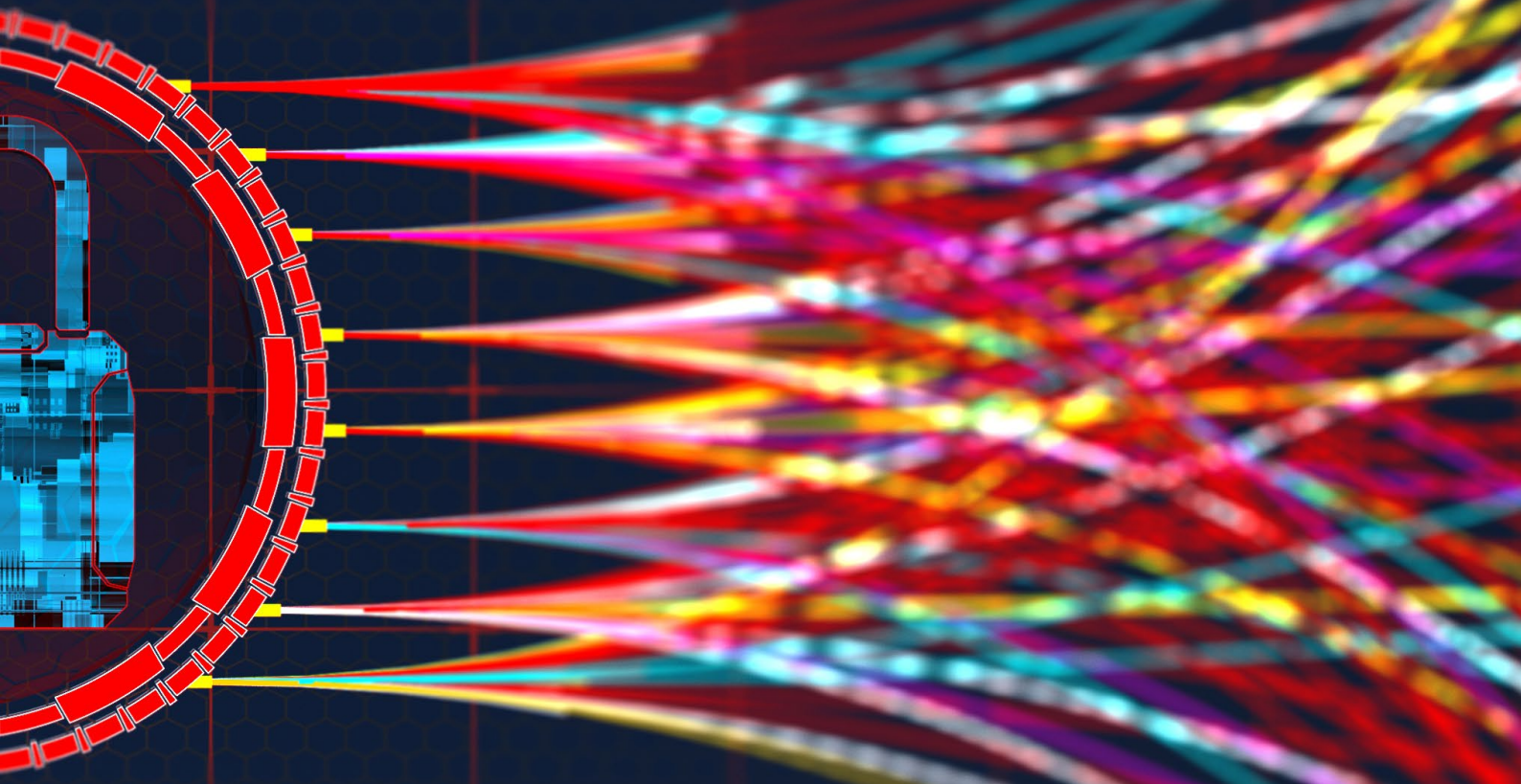
The Economist INTELLIGENCE UNIT

UNINTENDED CONSEQUENCES, UNEXPECTED BENEFITS:

Technology, crime and illicit trade



Supported by:

PHILIP MORRIS INTERNATIONAL

Acknowledgements

Unintended consequences, unexpected benefits: Technology, crime and illicit trade is a report from The Economist Intelligence Unit sponsored by Philip Morris International. The paper was written by Chris Clague and Michael Frank.

