaining high transparency levels. The democratization of the Internet, the widespread use of social media platforms, and the digitalization of data have transformed legitimate trade, as well as the activities of actors and networks involved in illicit trade. Increasingly, many trade transactions are initiated and conducted partially or entirely online. The COVID-19 pandemic accelerated this trend. Thus, the Internet has become a valuable source of information for Customs administrations, and this must be leveraged effectively. Digital footprints (i.e. the trail of data that a person leaves behind while using the Internet), which are challenging for illicit actors to control, present significant opportunities for Customs administrations to monitor and intercept illegal activities.

In order to successfully fulfil their mission of safeguarding national borders, ensuring compliance with trade regulations, and contributing to national security, Customs administrations have had to ensure the continuous enhancement of their capabilities.

Three major capability-enhancing measures have a positive impact in bolstering Customs enforcement capacities globally. The first is related to leveraging technologies, as integrating advanced ICT for Customs clearance, electronic tracking of shipments, and real-time data analytics are vital for modern Customs enforcement. These technologies significantly reduce manual intervention, minimize errors, and expedite the processing of goods, thereby enhancing efficiency and accuracy. The use of disruptive technologies,<sup>6</sup> such as

<sup>5</sup> WCO (2018), *IT Guide for Executives*, p.15, available at <https://www.wcoomd.org/-/media/wco/public/global/pdf/topics/facilitation/instruments-and-tools/tools/it-guide-for-executives/it-guide-executives.pdf?db=web>

<sup>6</sup> See WCO/WTO Study Report on Disruptive Technologies 2022, available at

Artificial Intelligence (AI), machine learning, and blockchain technology, offers tremendous potential for Customs authorities. In the context of countering illicit trade and fulfilling the security functions, these technologies help identify patterns indicative of illicit activities, anticipate and mitigate risks, and provide transparency. However, the implementation of these technologies requires significant investments, both in time and finances.

The second measure relates to investing in continuous learning and capacity building. The evolving role of Customs administrations necessitates ongoing training for its officers to cover the latest enforcement techniques, technological tools, and legal frameworks. Training ensures that Customs officers are well-equipped to handle modern challenges. In order to bolster the capacities of Customs administrations and regularly provide them with new learning opportunities, the WCO developed an e-learning platform, CLiKC!, which offers more than 60 courses and currently has around 40,000 users.<sup>7</sup> Using this platform as a complement to individual Customs administrations' own continuous learning and capacity-building efforts may assist these agencies in ensuring that their training materials are regularly updated, and that they encompass the latest trends and patterns in the Customs realm.

Effective Customs operations require internal collaboration across the organization, as well as global cooperation, which is the third measure, aimed at breaking down silos. Silos can constrain information flows and hamper the full use of resources. While necessary for operational and security reasons in some areas of Customs enforcement, they can quickly become a serious impediment to progress in others. Being open to dialogue is essential to Customs. Cultivating the culture of sharing knowledge and best practices, participating in international initiatives, and establishing cross-border partnerships are therefore vital for the success of Customs operations. Additionally, participation in global initiatives provide Customs administrations with access to valuable resources, expertise, and best practices. These initiatives promote a standardized approach to Customs enforcement, enhancing its overall effectiveness.

As a product of global technological advancements, OSINT can become an important tool for Customs administrations, particularly because the entry barrier is relatively low, given its open-source nature, and cooperation is ingrained into its philosophy. From a more practical perspective, Customs administrations can leverage OSINT to enhance specific enforcement functions, namely:

- (i) Threat Identification and Risk Assessment: monitoring global news, social media, and specialized forums to detect new smuggling methods, shifts in trafficking patterns, and changes in trade dynamics;
- (ii) Trade Compliance and Fraud Detection: verifying trade documents, monitoring corporate social media, and detecting misclassification and undervaluation of goods;
- (iii) Smuggling and Trafficking Prevention: identifying smuggling routes, tracking illegal shipments, and monitoring smuggling networks; and
- (iv) Border Security: real-time border monitoring, identifying high-risk individuals and cargo, and improving cargo inspection processes.

---

<https://www.wcoomd.org/en/topics/facilitation/instrument-and-tools/tools/wco-wto-study-report-on-disruptive-technologies-2022.aspx>

<sup>7</sup> For more information on CLiKC!, see <https://clikc.wcoomd.org/>

Due to its origins in the public sphere, OSINT is collaborative by nature, which may lead to enhancing different types of cooperation. First, partnering with private sector entities such as logistics companies, data brokers, and financial institutions can enhance the collection and analysis of OSINT. These partnerships bring additional data sources and analytical capabilities, strengthening Customs enforcement efforts.

Second, cooperation with civil society organizations that are versed in digital investigations can provide Customs administrations with specialized knowledge and tools to better understand and combat illicit activities.

Last but not least, having access to tax data is a powerful tool for the Customs enforcement function. In countries where Customs is not integrated into a single revenue authority, establishing inter-agency cooperation to enable access to taxpayer data can significantly enhance the accuracy of intelligence products.

OSINT is particularly beneficial to Customs administrations in fragile and conflict-affected situations, where access to terrain might be limited because of violent events. Moreover, Customs administrations in these environments often operate with limited budgets and lack structural support. After transitioning from paper-based declarations to automated and electronic declaration processing, OSINT offers a replicable solution that can be implemented across various Customs functions, providing another valuable tool in the fight against illicit trade. Its cooperative nature also may bring value added by allowing Customs administrations to leverage new, previously underexplored resources and build new partnerships.

## I. The Evolving OSINT Landscape

### 1. Defining what OSINT is and is not

The datafication of the world has brought about a transformative change, with the total amount of digital data projected to reach approximately 175 trillion gigabytes by 2025, according to the International Data Corporation.<sup>8</sup> A substantial portion of this data is generated and stored online, with about 2.5 quintillion bytes created every day. This encompasses a diverse range of data, including text, images and videos.

There are over 1.8 billion websites on the Internet, although not all are active. These websites contribute significantly to the vast volume of data available online. Social media platforms like Facebook, YouTube, Twitter and Instagram generate enormous amounts of data daily through user interactions, posts and multimedia uploads.

This data revolution has been driven by three key factors. The first is the growth of user-generated data. The proliferation of mobile phones and the development of social media platforms have led to a significant increase in user-generated data.

Demand for transparency is the second factor. Governments, public administrations, and businesses are increasingly required to be transparent, leading to the public availability of data that was previously restricted to specific groups of stakeholders. Traditional paper-based processes are being replaced by digital platforms to facilitate administrative work and processes, and the public demand for transparency through the pressure to publish data has been increasing in the past years. Data mobilization<sup>9</sup> in Customs is an ongoing topic for research and development.

Last but not least, increasing connectivity is the third factor. People, organizations, processes, and applications are becoming more interconnected. In 2024, there are approximately 5.3 billion Internet users, corresponding to 66.2% of the total population. Since 2000, a similar proportion of people have also adopted social media networks, at a total of 5.03 billion individuals.<sup>10</sup>

Technologies like satellite imagery and Global Positioning Systems (GPS), which were once primarily military capabilities, are now widely accessible for consumer/civilian applications. The cost of these technologies has decreased remarkably, making them available in everyday applications such as smartphone maps and products such as Google Earth.

Not only is more data being generated, but people and organizations have also shifted their ways of consuming media, conducting business, and identifying themselves by integrating online components into their daily lives. This phenomenon has direct implications for Customs authorities. Business practices, including illicit ones, are now conducted partially or fully online.

Additionally, individuals or organizations involved in illicit trade, border trafficking, or fraud are likely to leave digital footprints on the Internet, either created by themselves or generated by others.

---

<sup>8</sup> Reinsel, D., Gantz, J., & Rydning, J. (2018). The Digitization of the World: From Edge to Core. *International Data Corporation (IDC)*.

<sup>9</sup> Mikuriya, K. and T. Cantens (2020). If algorithms dream of Customs, do customs officials dream of algorithms? A manifesto for data mobilisation in Customs. *World Customs Journal*, 14(2), 3-18.

<sup>10</sup> Kemp, S. (2024), *Digital 2024: Global Overview Report*, available at <https://datareportal.com/reports/digital-2024-global-overview-report>

### Box 1. Definition of OSINT

*Open-source intelligence (OSINT) refers to the process of collecting, analysing, and utilizing information that is publicly and commercially available to support intelligence and decision-making processes.*

Leveraging this data for Customs administrations is about generating OSINT. This type of intelligence can be gathered from a wide array of sources, including the Internet, social media platforms, news articles, public or commercial records, academic publications, and other accessible data repositories. OSINT plays a critical role in a number of fields such as national security, law enforcement, corporate security, taxation, disaster relief and competitive intelligence, to name but a few. Despite its significant advantages, OSINT has inherent limitations that must be acknowledged and addressed.

