Postal Services and Organised Crime


Alexandria Reid

E-commerce and cross-border delivery services within the EU are about to become more competitive, as new regulations introduced by the European Commission will permit a consumer in France to purchase a Gucci handbag from the company’s Romanian website with greater ease. While consumers are likely to rejoice at renewed efforts to harmonise prices across the single market, organised crime groups reliant on the postal system to traffic illicit goods are also likely to benefit.

Postal and parcel delivery services are the unsung heroes of the global e-commerce revolution. In Europe, where more than four billion packages containing goods ordered online are delivered each year, these services have become part and parcel of European prosperity. At face value, this figure may seem high, but what it belies are the remaining barriers that continue to hinder cross-border e-commerce within the single market.

Taking aim at two such barriers, the European Commission has introduced two new regulations: to drive down cross-border delivery prices; and to help consumers order from online businesses in neighbouring European states by banning ‘geo-blocking’ (discrimination against online consumers based on the territory where a consumer’s IP address is based). Promisingly, these measures are set to significantly increase e-commerce and parcel traffic across the EU. Yet, in the absence of a rigorous risk assessment, they could also have unforeseen security implications. Although it is seldom considered a national security threat, the use of postal and parcel delivery services by organised crime groups (OCGs) is a growing concern for European law enforcement. Left unchecked, small parcels can bring big environmental, social and health risks straight to the door of European consumers.

As part of its Digital Single Market Strategy, the European Commission is right to try and eliminate any remaining barriers to e-commerce in Europe. Although many of these barriers may seem invisible to the individual consumer, e-commerce in Europe still has a distinctly national character. In 2016, for example, almost all of the EU-28 enterprises surveyed by Eurostat reported that they made web sales to customers in their own country, but only 7% of enterprises made web sales to other EU countries. This is attributed to two factors: the high price of cross-border delivery services; and the barriers created by geo-blocking.

Europol’s 2015 assessment of the future of organised crime devotes significant attention to the postal system

While these incoming regulations will help entrepreneurs to corner new markets, expand their production capacity and increase their profitability and resilience, they will also benefit criminal actors. Over the past few years, OCGs have already demonstrated a vast capacity to permeate the postal and delivery service market, using these often-unwitting providers to move all manner of illegal goods, from counterfeit clothing to weapons and drugs. This incessant flow of postal traffic does not minimise the significance of large-scale containerised shipping methods in moving illicit and illegal commodities, but it does demonstrate the versatility and creativity of OCGs and their ability to capitalise on new trends in the delivery marketplace. These new regulations are one such trend.

Although it is challenging to accurately estimate the size of the problem, recent research by the UK Intellectual Property Office suggests that EU customs agencies have struggled to adapt to the risks posed by shifting delivery patterns, characterised by the decline of letter volumes and a steady rise in the volume of small parcels in the postal system. Indeed, an influential 2016 study found that 60% of the total volume of global seizures in counterfeit goods between 2011 and 2013 were of small packages. Even without the added pressure of increased postal traffic created by these incoming regulations, many European customs agencies continue to grapple with these more fundamental changes in delivery patterns.

For law enforcement, detecting and seizing counterfeit goods transported
this way is a time-consuming and costly activity. Criminals know that the resourcing required to police this high volume of traffic means that only those consignments deemed most suspicious or conspicuous are pulled out for inspection. This low-volume, high-frequency method has benefits for an OCG: not only do consignments carry a low risk of detection, but the financial loss incurred in the event of a seizure represents only a small loss to their overall profit margin.

Recognising this threat, Europol’s 2015 assessment of the future of organised crime devotes significant attention to the postal system, including the risk posed by increased automation, decentralisation and new technologies in the delivery sector. Likewise, the UK National Crime Agency’s 2018 National Strategic Assessment devotes a significant portion of its threat assessment to the postal system and fast parcel-service providers, specifically in the fight against Class A drugs and weapons. In the UK to date, all known seizures of the synthetic opioid known as fentanyl have originated in the fast parcel or postal system.

Yet, as RUSI’s recent research on the use of delivery services in the illicit tobacco trade has found, the risk of carrying illicit tobacco products
varies considerably across the delivery service market. For example, whereas the largest Europe-wide carriers usually offer fully integrated supply chains that are less vulnerable to those seeking to smuggle illicit tobacco products, many medium and small-sized operators run more fragmented and consequently vulnerable operations. This marketplace is further fragmented by the practically unregulated smaller operators, many running ‘one man, one van’-style cross-border deliveries throughout Europe under little scrutiny.

Given these well-known security risks, the European Commission has described the delivery measures have taken effect. Liberalising cross-border parcel delivery at the end of 2020, two years after the advanced data regulations at the future customs planning. Indeed, at present, several European customs agencies across Europe remain critically under-resourced. The German customs authority, for example, has 40,000 staff, with 1,600 new positions to be filled by 2022, but Customs and Financial Trade Union leader Dieter Dewes has described the force as only ‘conditionally operational’ (not operating at full capacity or with the resourcing required to meet strategic objectives) under current staffing levels. This also comes at a time when resourcing for the UK’s own Border Force has been cut considerably, and the future of UK customs arrangements continues to hang in the balance in Brexit negotiations. For other countries, the fact that these regulations entered into force on 3 December may compound issues created by increasing traffic in combination with the usual already burdensome Christmas rush.

The European Commission plans to evaluate the impact of these new regulations in May 2020. So far, it is anticipated that this evaluation will centre on expanding the policy to electronically supplied services offering copyrighted content such as e-books, software and online games. But this review also creates an opportunity for the European Commission to propose new rules ‘where necessary’, or in light of legal, technical and economic developments. With this in mind, the review should also be used as an opportunity to assess what effect these policies have had on the organised crime landscape in Europe.

**An influential 2016 study found that 60% of the total volume of global seizures in counterfeit goods between 2011 and 2013 were of small packages**

Meanwhile, there are also unique vulnerabilities in the postal system. It is widely recognised, for example, that national postal operators are vulnerable because they receive little reliable advance data about incoming postal traffic. This makes it extremely challenging to perform the advance risk assessments on which European customs agencies rely. This is a well-recognised vulnerability, leading the Universal Postal Union to integrate new electronic advance data requirements into its universal obligations. Under current plans, however, European operators will only become compliant with these advanced data regulations at the end of 2020, two years after the liberalising cross-border parcel-delivery measures have taken effect.

**The use of postal and parcel delivery services by organised crime groups is a growing concern for European law enforcement**

To do this effectively, the architects of the review must lay the groundwork now by beginning to think about what data-collection methods they plan to use to measure the effects of these regulations in two years’ time. At a time when European law enforcement agencies are already concerned about crime in the postal and parcel system, the failure to include a security-related metric in the review would be short-sighted. When it comes to the necessary trade-offs between trade facilitation and potential security threats, it is the European Commission’s duty to take only calculated risks and guarantee the security of EU consumers this Christmas and beyond.

**Alexandria Reid**

Alexandria is a Research Analyst in the National Security Studies group at RUSI. Her research covers a range of topics related to serious and organised crime, including environmental crime and illicit trade.


The views expressed in this article are the author’s, and do not necessarily represent those of RUSI or any other institution.