1. Introduction

Advances in technology bring many benefits, as the speed of development of the covid-19 vaccines demonstrates. But they also create new tensions across a host of areas. Automation increases returns to capital and lowers the costs of goods, but at the same time raises concerns about a shrinking labour market. The internet and social media were once heralded as breakthroughs that would improve communications and grant everyone access to the world's knowledge at the click of a mouse. While those hopes have been realised, they've also been accompanied by an ugly downside of widespread rage, vitriol and disinformation enabled by, among other features, the mask of anonymity many websites and apps grant users.

Advances in technology bring many benefits, but they also create new tensions across a host of areas.

These tensions play out in a similar fashion in the world of crime and illicit trade. Take, for example, the fentanyl epidemic in the US. Fentanyl, a synthetic opioid, is 50 times more powerful than heroin and in 2017 alone, it and other synthetic opioids were responsible for 28,000 deaths from overdose.[1] Unlike the oxycontin opioid epidemic that preceded it, however, fentanyl wasn't over-prescribed by physicians. Instead, it was—and continues to be—ordered online through individual sellers and marketplaces, which are almost all located in China. Orders are then shipped to America in small packages that often go undetected because of the immense—and still growing—volume of similarly-sized packages inundating the system as a result of the rapid expansion of e-commerce over the past decade or so. In fact, the sellers even told US senate investigators posing as buyers that they preferred to ship via the US Postal Service because "delivery was essentially guaranteed".[2]

The pandemic of 2020 has played a major role in accelerating illicit trade's online market expansion. While the accelerated transition from brick-and-mortar to e-commerce saved legitimate businesses and benefited consumers.[3] it has also created opportunities for criminals to profit through selling fake Personal Protective Equipment (PPE) and carrying out data theft.[4] Individuals and government authorities suffered as a result. The Financial Action Task Force recorded cases of counterfeiting medical goods and PPE fraud in over a dozen countries, including Germany, United Kingdom and Korea.[5] As predicted, merely weeks after the approval of the first covid-19 vaccines, fraud relating to fake vaccines are already emerging.[6]

1 *Synthetic Opioid Overdose Data*. Centers for Disease Control and Prevention. Last Reviewed on 19 March 2020. Available online at https://www.cdc.gov/drugoverdose/data/fentanyl.html
2 *Combatting the Opioid Crisis: Exploiting Vulnerabilities in International Mail*. Statement of Chairman Rob Portman, U.S. Senate Permanent Subcommittee on Investigations. 25 January 2018. Available online at https://www.hsgac.senate.gov/imo/media/doc/01.25.18%20Chairman%20Portman's%20Opening%20Statement.pdf
3 *E-commerce in the times of COVID-19*. OECD. 7 October 2020. Available online at https://read.oecd-ilibrary.org/view/?ref=137_137212-tofjgnerdb&title=E-commerce-in-the-time-of-COVID-19
4 *Research Brief*: COVID-19-related Trafficking of Medical Products as a Threat to Public Health. UNODC. 2020. Available online at https://www.unodc.org/documents/data-and-analysis/covid/COVID-19_research_brief_trafficking_medical_products.pdf
5 *COVID-19-related Money Laundering and Terrorist Financing Risks and Policy Responses*. FATF. May 2020. Available online at https://www.fatf-gafi.org/publications/fatfgeneral/documents/covid-19-ml-tf.html
6 *Fake NHS vaccine messages sent in banking fraud scam*. BBC News. 6 January 2021. Available online at https://www.bbc.co.uk/news/business-55563748

The National Crime Agency (NCA) in the United Kingdom issued a warning in January urging the public to be vigilant as malicious opportunists start to profit through covid vaccine scams.[7]

The availability of counterfeit products on various platforms has been an issue for e-commerce almost since their very beginning. The possibility that the success of these platforms would open the door for greater cross-border trade in illicit substances, a greater crime, probably did not occur to many at the time.