OSINT derives from a multitude of publicly available information. This can be broadly categorized into the following:

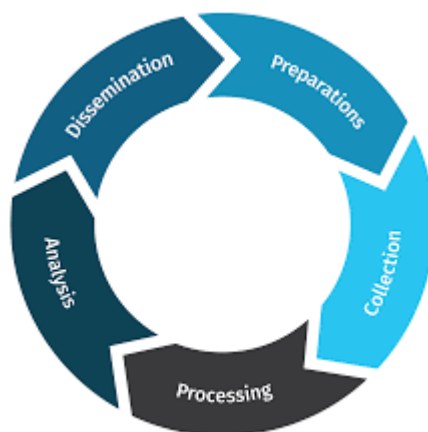
- User-generated content: Content which has been created on social media platforms or on websites, blogs and forums. It includes not only text but also images and videos.
- Databases and specialized repositories: All types of databases based on topics such as online commercial and land registries, vehicle registries, import/export commercial databases, etc.
- Social media platforms: X, Facebook, LinkedIn, VK, TikTok and Instagram, but also messaging services such as Telegram, etc.
- E-market platforms: Online market platforms to conduct B2B or B2C trade.
- Traditional media: Articles, broadcasts, and newswire services.
- Government publications: Official reports, public records, and legal documents.
- Academic and professional publications: Research papers, journals, and records of conference proceedings or catalogues.
- Corporate publications: All mandatory and commercial documents required for transparency and public availability, such as financial statements, annual reports or commercial presentations.
- Technical information: identifiers such as telephone numbers, emails, domain names, website page codes, analytics trackers and security certificates which can appear in documents or online.
- Geotagged data: geolocation information which can appear on social media platforms, maps and satellite imagery, metadata embedded in images and videos.
- Transportation data: maritime and aviation tracking data, ownership and incident registries, sale repositories.
- Financial data: blockchain analysis platforms for crypto-currencies, bank sort code analysers, broker reports, financial statements.

Additional sources of information can be leveraged but are more controversial. For example, cyber leaks, which can be defined as data extracted during hacking operations, are considered to be stolen data in many jurisdictions and cannot be legally accessed or used. Data revealed by hacking and leaking operations, a form of cyber influence technique, should be thoroughly analysed in order to detect whether the data set might have been compromised by false information.

In order to develop OSINT, it is necessary to follow the same process as the open-source

intelligence cycle shown below, as simply having access to PAI is not OSINT per se.

Graph 2. Open-Source Intelligence Cycle



Five major steps are required to produce OSINT in order to transform a collection of data into fused, actionable intelligence for Customs enforcement:

- I. Preparation: defining the research strategy and intelligence priorities.
- II. Collection: gathering data from various open sources.
- III. Processing: verifying, archiving; organizing and structuring collected data.
- IV. Analysis: evaluating the data to extract actionable insights.
- V. Dissemination: sharing the intelligence with relevant stakeholders for decision-making and operations.

However, OSINT is not a magic methodology or tool, and has some key limitations. One of the primary challenges of OSINT is the sheer volume of available data. The vast amount of information can be overwhelming, making it difficult to identify relevant and accurate data. Analysts have to sift through extensive datasets to find valuable insights, which can be time-consuming and resource intensive. In some cases, the digital footprint may be missing or partial. Integrating OSINT into Customs intelligence models enables administrations to transition to an all-source intelligence<sup>11</sup> model that encompasses all intelligence techniques. The open nature of OSINT sources means that not all information is reliable or accurate. Misinformation, disinformation, and outdated information are common issues. Analysts must apply rigorous verification processes to ensure the credibility of the sources and the validity of the information. This often involves cross-referencing data with multiple sources to confirm its accuracy. The dynamic nature of open sources means that information can quickly become outdated or disappear. OSINT must be conducted in a timely manner to ensure that the intelligence remains relevant and is captured on time. An archiving process needs to be put in place in order to retain information.

In addition, four specific points deserve attention. These points are further developed and addressed in Chapter IV. First, OSINT operations must adhere to laws and regulations of the country in which they are used. While the information is publicly available, its collection and use must respect privacy laws and regulations. Analysts must navigate complex legal landscapes to ensure compliance with local legislation, which can vary significantly between

<sup>11</sup> All-source intelligence means incorporating all available sources of information, for example, human intelligence, imagery intelligence, signals intelligence, open-source data etc.

jurisdictions.

Second, OSINT operations must respect ethical standards which are linked to the protection of personal data, but also the ethos of OSINT practitioners who have been trained to investigate.

Third, the effectiveness of OSINT, like many other techniques, depends on resources. Basic OSINT resources can be easily accessed at no cost or with a limited amount of funding. However, the OSINT sector has become a multi-million dollar market. More effective and sophisticated OSINT requires access to advanced tools and technologies for data collection, processing, and analysis. These tools can be extremely costly, and not all organizations may have the resources to invest in them. Furthermore, having a pool of skilled analysts is critical to develop intelligence accurately and exploit these tools to their maximum capacity.

Last but not least, engaging in OSINT activities can expose Customs administrations to security risks. Analysts may inadvertently access malicious websites or be subject to phishing attempts. Additionally, the digital footprint left by OSINT activities can be traced, potentially revealing the Customs administration's intelligence-gathering efforts to adversaries. OSINT often requires the creation of online personas to access social media platforms, which may necessitate additional authorizations<sup>12</sup> as well as certain skills in creating accounts which meet the registration criteria of the social media platforms while maintaining an acceptable level of discretion for the Customs administration.

## 2. Brief history and evolution of OSINT

The concept of OSINT is not new. The collection and use of open-source information can be traced back to governments and scholars, who gathered publicly available data to inform their decisions. The systematic use of open-source information, however, began to take shape in the 20th century.

During World War I, nations began to recognize the value of intercepting and analysing open communications. Newspapers, radio broadcasts, and public speeches were scrutinized for valuable information. For example, the British Admiralty's Room 40 intercepted and deciphered German naval codes, gaining insights from publicly transmitted messages. Embassies worldwide were valued for their access to local newspapers and media.

The establishment of the Office of Strategic Services (OSS) by the United States during World War II marked a significant development in OSINT. The OSS collected and analysed information from newspapers, periodicals, and radio broadcasts from around the world. The United Kingdom also employed similar tactics, with the BBC Monitoring Service playing a crucial role in gathering and interpreting foreign broadcasts.

The period prior to the Cold War saw the institutionalization of OSINT. In 1941, the United States created the Foreign Broadcast Information Service (FBIS), which monitored and translated foreign broadcasts, publications, and other open sources. The Soviet Union also utilized open-source information extensively, analysing Western media to understand political and military strategies.

The evolution of technology in the second half of the 20th century has significantly transformed OSINT. Advancements in communication technologies, computing, and the Internet have revolutionized the collection and analysis of open-source information, which has moved from

---

<sup>12</sup> In many countries, specific legislation has to be passed in order to allow Customs administrations or Police to create online personas.

the use of telecommunications and broadcasting services to the opportunities provided by computing, automation and the Internet.

In particular, the proliferation of television and radio broadcasts expanded the scope of OSINT. Intelligence agencies were able, as a result, to access real-time information from around the world. The development of satellite technology further enhanced the ability to monitor broadcasts globally.

The advent of computers enabled the automation of data collection and analysis processes. Early computer systems facilitated the storage, retrieval, and processing of vast amounts of information. This period also saw the emergence of database systems that allowed for more efficient organization and analysis of open-source data.

The introduction of the Internet in the late 20th century was a game changer for OSINT. The Internet provided unprecedented access to information, with millions of websites, online publications, and databases becoming accessible. Intelligence agencies began to exploit the Internet for information gathering, leading to the development of new tools and techniques for OSINT.

The 21st century has witnessed an exponential growth in the volume and variety of open-source information. The digital age has ushered in new platforms, technologies, and methodologies that have transformed OSINT into a sophisticated and essential component of modern intelligence operations.

The rise of social media platforms like Facebook, Twitter/X, and YouTube has created a wealth of user-generated content. The explosion of data and digitalization has supported the collection work of traditional actors. Intelligence agencies leverage these platforms to monitor public sentiment, track the activities of individuals and groups, and gather real-time information on events as they unfold. Social media analysis has become a critical aspect of OSINT, providing insights into everything from political movements to criminal activities. More importantly, new actors have emerged beyond intelligence and the military, ranging from individuals to businesses, media, civil society, law enforcement and eventually The explosion of digital data has necessitated the development of advanced analytical tools and techniques. Big data analytics enables the processing and analysis of massive datasets to uncover patterns, trends, and correlations. Machine learning and AI have further enhanced the capabilities of OSINT by automating data analysis and generating predictive insights.

The integration of geospatial data with open-source information has given rise to geospatial intelligence. Satellite imagery, Geographic Information Systems (GIS), and location-based data are used to provide spatial context to open-source information. Geospatial Intelligence (GEOINT) has applications in areas such as natural disaster response, military planning, urban security and environmental monitoring, to name but a few. In the context of fragility, the WCO and its Members have also been exploring the use of GEOINT since 2019.<sup>13</sup> The first e-learning module on the use of GEOINT in Customs enforcement will be available on the WCO CLiKC! platform<sup>14</sup> in 2024. Commercial satellite imagery has been a fast-growing market in recent years, reducing the barrier to accessing imagery which used to be a sovereign capability. Individuals can purchase images directly from satellite imagery providers or access Google Earth, which releases free satellite imagery, albeit of lower quality.

---

<sup>13</sup> See WCO (2019), *Geodata Discovery Day*, available at <https://www.wcoomd.org/en/media/newsroom/2019/may/geodata-discovery-day.aspx>

<sup>14</sup> For more information on CLiKC!, see <https://cli kc.wcoomd.org/>

The digital age has also seen the emergence of digital forensics and cyber threat analysis, which focus on gathering and analysing information from cyberspace. These include monitoring hacker forums, analysing network traffic, and tracking digital footprints. Cyber digital forensics and cyber threat analysis have been crucial for understanding cyber threats, identifying vulnerabilities, and attributing cyberattacks.

OSINT has a wide range of applications across various sectors and is used by different stakeholders. Its ability to provide timely and relevant information makes it invaluable for decision makers in both public and private domains. Below are some examples on the use of OSINT in specific domains.

**Military and Defence:** OSINT plays an historical and crucial role in military intelligence, providing insights into the capabilities and intentions of adversaries. It supports strategic planning, threat assessment, and operational decision-making. During conflicts, OSINT can be used to monitor enemy communications, track troop movements, and assess the impact of military operations.

**Law Enforcement and Security:** Law enforcement agencies use OSINT to combat crime, terrorism, and other threats. It is a useful tool to identify suspects, track criminal networks, and gather evidence. OSINT is also used in the border security context to monitor illegal activities such as smuggling and human trafficking.

**Media:** Newsrooms have integrated OSINT into their reporting techniques and production, with dedicated teams working on visual and data-driven investigations and fact-checking units using OSINT techniques to debunk misinformation and disinformation.

**Corporate Intelligence:** Businesses leverage OSINT for competitive intelligence, market research, and risk management. It helps companies understand market trends, monitor competitors, and identify potential threats. OSINT is also used in due diligence processes, providing insights into the reputation and activities of business partners.

**Disaster Response and Humanitarian Aid:** OSINT supports disaster response efforts by providing real-time information on natural disasters, humanitarian crises, and other emergencies. It helps organizations assess the situation, coordinate relief efforts, and allocate resources effectively.

**Academic and Policy Research:** Researchers and policymakers use OSINT to gather data, analyse trends, and develop informed strategies. OSINT supports academic research across various disciplines and assists in the formulation of policies and regulations.

**Citizen Journalism and Communities:** OSINT has also been used as a hobby by citizen journalists and cyber communities which have been leading cutting-edge investigations or creating tools and tracking the latest technical development of the sector out of passion. These communities have been proven invaluable to government agencies by conducting a thorough monitoring of niche research areas such as marine vessel tracking and plane spotting.

Thus, over the years OSINT has become a widely available discipline leveraged by different actors beyond the military and law enforcement agencies. The opportunities it offers are immense, given the datafication processes across the globe. While Customs is new to leveraging OSINT fully, it can be a highly beneficial tool for enhancing its enforcement capacities.

## II. Application of OSINT in Customs

### 1. Threat identification and risk assessment

On a macro level, Customs authorities use OSINT to identify emerging threats by monitoring global news, social media, and specialized online forums. This monitoring allows for early detection of new smuggling methods, shifts in trafficking patterns, and changes in global trade dynamics. On a micro level, OSINT enables Customs administrations to follow up on the activities of a specific organized crime group, or to identify trends in a defined geographical area or for a particular commodity, in order to anticipate upcoming actions or detect new operational patterns. The diverse nature of PAI means that OSINT can be used for countless commodities, ranging from tobacco products and other excise goods to protected flora and fauna,<sup>15</sup> cultural objects, intellectual property infringing goods, drugs and precursors, and goods that can be used to devise, build, and deliver Weapons of Mass Destruction (WMD), Small Arms and Light Weapons (SALW), explosive precursors, or other items of concern.

Risk profiling involves creating detailed profiles of high-risk individuals, organizations, commodities and shipments. OSINT contributes to risk profiling and targeting by providing insights derived from publicly and commercially available information to identify potential risks. Customs can use OSINT to map out smuggling networks by analysing connections between individuals and entities involved in illegal activities. This helps in identifying current risks triggered by actors, routes or commodities, and targeting inspections and investigations more effectively, ensuring resources are focused on the highest risks.

Predictive analytics involves using historical data and trends to forecast future risks. OSINT provides a wealth of data that can be fed into predictive models to anticipate potential threats and allocate resources accordingly. By analysing historical trade data and applying a predictive model, Customs can predict periods of increased smuggling activity, such as around holidays or during economic downturns, and even detect actors who may be more prone to engage in illegal activity. In addition, predictive analysis can be applied to patterns in the operational habits of organized criminal groups to anticipate upcoming actions. This allows for better preparedness and resource allocation.

OSINT tools enable real-time monitoring of major events that could impact Customs operations. These include natural disasters, political instability, cross-border violence and conflicts, and economic shifts, as well as international sporting events such as the Olympic Games, world championships or regional events which can influence trade patterns and create opportunities for illegal activities.

OSINT is a complementary tool to real-time alert systems used by Customs as it provides immediate visibility on an incident or an event as well as an appreciation of the threat posed by the situation. This allows for swift responses to emerging threats.

---

<sup>15</sup> On wildlife trafficking, see Routes Partnership reports: <https://routespartnership.org/industry-resources/publications>

## 2. Trade compliance and fraud detection

OSINT helps in verifying the authenticity of trade documents by cross-referencing information from various public sources, such as government databases, corporate filings, and industry reports. By comparing the details on invoices with data from trade databases, Customs officers can detect discrepancies that may indicate fraudulent declarations or undervaluation of goods. Customs monitors the activities of companies involved in international trade to ensure compliance with regulations. OSINT research can provide insights into business practices, previous violations, and industry trends.

Analysing corporate websites and social media accounts can reveal non-compliance with trade regulations. This information helps Customs take pre-emptive action to ensure adherence to laws and regulations.

Trade misclassification and undervaluation are common methods used to evade Customs duties. OSINT enables the detection of these practices by analysing market data, industry reports, and historical trade records. Customs officers can compare the declared values of goods with market prices to identify significant discrepancies that may indicate underreporting or misclassification.

OSINT is also a crucial tool in uncovering complex fraudulent schemes, such as trade-based money laundering (TBML), in which the value of goods is manipulated to launder money. TBML is a complex financial crime that poses a significant challenge to global efforts in combating illicit financial flows. Customs uses OSINT to identify and combat TBML by analysing financial transactions, ownership structures, and trade patterns.

## 3. Smuggling and trafficking detection

OSINT is instrumental in identifying smuggling routes and methods by analysing PAI from various sources, including social media, news articles, geotagged data, and online marketplaces. Customs monitor online marketplaces, e-marketplaces and forums where controlled and illegal goods are advertised. This helps in identifying smuggling routes and the methods used to transport contraband. In particular, Customs officers use OSINT to track and intercept illegal shipments by analysing shipping data, trade records, and logistical patterns.

OSINT also allows Customs to map out smuggling networks by analysing connections between individuals and entities involved in illegal activities. Using graph network analysis tools, Customs officers can visualize and understand the structure of smuggling networks, making it easier to target key players and dismantle networks.

Customs can use OSINT to enhance cross-border anti-smuggling operations by sharing information and coordinating efforts with international counterparts, without compromising on intelligence security, since OSINT information is from publicly and commercially available sources.

## 4. Border security

Customs administrations use OSINT to enhance border surveillance systems by integrating real-time data from various sources, such as social media, news feeds, and geodata.

In particular, GEOINT complements OSINT by providing spatial context to the information gathered. This is particularly useful for mapping smuggling routes, including the identification of clandestine runways for general aviation, and identifying hotspots, or so-called Areas of Interest (AoI). GEOINT can be leveraged in fragile and conflict-affected situations in particular to gather and analyse information from distant or difficult-to-access areas in order to optimize Customs patrols.<sup>16</sup> With this in mind, the WCO developed a specific platform for general aviation surveillance, using GIS (geoportal) technology and enabling GEOINT data to be superimposed on geolocalized law enforcement and Customs data.<sup>17</sup>

OSINT can be leveraged by Customs and other law enforcement agencies to identify high-risk individuals and cargo by analysing PAI and cross-referencing it with internal databases. It provides ready solutions for Customs officers on the ground or intelligence teams to complement information they already have, such as Advance Passenger Information (API) and Passenger Name Record (PNR) data or tax records. OSINT may also improve cargo inspection processes by providing additional context and information about shipments, transportation, and logistics, helping Customs make more informed decisions.