In this paper, we look at three other technologies that have had unintended consequences or unexpected benefits (or both) when it comes to illicit trade. The first is encryption and the reasons why it has become more important for citizens and criminals alike. The second is blockchain, which is helping to counter illicit trade by verification and authentication of shipments while at the same time serving as the backbone for various cryptocurrencies favored by criminals. The third is 3D printing, an emerging technology that, most notoriously, enables the printing of firearms, but could also provide a useful tool for law enforcement agencies in combating illicit trade and other criminal activities.

6 *Fake NHS vaccine messages sent in banking fraud scam*. BBC News. 6 January 2021. Available online at https://www.bbc.co.uk/news/business-55563748

7 Public urged to be vigilant as fraudsters target elderly and vulnerable with fake Covid vaccine. National Crime Agency. 8 January 2021. Available online at https://www.nationalcrimeagency.gov.uk/news/public-urged-to-be-vigilant-as-fraudsters-target-elderly-and-vulnerable-with-fake-covid-vaccine

2. Encryption

Encryption is both a technology that protects legitimate interests and one that is open to abuse by malicious actors. There is a constant struggle to strike a balance when regulating this technology, as policy responses can also be double edged swords.

Europol has confirmed the upward trend in cybercrime sparked by covid-19.[8] So did the UN Office on Drugs and Crime (UNODC) when it issued guidance on how to stay safe from cyber criminals' attacks using encryption in ransomware.[9] The key finding from Europol's Internet Organised Crime Threat Assessment 2020 states that despite cybercrime remaining largely the same as before the pandemic, the narrative changed. Ransomware is recognised as a top priority threat in this report by the majority of law enforcement respondents. Encryption is used to hide the identity of criminals behind these cyber-crimes, complicating law enforcement's ability to gather data.

There is an urgency to react with policies to limit the protection offered by encryption to criminals, without compromising protection offered to citizens. This is recognised in the Council of the EU's Resolution on Encryption, which outlines the need for an effective regulatory framework to tackle the unintended effects of encryption.[10]

However, law-abiding citizens also value the protection offered by encryption to safeguard privacy in their daily lives.

On the criminal side, an event in 2013 provided motivation for those conducting illicit activities online to seek stronger encryption. That year, Ross Ulbricht, the creator and operator of Silk Road, a dark web drug market, was captured by US authorities and charged with various crimes related to drug trafficking, as well as money laundering. Silk Road sold itself as a marketplace by claiming its users would be hidden behind a wall of heavy encryption that law enforcement would not be able to penetrate. That turned out not to be the case, and as a result, according to research by IntSights, a cyber security firm, more of the dark web is moving to mobile messaging apps—WhatsApp, Discord, Telegram, Skype and ICQ—under the assumption they provide stronger encryption and therefore more protection.[11] The types of criminal and cross-border illicit trade activities IntSights uncovered ranged from hacking services and fake bills, to stolen credit cards and counterfeit and IP-infringing goods.

This tension created by technology that protects the privacy of both law-abiding citizens and illicit traders and other criminals ultimately leads to the philosophical question of "What does society want?" says a senior official in an international law enforcement organisation. "What is acceptable to society in the space of encryption? There's a right to privacy, but then people also have the right to life, as well. People have the right to have crime prevented and serious organised crime prevented." The official acknowledged that while having access to data and information is advantageous or beneficial for law enforcement in the pursuit of criminals, that access should also come with checks and balances.

8 *COVID-19 sparks upward trend in cybercrime.* Europol. 5 October 2020. Available online at https://www.europol.europa.eu/newsroom/news/covid-19-sparks-upward-trend-in-cybercrime
9 *COVID-19: How to stay safe from cybercriminals exploiting the pandemic.* UNODC. Accessed on 19 February 2021. Available online at https://www.unodc.org/middleeastandnorthafrica/en/web-stories/covid-19_-how-to-stay-safe-from-cybercriminals-exploiting-the-pandemic.html
10 *Chief Economist Note:* Trade policy reflections beyond the COVID-19 outbreak. European Commission. June 2020. Available online at https://trade.ec.europa.eu/doclib/docs/2020/july/tradoc_158859.07.01%20Chief%20Economist%20Note%202%202020%20Final.pdf
11 *Messaging Applications:* The New Dark Web. INTSIGHTS. Available online at https://wow.intsights.com/rs/071-ZWD-900/images/Messaging%20Applications%20The%20New%20Dark%20Web.pdf