---

<sup>16</sup> For more on the use of geodata, see Cantens, T. (2019), “Potential uses of geodata for border management”, WCO News 89, available at <https://mag.wcoomd.org/magazine/wco-news-89/potential-uses-of-geodata-for-border-management/>.

<sup>17</sup> For more on Project Colibri, see <https://colibri.wcoomd.org/en>.

### III. Special Focus: OSINT in Strategic Trade Control Enforcement

The global trade environment is increasingly complex, with a significant rise in the volume and variety of goods being traded across international borders. Customs administrations play a crucial role in regulating and monitoring trade to ensure compliance with national and international laws and regulations. Strategic Trade Control Enforcement (STCE) is essential in preventing the illicit trafficking of goods that can contribute to the proliferation of WMD, as well as dual-use commodities<sup>18</sup> that are subject to export controls.

Chemical, biological and nuclear weapons, other conventional weapons, the materials or equipment and technology required for their production and delivery, as well as the know-how to manufacture them can pose a threat to international security if they are transferred to state and non-state actors not authorized to have them under existing international agreements. These goods can be defined as strategic goods. The efforts to prevent the illicit cross-border movement of strategic goods are further complicated by the fact that many of these technologies are dual use.

International organizations have created frameworks to prevent the proliferation of WMD. United Nations Security Council Resolution 1540 (UNSCR 1540) of 2004<sup>19</sup> calls on all States to adopt and enforce appropriate laws, and to take effective measures to prevent the proliferation of WMD and their means of delivery to non-State actors. It is the first international instrument aimed at preventing non-State actors from acquiring WMD. The WCO's STCE programme supports its Members in fulfilling key requirements outlined in the Customs component of UNSCR 1540, thereby recognizing the central role played by Customs in enforcing strategic trade controls at international borders. STCE involves monitoring and controlling the trade in goods that may have military applications or be used in the development of WMDs.

STCE is a challenging area for Customs and other agencies, as illicit strategic trade transactions consist of complex chains of actions to acquire and transport strategic goods covertly. These actions usually take place in multiple jurisdictions. To understand where a Customs intervention could yield optimal results, it is important to have a holistic picture of the strategic trade transaction.

Three steps<sup>20</sup> are needed to form a transaction: (i) transaction arrangement; (ii) purchase and pre-shipment arrangement; and (iii) transportation.

During the first stage, the decision maker is the party initiating the process of illicitly procuring strategic goods, often distancing itself by creating or working through front companies. Facilitators work on behalf of the decision maker to source strategic goods with direct inquiries to a manufacturer or through its subsidiaries, sales offices or distributor network. It may take several iterations to move to the next phase of the transaction. Sometimes inquiries made by facilitators can be seen using open-source data, as they may appear on e-market places or social media such as LinkedIn or Facebook.

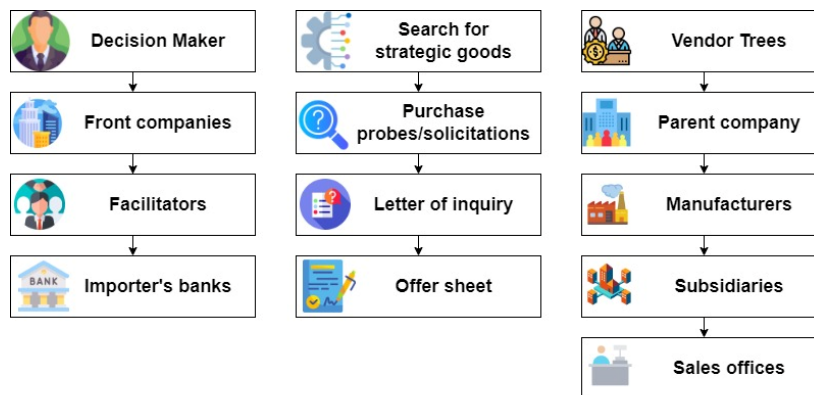
---

<sup>18</sup> Dual-use commodities are items that can be used for both civilian and military purposes.

<sup>19</sup> UN Security Council Resolution 1540 (2004), available at [https://documents.un.org/symbol-explorer?s=S/RES/1540\(2004\)&i=S/RES/1540\(2004\)\\_0402930](https://documents.un.org/symbol-explorer?s=S/RES/1540(2004)&i=S/RES/1540(2004)_0402930)

<sup>20</sup> Nelson, C. (2023). *Methods of strategic trade analysis: Data-driven approaches to detect illicit dual-use trade*. Springer.

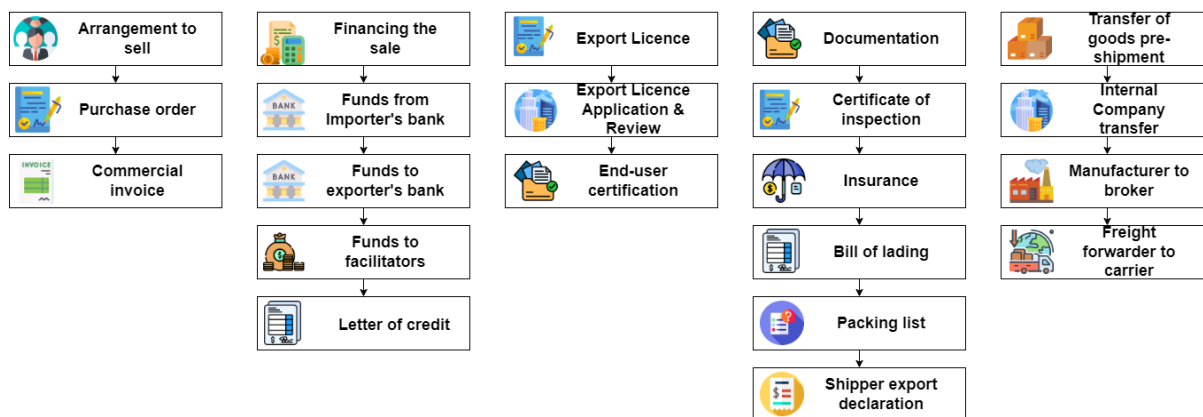
Graph 3. Transaction Arrangement



Source: Nelson, C. (2023), p. 93 (Kindle version used for sourcing: page number may differ from the paperback edition).

In the second stage, the parties issue documentation: invoices, and even international trade documentation, sometimes including export licences. These documents contain important data: purchase value, product name and description, value, HS code, shipping details (consignor, consignee, applying the Incoterms rules), transshipment details and insurance. The final act of this phase is to get the goods ready for transportation with shipping documentation. This information will later appear in commercially available import/export databases.

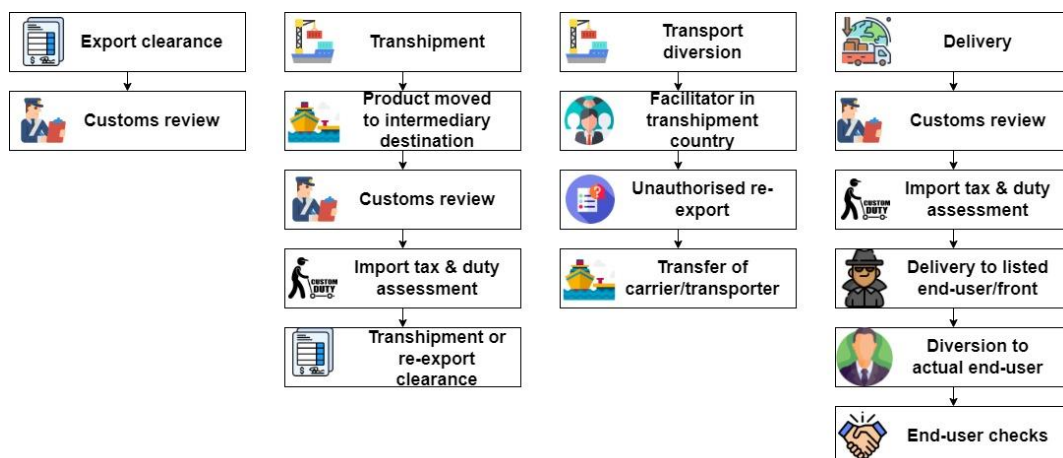
Graph 4. Purchase and Pre-shipment Arrangements



Source: Nelson, C. (2023), p. 93 (Kindle version: page number may differ from the paperback edition).

The final phase, transportation, starts with the completion of the necessary shipping documents either by the consignor or the Customs broker, followed by the loading of goods onto the means of transport. The Customs clearance process follows, as the strategic goods depart the country. Once the products have cleared Customs, they are transported to their destination, often with intermediary stops that might present the opportunity for re-export and transshipment to the final destination and final end-user. The use of the shipper's name as consignee on the export/import declaration should be perceived as a red flag. Some shipping companies and commercial transporters can also trigger red flags, as they may be historically known to have participated in proliferation networks.

Graph 5. Transportation Phase



Source: Nelson, C. (2023), p. 94 (Kindle version: page number may differ from the paperback edition).

These steps demonstrate that strategic trade transactions have elements that take place in different jurisdictions, creating the need for a broad commonality of purpose and mandate to investigate and repress illicit strategic trade.

Investigating illicit strategic trade can pose serious challenges to Customs administrations for a number of reasons. First, international trade has dramatically increased over the past decades and accounts for an estimated USD 31 trillion in 2024.<sup>21</sup> The challenge for Customs administrations, vis-à-vis this trade volume, is to efficiently identify and control goods that can potentially be strategic, and, within this category, identify the small percentage of goods that may be illicitly shipped (see Graph 6). Effective enforcement powers further enable them to detain these consignments, launch an investigation, and apply various investigative techniques, including intelligence gathering.

Graph 6. Detection Target for Illicit Strategic Goods



Source: Nelson, C. (2023), p. 45 (Kindle version: page number may differ from the paperback edition).

<sup>21</sup> Willige, A. (2024), *Global trade growth could more than double in 2024. Here's why*, available at <https://www.weforum.org/agenda/2024/05/global-trade-to-double-2024-imf-wto/>

Another challenge which makes illicit strategic trade quite unique is the complexity of supply chains involving multiple actors and jurisdictions to evade controls. The rapid technological advancements and changes in the geopolitical landscape require awareness and continuous adaptation by Customs administrations and regulatory bodies.

Finally, in the context of general resource constraints, where more emphasis on the national level is placed on inbound activities that can offer the potential for revenue collection, export-related enforcement may become less of a priority. Coupled with other challenges that include a lack of domestic and international cooperation, and, most of all, the inability to identify potentially strategic items, can create a fruitful ground for proliferators.

Nevertheless, OSINT can potentially become another tool to be integrated within the all-source intelligence approach. OSINT can support Customs administrations in analysing strategic trade, and can be used to complement traditional intelligence gathering and controls. OSINT could be beneficial in three areas in particular, namely: identification of illicit trade patterns, risk assessment and profiling, and enhancing overall supply chain security.

First, OSINT can help identify trends and patterns in illicit trade by analysing data from various sources. For instance, monitoring online marketplaces and forums can reveal the sale of controlled or prohibited substances, commodities or technologies. By tracking keywords and phrases associated with illicit activities, Customs authorities can pinpoint suspicious transactions and entities.

OSINT can also help complement and build a quick transaction risk profile based on several indicators which can be researched using publicly and commercially available information:

- Consignor and consignee, including corporate structures;
- Commodity;
- Trade route;
- Jurisdiction;
- History of trade for both consignor and consignee; and
- Availability of a valid export licence.

The WCO has produced extensive manuals and training materials on trade risk assessment using complex methodologies.<sup>22</sup> Strategic trade risk profiling consists of online research to identify red flags which may warrant an inspection or enhanced controls.

Within this first area, several techniques can assist in assessing transaction risks. The first technique is macro- and micro-mirror statistics. Access to trade data can help Customs administrations detect discrepancies in the import of strategic goods at the macro and micro levels, and to identify whether an illicit acquisition programme may be in place for specific equipment or countries. Working at the micro level with commercially available nominal trade data helps provide an overview of historical transactions and an assessment of whether they could explain macro discrepancies. Sets of commercial trade data are difficult to source and acquire, but can be critical in detecting potential illicit trade and identifying a risk profile as described above.

---

<sup>22</sup> WCO *Customs Risk Management Compendium*, available at <https://www.wcoomd.org/en/topics/facilitation/instrument-and-tools/tools/risk-management-compendium.aspx>

The second technique is transshipment analysis, focusing more on the transport phase to identify the extent to which the route provider, point of departure or point of arrival might raise red flags. Transshipment and re-export are common features of international trade but can be used to obfuscate illicit strategic trade by using multiple ports or diversion of goods from their stated destination.

The third technique is comprehensive data analysis. The vast amount of data available through OSINT enables comprehensive analysis and cross-referencing of information. Advanced analytical tools can sift through large datasets to identify patterns, anomalies, and correlations that might be missed through traditional intelligence methods. This depth of analysis enhances the accuracy and reliability of the intelligence produced.

The fourth technique in this area is network analysis. Network analysis, using visualization tools like graphs and opensource research, enables Customs administrations to map relationships between the entities that are parties to a transaction as well as their historical interactions. It provides a way to detect patterns more easily.

In the second specific area, risk assessment and profiling, Customs administrations use OSINT to assess the risk associated with specific shipments, companies, or individuals. This involves gathering information from business registries, social media profiles, and financial records to build a comprehensive risk profile. OSINT tools can flag high-risk shipments for further inspection, improving the allocation of resources. OSINT can also be useful in preparing for the conduct of on-site post-control audit of a business entity.

Lastly, ensuring the security of global supply chains is a critical aspect of STCE. One way to do this is by enhancing existing STCE initiatives worldwide. For example, the WCO has implemented regular enforcement operations dubbed Operation Cosmo.<sup>23</sup> The first Operation Cosmo was conducted in 2014, as a global initiative aimed at enhancing the enforcement of strategic trade controls. This was the first-ever operation focused specifically on strategic goods, involving numerous international partners such as INTERPOL, the United Nations Office on Drugs and Crime (UNODC), the United Nations Office on Disarmament Affairs (UNODA), the International Atomic Energy Agency (IAEA), and the Organisation for the Prohibition of Chemical Weapons (OPCW). The operation had two key objectives:

- Detection and prevention through targeting illicit trafficking of strategic goods; and
- Capacity assessment through the evaluation of the Customs community's ability to enforce international strategic goods-related resolutions, such as UN Security Council Resolution 1540 concerning Weapons of Mass Destruction (WMD).

Operational coordination plays a key role in achieving these objectives. For this reason, the WCO usually establishes an Operational Coordination Unit (OCU) to support participating countries and facilitate international communication. In the case of Operation Cosmo, the OCU was established in Brussels.

The results of the Operation were significant, with over 140 high-risk consignments flagged, 380 messages exchanged on various cases, and 180 technical advice inquiries. About ten

---

<sup>23</sup> See WCO (2015), "Operation Cosmo – the first ever global WCO operation on strategic goods", WCO News 77, available at <https://mag.wcoomd.org/magazine/wco-news-77/operation-cosmo-the-first-ever-global-wco-operation-on-strategic-goods/>

cases of suspected trafficking and criminal activities were referred for further investigation.

Expanding on its success, Cosmo 2 was launched in 2018, attracting participation from 114 countries. The findings of Cosmo 2 suggested a need to shift towards the implementation of the regional operations instead of global ones. Based on this direction, several regional Cosmo operations have since taken place, specifically: Operation ASEAN Cosmo (2020), Operation Cosmo Central Asia (2022) and Operation Cosmo Mediterranean (2023). Additionally, future Cosmo operations are anticipated based on existing threat analysis.

Incorporating OSINT into future iterations of Operation Cosmo could provide real-time insights that can be critical at all stages of the operational activity. By integrating OSINT into the Operation Cosmo cycle, officers would be able to access timely and relevant information that complements traditional intelligence sources, enabling more accurate risk assessments and informed decision-making. The use of OSINT could also enrich the quality of information shared through the CENcomm platform<sup>24</sup> by providing a broader context and corroborative data that can be securely exchanged via encrypted channels. This integration would not only enhance the operational capabilities during the Operation Cosmo iterations but also ensure that participating countries have access to comprehensive intelligence, thereby improving the overall success of these enforcement efforts.

---

<sup>24</sup> See *Customs Enforcement Network Communication Platform (c)*, available at <https://www.wcoomd.org/en/topics/enforcement-and-compliance/instruments-and-tools/cen-suite/cencomm.aspx>

## IV. Implementing OSINT

### 1. Analysing challenges and identifying success factors

A SWOT analysis identifying strengths, weaknesses, opportunities and threats may provide a useful insight into the benefits of implementing OSINT in Customs.

Graph 7. SWOT Analysis: OSINT in Customs Enforcement

Strengths	Weaknesses
Cost-effectiveness Accessibility Real-time information Diverse data sources Enhanced collaboration Improved targeting	Data overload Information reliability issues Policy, privacy and legal concerns Resource intensity Fragmentation Evolving evasion techniques
Opportunities	Threats
Enhanced fraud detection Improved supply chain security Better resource allocation (e.g. patrolling) Proactive threat identification Collaboration with different partners Technology advancement	Evolving threat landscape with adaptive countermeasures from criminal organizations Cybersecurity risks Evolving data privacy regulations Limited financial and human resources for Customs

OSINT techniques present significant advantages in the field of Customs enforcement. Unlike other intelligence-gathering methods that may require expensive equipment and covert operations, OSINT leverages publicly available information, which is often free or inexpensive to access in a cost-effective manner. The accessibility of PAI allows Customs authorities to gather a wide variety of information without significant legal or logistical barriers. The dynamic nature of online platforms ensures that Customs can receive real-time updates on relevant activities. This is crucial for responding to time-sensitive situations, such as imminent smuggling attempts or fraud schemes.