Encryption has continued to enable crime through the pandemic. The NCA reported, for example, that 100% of its investigations encounter some form of encryption.[12] The pandemic elevated the importance of encryption to criminal networks just as it did for legitimate players, as societies become increasingly more active in the virtual world. The remote working trend has forced the financial sector to adapt quickly to technology changes, such as investing in encryption and digital identity verification.[13]

In 2020, the dismantling of EncroChat, a secured communication tool regularly appearing in operations against organised crime groups, offered a glimpse into the extent to which criminal organisations rely on encrypted networks for conducting a wide range of activities, including illicit trade.[14]

Many organisations are not going back to a world of 40 hours a week in an office, and that means there is a permanent step change in the proportion of work that gets done remotely – and therefore relies on remote network security including encryption.

So far, however, the owners of the messaging apps—along with the broader mobile and app industry—have mostly resisted government petitions for access to encrypted customer data. They've done so on the grounds that doing so will result in getting onto a slippery slope of eroding privacy. The most high profile case on this issue in recent years was when the FBI, as part of an investigation into a 2015 mass shooting in California, requested Apple turn over a "master key" that would have allowed it to unlock any Apple product. Apple's CEO Tim Cook refused; in a statement from the company, it claimed that "users' privacy was more important than anything else."[15]

More recently, the pandemic put the value of privacy to the test as contact tracing became prevalent. Concerns are raised about creating potential risks of surveillance in the name of public health,[16] and they should not be dismissed. However, encryption can address the legitimate concerns users have about their data. For contact tracing apps to work across the EU, personal data is protected as information exchanged is fully anonymised and encrypted.[17]

The policy responses to manage the tension between privacy and health will likely have wider repercussions in other areas such as crime management in the future.

In October 2019, the United States and United Kingdom signed an agreement to access data from internet and mobile companies, but companies which encrypt their users' data are still refusing to provide encryption keys or other means to access that data. The issue is likely to remain unresolved for years to come.

12 *National Strategic Assessment of Serious and Organised Crime.* National Crime Agency. 2020. Available online at https://www.nationalcrimeagency.gov.uk/who-we-are/publications/437-national-strategic-assessment-of-serious-and-organised-crime-2020/file

13 *Banks determined to lock in coronavirus technology changes.* Financial Times. 28 May 2020. Available online at https://www.ft.com/content/3f23d208-904b-11ea-bc44-dbf6756c871a

14 *Dismantling of An Encrypted Network Sends Shockwaves Through Organised Crime Groups Across Europe.* Europol. 2 July 2020. Available online at https://www.europol.europa.eu/newsroom/news/dismantling-of-encrypted-network-sends-shockwaves-through-organised-crime-groups-across-europe

15 *Encryption: A Godsend to All Who Seek Privacy, Even Criminals.* Organized Crime and Corruption Reporting Project. 31 October 2018. Available online at https://www.occrp.org/en/61-ccblog/8822-encryption-a-godsend-to-all-who-seek-privacy-even-criminals

16 *Escaping the lockdown: Don't rely on contact-tracing apps.* The Economist. 16 May 2020. Available online at https://www.economist.com/leaders/2020/05/16/dont-rely-on-contact-tracing-apps

17 *How tracing and warning apps can help during the pandemic.* European Commission. Accessed on 19 February 2021. Available online at https://ec.europa.eu/info/live-work-travel-eu/coronavirus-response/travel-during-coronavirus-pandemic/how-tracing-and-warning-apps-can-help-during-pandemic_en

3. Blockchain

Despite its libertarian origins, blockchain may emerge as a leading enforcement technology for combating illicit trade. As of March 2019, the OECD and EU Intellectual Property Office estimate that trade in fake goods constitutes 3.3% of global trade.[18] The trend is broadly increasing, for goods as diverse as ineffective prescription drugs and PPE, unsafe dental filling materials, defective electronic products, and sub-standard chemicals in cosmetics and baby formula. Blockchain could provide a remedy. Distributed ledgers can enhance authenticity through a verifiable digital footprint for barcodes, serial numbers or cryptographic seals.[19] Any product on the blockchain has an identity that can be updated at every stage of the supply chain – from the production plant through distribution chains to the end user. When products go missing, governments and industry can cooperate to identify the most recent entity on the ledger and investigate the cause of the problem. In theory, blockchain registration could apply to any traded product. Even individual components can be registered on blockchain, improving efficiency and transactional trust in global resale markets such as the one for commercial aircraft parts.[20]