OSINT encompasses a wide range of data types, including text, images, videos, and geolocation data. This diversity enables comprehensive analysis and a multifaceted understanding of the threat landscape. OSINT facilitates information sharing and collaboration between Customs and other law enforcement bodies, both domestically and internationally. Shared intelligence helps build a unified approach to combating cross-border crimes. With OSINT, Customs can better target their inspections and plan more effective interventions. By identifying high-risk shipments or individuals, they can focus their resources more efficiently, leading to increased interception rates of illicit goods.

The opportunities are multiple. Integration of OSINT into intelligence practices can enhance fraud detection and contribute to overall supply chain security. It may allow for better resource allocation, particularly when it relates to the deployment of border patrols in remote areas or

any other physical interventions. Given the real-time availability of PAI, proactive threat identification can be more easily achieved through OSINT than through some other intelligence sources, while its public availability can support the development of new partnerships with other governmental, non-governmental and business actors. As with any new ICT tool, the implementation of OSINT practices may serve as a catalyst for further technological advancements in the Customs administration due to the need to revise and strengthen certain protocols and Standard Operating Procedures (SOPs).

On the downside, Customs administrations may struggle to filter out irrelevant information and focus on actionable intelligence. Sophisticated tools and skilled analysts are therefore required. Customs administrations should invest in verification processes to ensure that the information they use is reliable, as information manipulation by malign actors has become an area of increasing concern in the open-source community. Collecting and using OSINT involves navigating complex legal and ethical issues related to privacy. Customs administrations must adhere to data protection regulations and respect individual privacy rights while conducting their intelligence operations. While OSINT is cost-effective in terms of data acquisition, it requires substantial human and technical resources for data analysis. Skilled analysts, advanced software tools, and continuous monitoring are necessary to extract meaningful insights from the data.

Open-source data is also often fragmented across multiple platforms and formats. Integrating and synthesizing this disparate information into coherent intelligence can be costly, challenging and time-consuming. Finally, as Customs authorities become more adept at using OSINT, criminals and smugglers are also developing more sophisticated methods to evade detection. These include encrypted communication channels, deep web platforms, and other means to obfuscate their activities.

The use of OSINT also presents a number of threats that need to be mitigated from the onset. These include an evolving landscape with adaptive countermeasures by criminal organizations, cybersecurity risks stemming from the use of OSINT without taking into consideration operational security (OPSEC) rules, evolving data and privacy regulations that require constant monitoring and adjustment, and limited financial and human resources in Customs administrations to support the deployment and smooth running of the OSINT operations.

Successfully addressing these threats and weaknesses requires time and a multifaceted approach. In this context, a number of key success factors can be identified.

The first factor in the successful implementation of OSINT in Customs administrations is a strategic decision to support its use at the highest levels of the organization. This decision must be backed by a clear understanding of the potential benefits of OSINT, including enhanced risk management, improved detection of illegal activities, and more effective enforcement actions. High-level commitment is crucial because it ensures that OSINT initiatives receive the necessary attention, resources, and support to succeed.

The development of dedicated policies and regulatory frameworks is crucial for defining how OSINT should be applied within the Customs administration. These policies should provide clear guidance on the scope and objectives of OSINT activities, as well as the related legal and ethical considerations.

## Box 2. Policy development and regulatory framework

*Policy development involves defining what OSINT is, how it will be used, and the specific procedures and protocols that will govern its implementation. Policies should address key issues such as data privacy, information security, and compliance with relevant laws and regulations. They should also outline the roles and responsibilities of different stakeholders, including the OSINT unit, other units within the Customs administration, and external partners.*

*In some cases, the implementation of OSINT may require the development of a special regulatory framework. This should establish the legal basis for OSINT activities, including the authority to collect and analyse PAI. It should also provide safeguards to protect the rights and privacy of individuals, as well as mechanisms for oversight and accountability. The regulatory framework should be designed to be flexible and adaptable, allowing for adjustments as new technologies and methodologies emerge.*

*Adequate budgets, resources and equipment* are essential for the successful implementation of OSINT in Customs administrations. Without sufficient funding and resources, OSINT initiatives are unlikely to achieve their full potential. Effective resource management involves ensuring that OSINT specialists have access to the necessary tools and technologies to perform their functions. These includes equipment, advanced data analytics software, and the relevant databases and information sources. Resource management also involves optimizing the use of available resources, such as leveraging partnerships with external agencies to enhance information sharing and reduce costs.

The creation of a dedicated OSINT team or pool of specialists within Customs administrations is another critical factor in successful implementation. This team should be responsible for all aspects of OSINT operations, from data collection and analysis to dissemination of intelligence products. A dedicated team ensures that OSINT activities are conducted in a coordinated and systematic manner, leveraging specialized expertise and resources.

The success of OSINT initiatives in Customs administrations relies heavily on the identification, hiring, and training of skilled personnel. Talented individuals with the right skills and expertise are essential to conducting effective OSINT operations.

Identifying the right talent involves understanding the specific skills and expertise required for OSINT activities. This includes knowledge of data acumen, technical aptitudes, and relevant foreign languages. It also involves identifying individuals with the ability to think critically and creatively, as well as the capacity to adapt to new technologies and methodologies.

Recruitment and hiring processes should be designed to attract and select the best candidates for OSINT roles. This includes developing targeted recruitment strategies, conducting rigorous selection processes, and offering competitive compensation and benefits packages which are competitive for the sector. Recruitment efforts should also focus on building a diverse and inclusive workforce, recognizing that different perspectives and experiences can enhance the effectiveness of OSINT operations.

Training and development are crucial for building and maintaining the skills and expertise of OSINT specialists. This includes providing initial training for new recruits, as well as ongoing professional development opportunities to keep staff up to date with the latest advancements in the field. Training programmes should cover a range of topics, including cyber security, OSINT methodology, automating data collection and creating personas (where allowed by national legislation), and best practices for OSINT operations.

Last but not least, cooperation with other teams within the Customs administration is essential for the success of the OSINT unit. This includes working closely with enforcement, risk management, and traditional intelligence units to ensure that OSINT activities are aligned with broader organizational objectives. Inter-agency cooperation, with tax teams for example, is also beneficial, as access to tax data can significantly enhance the all-source intelligence approach. Thus, implementing OSINT will lead toward the establishment of partnerships with external agencies, such as law enforcement, intelligence services, private sector organizations and academics, to enhance information sharing and leverage additional resources.

## 2. Avoiding pitfalls

Implementing OSINT in Customs administrations can be challenging as the domain is new and structures or regulatory frameworks may not be sufficiently updated to govern use of advancing technology or new practices. Implementing OSINT requires a multifaceted and strategic approach. By addressing technical, operational, legal, ethical, organizational, and resource-related challenges, Customs administrations can effectively integrate OSINT into their operations and realize its full potential for the purpose of improving enforcement capabilities.

### *Achieving buy-in from senior management*

Achieving internal buy-in for OSINT initiatives can be challenging, in the face of resistance to change or scepticism about the value of OSINT in Customs operations. Demonstrating quick wins is an important strategy for building support for OSINT initiatives within Customs administrations. Quick wins are small, achievable success stories that demonstrate the value of OSINT and generate buy-in from stakeholders.

Identifying quick wins involves selecting specific projects or initiatives that can deliver immediate and tangible results. These projects should be carefully chosen to showcase the benefits of OSINT and align with the strategic objectives of the Customs administration. Quick wins might include revenue recovery or successful interdictions of illicit goods, enhanced risk assessments, or improved intelligence sharing with external partners. Communicating the successful is crucial for generating buy-in and support for OSINT initiatives. This involves sharing success stories with stakeholders, including senior leadership, staff, and external partners. Communication efforts should highlight the specific benefits of OSINT, such as improved enforcement outcomes, enhanced risk management, and increased operational efficiency.

Building on the momentum of quick wins is essential for sustaining support for OSINT initiatives. This involves using the success of quick wins to advocate for continued investment in OSINT and to promote the adoption of OSINT practices more broadly. It also involves leveraging the lessons learned from quick wins to inform the ongoing development and refinement of OSINT strategies and operations.

### *Overcoming legal hurdles*

The legal landscape surrounding OSINT is complex, with various laws and regulations governing data privacy, surveillance, and information sharing. Customs administrations have to navigate these carefully.

Collecting and analysing PAI raises significant privacy concerns, particularly when it involves personal data. Balancing the need for intelligence with respect for privacy rights is a critical ethical challenge. A strategy encompassing the following elements can be adopted:

1. **Legal Consultation:** Engaging legal experts to review OSINT policies and practices ensures compliance with relevant laws and regulations.
2. **Clear Policies and Guidelines:** Developing clear policies and guidelines that outline the legal boundaries and ethical considerations for OSINT activities.
3. **Regular Legal Reviews:** Conducting regular reviews of legal frameworks and updating OSINT practices accordingly to remain compliant with any changes in the law.
4. **Data Anonymization:** Implementing techniques to anonymize personal data can help mitigate privacy risks while still allowing for valuable intelligence gathering.
5. **Ethical Standards and Continuous Training:** Establishing strict ethical standards and providing training on privacy issues ensures that officers are aware of the importance of respecting individuals' privacy.
6. **Transparency and Accountability:** Maintaining transparency with respect to OSINT activities and establishing mechanisms for accountability can build trust and ensure ethical practices.