The pandemic exposed the weaknesses in supply chains, such as overreliance on paper documents, that can be strengthened by blockchain. While blockchain deployments have been largely put on the backburner, one area that is accelerating digital transformation plans is in supply chains.[21] More recently, a study prepared for the European Parliament reports on the key features, impacts and policy options relating to blockchain for supply chains and international trade, and discusses various ways in which blockchain can facilitate trade.[22] It warns of dangers that the technology could be used to facilitate illicit trade or trade-based money laundering unless tracking of payments is made possible. Despite early prophesies that blockchain-backed cryptocurrencies would proliferate as a domain of criminality, decentralised ledgers have the potential to drastically reduce money laundering.

Blockchain is not a trading technology of the future. As of the end of 2020, Japan was preparing for digital currency issuance thanks to the technological advancements including blockchain.[23] Companies have already started moving authentication platforms onto the blockchain. TradeLens, a joint initiative led by Maersk and IBM, is an active distributed ledger that shares trade data with shipping companies, ports, and customs officials with the goal of improving efficiency and transparency in international trade.[24] The platform has grown to include over 100 participants and process thousands of documents each week.[25]

18 *Trade in fake goods is now 3.3% of world trade and rising.* OECD. 18 March 2019. Available online at https://www.oecd.org/newsroom/trade-in-fake-goods-is-now-33-of-world-trade-and-rising.htm
19 *Combating Illicit Markets With Blockchain: Smart Supply Chains Solutions.* Forbes. 3 July 2018. Available online at https://www.forbes.com/sites/samantharadocchia/2018/07/03/combating-illicit-markets-with-blockchain-smart-supply-chains-solutions/#7af649531e1d
20 *Transforming Illicit Trade Blockchain for Manufacturing.* Fujitsu. 22 February 2019. Available online at https://blog.global.fujitsu.com/fgb/2019-02-22/transforming-illicit-trade-blockchain-for-manufacturing/
21 *Into the New World: The Covid-19 Pandemic's Impact on Innovation.* The Economist Intelligence Unit. 27 November 2020. Available online at https://eiuperspectives.economist.com/technology-innovation/new-world-covid-19-pandemics-impact-innovation
22 *Blockchain for supply chains and international trade.* European Parliament. May 2020. Available online at https://www.europarl.europa.eu/RegData/etudes/STUD/2020/641544/EPRS_STU(2020)641544_EN.pdf
23 *Japan prepares for digital currency, in line with China and others.* The Japan Times. 24 December 2020. Available online at https://www.japantimes.co.jp/news/2020/12/24/business/economy-business/japan-digital-currency/
24 *TradeLens.* [https://www.tradelens.com/solution/]. Accessed January 16, 2020.
25 *Oman's Largest Port Joins Blockchain Shipping Platform TradeLens.* Coindesk. 8 January 2020. Available online at https://www.coindesk.com/omans-largest-port-joins-blockchain-shipping-platform-tradelens

According to Mike White, CEO of Maersk GTD and Maersk's point person for TradeLens, confidence in blockchain translates to greater trust for all market participants. "It provides the confidence that the data they are looking at is immutable… that helps supply chain participants when they are sharing data across this platform." However, Mr White notes that blockchain remains a nascent technology for trade enforcement. "Blockchain can be part of a layered approach to improve the enforcement – and not only the enforcement, but also the efficiency and effectiveness of transmitting sensitive information across jurisdictions," he says, "but I think it's a multi-year journey."

Sceptics point to blockchain's potential for exploitation among criminals, given the anonymity inherent to the technology. A 2018 research paper estimated that roughly one quarter of users of bitcoin, a cryptocurrency, were engaged in illegal activity, comprising nearly half of all bitcoin transactions.[26] However, the same paper found a steady downward trend in illegal activity since 2015.

A July 2019 report from Chainalysis, a provider of blockchain anti-money laundering and Know Your Customer solutions, found that over $500m worth of bitcoin had gone into illegal marketplaces on the dark web.[27] There is also evidence of cryptocurrency enabling the illicit arms trade – roughly $80,000 worth of illicit arms trade on the dark web every month.[28] Guns may make up a tiny fraction of cryptocurrency-enabled trades on the dark web, but the implications of such transactions are chilling.

> **Blockchain can be part of a layered approach to improve the enforcement—and not only the enforcement, but also the efficiency and effectiveness of transmitting sensitive information across jurisdictions, but I think it's a multi-year journey.**
>
> *Mike White, CEO of Maersk GTD*

Despite these examples, there is evidence that blockchain is less the asset of criminals than it was initially made out to be. A study from blockchain analysis firm Elliptic and MIT found that just 2% of bitcoin transactions in 2019 could be categorised as illicit.[29]

A more recent global survey on cryptocurrency conducted in 2020 by the Royal United Services Institute and the Association of Certified Anti-Money Laundering Specialists found that respondents predict a decrease in cryptocurrency use for illicit activities.[30] While the exact reason for this optimism was not stated, advancements in blockchain may be the answer.

26 *Sex, drugs, and bitcoin: How much illegal activity is financed through cryptocurrencies?* University of Oxford Faculty of Law. 19 February 2018. Available online at https://www.law.ox.ac.uk/business-law-blog/blog/2018/02/sex-drugs-and-bitcoin-how-much-illegal-activity-financed-through

27 *Bitcoin Criminals Set to Spend $1 Billion on Dark Web This Year.* Bloomberg. 2 July 2019. Available online at https://www.bloomberg.com/news/articles/2019-07-01/bitcoin-criminals-set-to-spend-1-billion-on-dark-web-this-year

28 *International arms trade on the dark web.* RAND Corporation. Accessed on 19 February 2021. Available online at https://www.rand.org/randeurope/research/projects/international-arms-trade-on-the-hidden-web.html

29 *Is Bitcoin a Haven for Financial Crimes? New MIT Study Finds Surprising Answer.* Observer. 5 August 2019. Available online at https://observer.com/2019/08/bitcoin-use-illegal-finance-mit-study-blockchain-ai/

30 *Cryptocurrency Risk & Compliance Survey.* RUSI and ACAMS. 2020. Available online at https://www.acams.org/en/ACAMS-RUSI-Crypto-Survey-Report

4. 3D printing

Advances in 3D printing have made the technology increasingly viable on a commercial scale. The direct role 3D printing had in meeting shortages of PPE near the start of the covid-19 crisis has been well reported.[31] Nevertheless, as with blockchain and encryption, much has been made of the criminal potential of 3D printing. Conventional wisdom says 3D printing is a problem for law enforcement to manage, rather than a tool to be leveraged. In its July 2019 "Study report on Disruptive Technologies", the World Customs Organization went as far as to begin a section on 3D printing with a statement that the technology has "no evident benefit of use by Customs".[32]

Advances in 3D printing have made the technology increasingly viable on a commercial scale.

Their pessimism could be forgiven. Dire predictions abound, such as "How 3D printing will revolutionise crime."[33] Intellectual property law is probably sufficient to handle violations stemming from 3D printing, but enforcement needs an overhaul. Customs authorities never see 3D-printed products, with blueprints being sent over the internet. Regulation moves squarely into the digital space rather than at physical points of transit. Another major concern is firearms. Weapons smuggling is an ancient part of illicit trade, and 3D printing presents a new risk in the digital age. While much has been made of the threat from printing firearms from scratch, there is a similarly nefarious risk of converting replica guns into fully functional weapons by printing just a few missing requisite components.[34] Even more concerning is the evidence of a decentralised online movement actively *promoting* the proliferation of illicit, 3D-printed guns, by sharing blueprints and encouraging production.[35]