### *Getting data access*

One of the primary technical challenges in OSINT implementation is ensuring access to data located on social media platforms, which requires the creation of an online persona. The following strategy can be adopted to overcome this challenge.

1. **Enhancing the Regulatory and Policy Framework:** Creating the right regulatory and policy framework to enable Customs administration to use online personas as passive research access keys while maintaining discretion and operational security (OPSEC).
2. **Providing Training:** Providing all OSINT Customs officers with the appropriate training plan to create and maintain online personas for passive online research.
3. **Supplying the Resources:** Providing dedicated units with the resources to configure a dedicated research environment with special equipment disconnected from equipment and machines used for work or personal affairs.
4. **Ensuring Accountability:** Putting in place solutions and mechanisms which allow tracking of work and auditing.

### *Hiring and retaining talent*

OSINT requires various skills including knowledge of languages, analysis, cyber intelligence, data acumen, technical aptitudes and a good awareness of information security challenges. These rare profiles are difficult to identify and recruit. In addition, the speed of technological development in the sector makes it hard to remain current. Ensuring that staff are adequately trained is a significant operational challenge. The following strategy can be adopted to mitigate this challenge:

1. **Comprehensive Training Programmes:** Developing comprehensive training programmes that cover all aspects of OSINT, including data collection, analysis, operational security, use of code and scripting, and ethical considerations.
2. **Continuous Professional Development:** Encouraging continuous learning and professional development to keep pace with evolving technologies and methodologies, with professional certifications and participation in more specialized workshops and professional conferences.

- 3. Partnerships: Partnering with academic institutions and professional organizations can provide access to specialized training and certification programmes.

*Learning from other parties*

Implementing OSINT in Customs administrations can be a long and cumbersome process. Other countries have reached a more mature model that integrates OSINT into the organization and processes. Exchanging best practices with others on the steps taken to implement OSINT, hurdles faced and ways to overcome them is critical for organizations that are committed to implementing OSINT effectively. The following strategy can be adopted:

- 1. Participation in sector-led OSINT community events: The WCO can provide a platform to facilitate information sharing and exchange of different practices among Member administrations related to OSINT implementation and associated challenges.
- 2. Developing a culture of information sharing: Customs can exchange approaches, best practices and the latest OSINT developments in bilateral discussions or by participating in communities of practice that can be established either with the support of organizations such as the WCO, or any other entities that promote the development of OSINT, with a view to facilitate peer-to-peer exchanges.

### 3. Addressing training and capacity building

Capacity building is critical in implementing OSINT in Customs administrations and provides an opportunity to create a training pathway for different Customs officers and to promote professionalization and standards in practising OSINT techniques. This would enable Customs to address different skill levels from foundation to expert level, developing cybersecurity, data and technical acumen. It would help prepare and train the next generation of the OSINT workforce. Not all Customs officers would follow the entire training path, but it would provide a general understanding of open-source research and online security while developing the skills and knowledge of more specialized teams. A description of four different levels of training that could be adopted by a Customs administration is set out below.

Graph 8. Levels of OSINT Training



Given the dynamic nature of OSINT, creating an OSINT Community of Practice (CoP) among Customs administrations would be vital to effectively implement OSINT techniques within teams, and would enhance risk management, improve border security, support trade facilitation and foster international collaboration. An OSINT CoP would be able to leverage diverse expertise, facilitate knowledge sharing and drive continuous improvement, as well as monitor technology advancement.

The main objectives of an OSINT CoP would be to ensure the roll-out of OSINT within Customs administrations by raising awareness, mentoring newly trained officers and following up on the latest developments in the OSINT sector. An OSINT CoP would also be the place to share best practices and reflect on the challenges to developing regulatory frameworks enabling the sector to effectively conduct OSINT investigations. An OSINT CoP could develop protocols for information sharing, ensuring that sensitive data is protected while enabling the free flow of information and establishing guidelines for data classification, access control, and information dissemination.

Not only would an OSINT CoP promote a degree of standardization of OSINT techniques among administrations, but it would also support the implementation of collaboration tools, such as secure messaging platforms, collaborative workspaces, and document-sharing systems. An OSINT CoP would, moreover, be in a position to create mechanisms for knowledge sharing, such as regular meetings, webinars, and online forums. It could encourage participants to share insights, experiences, and best practices related to OSINT in Customs administration. Trained groups and identified OSINT champions among Customs administrations could be the first members of the OSINT CoP.

## Conclusion

The integration of OSINT into Customs administration practices marks a significant advance in addressing the multifaceted challenges faced by modern Customs authorities. As global trade and the volumes of digital information continue to expand, the need for efficient, effective, and adaptive Customs enforcement becomes increasingly critical. OSINT offers a cost-effective, versatile and powerful toolset that enables Customs administrations to better enhance their capabilities in safeguarding national borders, ensuring compliance with trade regulations, and contributing to national and international security.

Customs administrations are tasked with a wide range of responsibilities, from revenue collection and trade facilitation to enforcing laws and regulations against illicit trade and enhancing national security. The traditional role of Customs as gatekeepers has evolved into a more dynamic function that necessitates the seamless facilitation of legitimate trade while robustly combating illicit activities. The use of OSINT plays a pivotal role in this transformation by providing real-time, actionable intelligence derived from PAI. In other words, the adoption of advanced ICT, coupled with OSINT, allows Customs administrations to leverage a diverse array of sources, including social media, news articles, government publications, and specialized databases, in a more streamlined and cost-effective way.

One of the primary benefits of OSINT is its ability to enhance real-time risk management and border security. By monitoring global news, social media platforms, and specialized forums, Customs administrations can identify new smuggling methods, shifts in trafficking patterns, and changes in trade dynamics. This proactive approach enables Customs to anticipate and mitigate risks more effectively, ensuring that resources are allocated where they are needed most.

The use of OSINT in real-time threat monitoring and risk profiling allows Customs to create detailed profiles of high-risk individuals, organizations, and shipments. This targeted approach not only improves the efficiency of inspections and investigations but also ensures that enforcement efforts are focused on the highest risks. Furthermore, the integration of predictive analytics enables Customs to forecast potential threats based on historical data and trends, facilitating better preparedness and resource allocation.

OSINT plays a crucial role in supporting trade compliance and fraud detection by providing Customs administrations with the tools to verify the authenticity of trade documents, monitor corporate activities, and detect fraudulent schemes. By cross-referencing information from various public sources, Customs officers can identify discrepancies in trade documents, uncover instances of misclassification and undervaluation, and detect complex fraudulent schemes such as trade-based money laundering.

The ability to monitor and analyse corporate social media and website activities provides additional layers of insight into business practices and potential violations of trade regulations. This comprehensive approach to compliance monitoring ensures that Customs can proactively address non-compliance issues and take appropriate actions to enforce trade laws.

The prevention of smuggling and trafficking is a core function of Customs administrations, and OSINT significantly enhances their capabilities in this area. By analysing PAI from various sources, Customs can identify smuggling routes, track illegal shipments, and monitor smuggling networks. The use of GEOINT further complements OSINT by providing a spatial context to the information gathered, enabling Customs to map out smuggling routes and identify hotspots of illegal activities.

The ability to track and intercept illegal shipments in real-time allows Customs to respond swiftly to potential threats and prevent the entry of illicit goods into the country. By leveraging

network analysis tools, Customs can visualize and understand the structure of smuggling networks, making it easier to target key players and dismantle these networks.

While OSINT offers numerous benefits, Customs administrations must also address certain challenges to fully leverage its potential. These challenges include managing the sheer volume of data, ensuring the reliability and accuracy of information, navigating legal and ethical considerations, and addressing resource limitations. By implementing robust data analytics tools, rigorous verification processes, and comprehensive training programmes, Customs can overcome these challenges and maximize the effectiveness of OSINT.

As technology evolves and the digital landscape expands, Customs administrations must remain agile and adaptive, embracing new opportunities that datafication offers in order to stay ahead of emerging threats. The future of Customs enforcement lies in the continuous enhancement of capabilities through the adoption of advanced technologies, fostering international collaboration, and offering continuous learning opportunities to its staff. In addition to its core value, OSINT can serve as a catalyst in these areas, as it is intrinsically interconnected with and highly dependent on them.

## Additional resources for further reading

### Government Strategy and Policy Papers

**Intelligence Community (IC) OSINT Strategy 2024-2026:** Published by the Office of the Director of National Intelligence (ODNI) and the Central Intelligence Agency (CIA), this strategy outlines the goals for OSINT within the U.S. Intelligence Community for the next three years. It focuses on improving the integration of OSINT across various intelligence disciplines, enhancing capabilities, and fostering collaboration with international partners ([DNI.gov](#)) ([ODNI](#)).