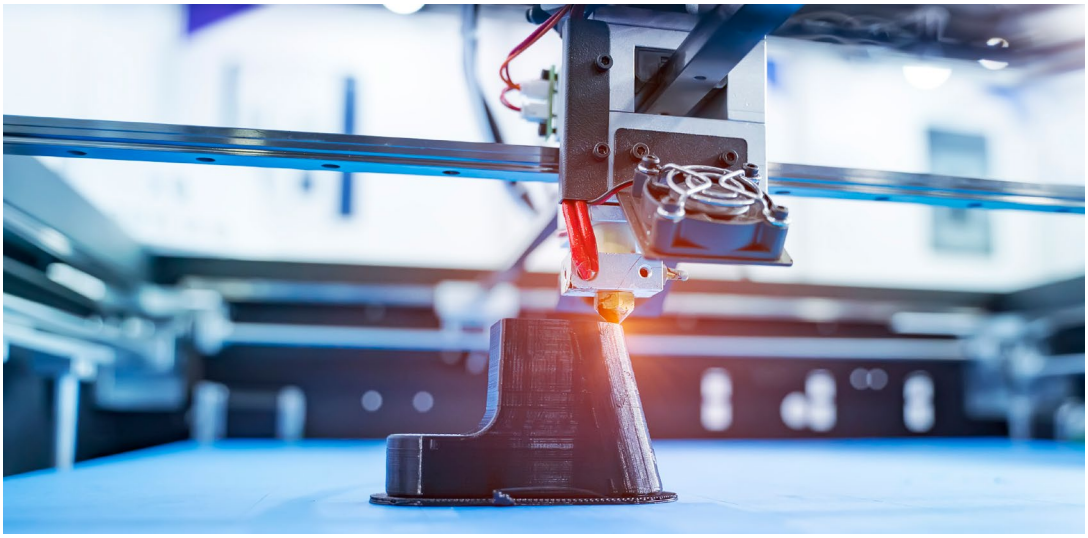
The subversive impact of 3D printing could require an evolution in customs administration. Raw materials could make up a growing share of international trade as manufacturing supply chains contract in the direction of the end user. The European Commission's trade policy outlook beyond the covid-19 outbreak finds several ways in which 3D printing will affect the prioritisation and method of implementation. Intellectual property rights, trade in services and data transfer are all areas 3D printing is likely to disrupt. Adequate regulatory frameworks to manage these areas of concern are crucial to keep 3D printing away from illicit activities.[36]

According to Shao Weijian, customs secretary for China's mission to the EU, customs' role will

31 *Coronavirus: Can we 3D-print our way out of the PPE shortage?* BBC News. 9 April 2020. Available online at https://www.bbc.co.uk/news/health-52201696
32 *Study report on Disruptive Technologies.* World Customs Organization. June 2019. Available online at http://www.wcoomd.org/en/topics/facilitation/instrument-and-tools/tools/disruptive-technologies.aspx
33 *Vice Wars: How 3-D Printing Will Revolutionize Crime.* Forbes. 31 July 2012. Available online at https://www.forbes.com/sites/stevenkotler/2012/07/31/the-democratization-of-vice-the-impact-of-exponential-technology-on-illicit-trades-and-organized-crime/#31972e7c1732
34 *International arms trade on the dark web.* Rand Corporation. Accessed on 19 February 2021. Available online at https://www.rand.org/randeurope/research/projects/international-arms-trade-on-the-hidden-web.html
35 *3D-printed guns are back, and this time they are unstoppable.* Wired. 20 May 2019. Available online at https://www.wired.co.uk/article/3d-printed-guns-blueprints
36 *Chief Economist Note: Trade policy reflections beyond the COVID-19 outbreak.* European Commission. June 2020. Available online at https://trade.ec.europa.eu/doclib/docs/2020/july/tradoc_158859.07.01%20Chief%20Economist%20Note%202%202020%20Final.pdf

have to transform from duty collection to social protection, with an emphasis on intellectual property rights, public safety and security.[37] In a world where 3D printing dominates manufacturing, the protection of people and their ideas is vastly more important than the collection of import tariffs at the border. There have been success stories that might provide a template for action, such as the decline in the illicit music trade following the spread online streaming platforms.[38]

However, new discoveries indicate that 3D printing could eventually become a greater tool for law enforcement than for criminals. In October 2018, researchers from the University of Buffalo announced they had developed a 3D printer identification system called PrinTracker, that effectively scans a product's unique fingerprint. PrinTracker compares the "intrinsic connection between the 3D printer hardware imperfections and the textures on the associated printed product", claiming a successful identification rate of 92%.[39] A system to identify hardware-based fingerprints would enable law enforcement, retailers and even end users to validate the authenticity of goods with confidence. While fingerprinting remains in its infancy, customs authorities have already put 3D printing to work in other ways. For example, the Hong Kong Customs and Excise Department has used 3D printing to manufacture exact replicas of genuine products to compare against potential counterfeits.[40] These steps represent good value for law enforcement in the fight against illicit trade.



37 *Influence of 3D Printing to the Future of Customs.* World Customs Organization. Available online at http://www.wcoomd.org/-/media/wco/public/global/pdf/topics/facilitation/ressources/permanent-technical-committee/209-210/items/pc_itemii_b_influence-of-3d-printing_china_en_only.pdf?la=en

38 *3D printing and IP law. WIPO Magazine.* February 2017. Available online at https://www.wipo.int/wipo_magazine/en/2017/01/article_0006.html

39 *PrinTracker: Fingerprinting 3D Printers using Commodity Scanners.* Presentation at 2018 ACM SIGSAC Conference on Computer and Communications, October 15-19, 2018. Available online at https://cse.buffalo.edu/~wenyaoxu/papers/conference/xu-ccs2018.pdf

40 *The Global Illicit Trade Environment Index - Asia.* The Economist Intelligence Unit. June 2018. Available online at http://illicittradeindex.eiu.com/documents/EIU%20Global%20Illicit%20Trade%20Environment%20Index%202018%20-%20Asia%20June%206%20FINAL.pdf

Concluding remarks

What will it take for citizens, the private sector and governments to find common ground on the issue of encryption and data privacy? Is there even common ground to be found? Will the potential good of blockchain outweigh the bad as it continues to scale? Is there a way to prevent the use of cryptocurrency by criminals without undermining its founding principles? Can the 3D printing of weapons be curtailed and if so, how?

These are just some of the questions raised by these technologies, each of which comes with unintended consequences and unexpected benefits with regards to crime and illicit trade. Positive outcomes will depend on a number of factors, of which trust would appear to be the most important. Without trust, meaningful cooperation between governments and the private sector, or between law enforcement and citizens, will never materialise.

Unfortunately, general levels of trust, while slightly improved as of the beginning of 2020, are still short where they need to be for this to happen.[41] The full impact on the level of trust in governments based on how they handle the tension between privacy and public health in light of the covid-19 crisis will emerge over time. This may foreshadow how well other tensions discussed in this paper are resolved in the future.

Positive outcomes will depend on a number of factors. Trust would appear to be at the core, however. Without trust, meaningful cooperation between governments and the private sector, for example, or between law enforcement and citizens, will never materialise.

41 *Edelman Trust Barometer 2020. Edelman. 2020.* Available online at https://cdn2.hubspot.net/hubfs/440941/Trust%20Barometer%202020/2020%20Edelman%20Trust%20Barometer%20Global%20Report.pdf?utm_campaign=Global:%20Trust%20Barometer%202020&utm_source=Website

The Economist INTELLIGENCE UNIT

LONDON

20 Cabot Square
London, E14 4QW
United Kingdom
Tel: (44.20) 7576 8000
Fax: (44.20) 7576 8500
Email: london@eiu.com

GENEVA

Rue de l'Athénée 32
1206 Geneva
Switzerland
Tel: (41) 22 566 2470
Fax: (41) 22 346 93 47
Email: geneva@eiu.com

NEW YORK

750 Third Avenue
5th Floor
New York, NY 10017
United States
Tel: (1.212) 554 0600
Fax: (1.212) 586 1181/2
Email: americas@eiu.com

DUBAI

Office 1301a
Aurora Tower
Dubai Media City
Dubai
Tel: (971) 4 433 4202
Fax: (971) 4 438 0224
Email: dubai@eiu.com

HONG KONG

1301
12 Taikoo Wan Road
Taikoo Shing
Hong Kong
Tel: (852) 2585 3888
Fax: (852) 2802 7638
Email: asia@eiu.com

SINGAPORE

8 Cross Street
#23-01 Manulife Tower
Singapore
048424
Tel: (65) 6534 5177
Fax: (65) 6534 5077
Email: asia@eiu.com