**U.S. Army OSINT Strategy:** The U.S. Army has developed a strategy to integrate OSINT into its intelligence operations. The strategy is structured around four main lines of effort: people, modernization, readiness, and allies and partners. It emphasizes the need to build dedicated OSINT teams, modernize training and equipment, ensure readiness through practical exercises, and enhance information sharing with allies ([CSIS](#)).

**“The Future of Open Source Intelligence for UK National Security”** by the Royal United Services Institute (RUSI): This paper explores the use of PAI and OSINT for national security in the UK. It discusses the implications of increased accessibility to OSINT tools and data, and provides recommendations for future policy development. It highlights the commercial, cultural, policy, and technological implications for national security stakeholders in the UK ([Homepage](#)).

**“Deploying OSINT in Armed Conflict Settings: Law, Ethics, and the Need for a New Theory of Harm”** by the International Committee of the Red Cross (ICRC): This policy paper examines the legal and ethical considerations of using OSINT in armed conflict. It addresses the gaps in International Humanitarian Law (IHL) regarding the classification of data and the implications of OSINT activities for privacy and data protection rights during conflicts ([ICRC Blogs](#)).

**“Open Source Intelligence”** by RAND Corporation: RAND has produced several reports on OSINT, focusing on various aspects such as its use in tracking extremism, civilian resistance, and national security. One notable report is on the use of night-time lighting data to analyse prisons and detention centres in Tibet, showcasing innovative applications of OSINT in human rights and security contexts ([RAND Analysis](#)).

**“Open Source Intelligence”** by International Cybersecurity Law Review: This paper discusses the integration of OSINT with Social Media Intelligence (SOCMINT) and Human Intelligence (HUMINT) for activities such as social engineering and risk management. It provides insights into how OSINT is used in different sectors, including law enforcement and civil protection ([Springer](#)).

## Books

**“OSINT Techniques: Resources for Uncovering Online Information” by Michael Bazzell (2023)** - This comprehensive guide is often considered a gold standard in the OSINT community, providing updated techniques, tools, and methods for effective online investigations.

**“We Are Bellingcat: An Intelligence Agency for the People” by Eliot Higgins (2021)** - This book details the story of Bellingcat, a collective of citizen journalists using OSINT to uncover truths behind major global events.

**“OSINT 101: The Ultimate Open Source Intelligence Handbook” (2023)** - A beginner-friendly guide that covers the basics of OSINT, including data collection, analysis, and visualization.

**“OSINT Handbook: The Ultimate Guide to Open Source Intelligence Methods and Tools” by Ambre Laurent (2023)** - A comprehensive resource for mastering OSINT, with practical methods and tools for gathering and analysing PAI.

**“OSINT for Everyone: A Beginner’s Guide to Open Source Intelligence” by Ezra Mendoza (2023)** - This book provides a practical guide for conducting investigations using OSINT, suitable for both beginners and experienced professionals.

## Glossary of terms

**Anonymization:** The process of removing or disguising identifying details to protect the identity of individuals and organizations.

**Big Data Analytics:** The process of examining large and varied data sets to uncover hidden patterns, unknown correlations, and other insights.

**Cybersecurity:** The practice of protecting systems, networks, and programs from digital attacks.

**Customs Enforcement:** The activities carried out by Customs authorities to monitor and regulate the flow of goods across borders, ensuring compliance with national and international laws.

**Data Archiving:** The process of storing data in such a way that it can be retrieved and used in the future.

**Digital Footprint:** The trail of data that a person leaves behind while using the Internet. This includes all the information that a user creates, shares, and interacts with online, such as social media posts, browsing history, emails, and online transactions.

**Digital Hygiene:** Basic principles and practices that ensure the security and proper handling of digital information.

**Geospatial Intelligence (GEOINT):** The use of satellite imagery, Geographic Information Systems (GIS), and location-based data to provide spatial context to information.

**Open-Source Intelligence (OSINT):** The process of collecting, analysing, and utilizing information that is publicly and commercially available to support intelligence and decision-making processes.

**Operational Security (OPSEC):** Measures taken to protect sensitive information and operations from being disclosed or compromised.

**Predictive Analytics:** The use of historical data and statistical techniques to predict future outcomes.

**Social Media Analysis:** The process of monitoring and analysing social media platforms for information.

**Strategic Trade:** international trade of goods, services, and technologies that are critical to national security, economic stability, and foreign policy interests. These items often include military and dual-use goods (items that can be used for both civilian and military purposes).

**Trade-Based Money Laundering (TBML):** The process of disguising the proceeds of crime and moving value through trade transactions.

## Bibliography

Cantens, T. (2019), "Potential uses of geodata for border management", WCO News 89, available at <https://mag.wcoomd.org/magazine/wco-news-89/potential-uses-of-geodata-for-border-management/>.

Kemp, S. (2024), Digital 2024: Global Overview Report, available at <https://datareportal.com/reports/digital-2024-global-overview-report>.

Mikuriya, K. and T. Cantens (2020). If algorithms dream of Customs, do customs officials dream of algorithms? A manifesto for data mobilisation in Customs. *World Customs Journal*, 14(2), 3-18.

Nelson, C. (2023). *Methods of strategic trade analysis: Data-driven approaches to detect illicit dual-use trade*. Springer.

Reinsel, D., Gantz, J., & Rydning, J. (2018). *The Digitization of the World: From Edge to Core*. International Data Corporation (IDC).

United Nations Security Council Resolution 1540 (2004), available at [https://documents.un.org/symbol-explorer?s=S/RES/1540\(2004\)&i=S/RES/1540\(2004\)\\_0402930](https://documents.un.org/symbol-explorer?s=S/RES/1540(2004)&i=S/RES/1540(2004)_0402930).

WCO (2015), "Operation Cosmo – the first ever global WCO operation on strategic goods", WCO News 77, available at <https://mag.wcoomd.org/magazine/wco-news-77/operation-cosmo-the-first-ever-global-wco-operation-on-strategic-goods/>.

WCO (2015), *Punta Cana Resolution*, available at <https://www.wcoomd.org/-/media/wco/public/global/pdf/about-us/legal-instruments/resolutions/resolution-of-the-wco-policy-commission-on-the-role-of-customs-in-the-security-context.pdf?la=en>.

WCO (2018), *IT Guide for Executives*, available at <https://www.wcoomd.org/-/media/wco/public/global/pdf/topics/facilitation/instruments-and-tools/tools/it-guide-for-executives/it-guide-executives.pdf?db=web>

WCO (2019), *Geodata Discovery Day*, available at <https://www.wcoomd.org/en/media/newsroom/2019/may/geodata-discovery-day.aspx>.

WCO (2022), *Secretariat Note on the Role of Customs in Fragile and Conflict-Affected Situations*, available at in [https://www.wcoomd.org/-/media/wco/public/global/pdf/topics/research/report/fragility\\_secretariatnote\\_pc\\_council\\_2022\\_may19version\\_en.pdf?db=web](https://www.wcoomd.org/-/media/wco/public/global/pdf/topics/research/report/fragility_secretariatnote_pc_council_2022_may19version_en.pdf?db=web).

WCO (2023), *Outcomes of the 2023 WCO Council Sessions: Election of a new WCO Secretary General and Chairperson of the WCO Council*, available at <https://www.wcoomd.org/en/media/newsroom/2023/june/outcomes-of-the-2023-wco-council-sessions.aspx>

WCO, *Customs Enforcement Network Communication Platform*, available at <https://www.wcoomd.org/en/topics/enforcement-and-compliance/instruments-and-tools/cen-suite/cencomm.aspx>.

WCO, *WCO Customs Risk Management Compendium*, available at

<https://www.wcoomd.org/en/topics/facilitation/instrument-and-tools/tools/risk-management-compendium.aspx>.

WCO/WTO (2022), “*The role of advanced technologies in cross-border trade: A customs perspective*”, available at <https://www.wcoomd.org/en/topics/facilitation/instrument-and-tools/tools/wco-wto-paper.aspx>.

WCO/WTO Study Report on Disruptive Technologies (2022), available at <https://www.wcoomd.org/en/topics/facilitation/instrument-and-tools/tools/wco-wto-study-report-on-disruptive-technologies-2022.aspx>.

Willige, A. (2024), *Global trade growth could more than double in 2024. Here’s why*, available at <https://www.weforum.org/agenda/2024/05/global-trade-to-double-2024-imf-wto/>.

**Contact us:**

[WCOSecurityProgramme@wcoomd.org](mailto:WCOSecurityProgramme@wcoomd.org)

**Visit our website:**

[www.wcoomd.org](http://www.wcoomd.org)

**Copyright © July 2024, World Customs Organization (WCO). All rights reserved.**  
The original version of this report was produced by the WCO in English.  
The WCO is the exclusive holder of all intellectual property  
rights on this report.



