**The war in Ukraine: Why knowing the country of origin of tech components is vital**

Is it possible to repurpose the Country of Origin (COO) concept to address cybersecurity risks in digital products?

(Online version published April 16 2023: <https://theacademic.com/why-knowing-the-country-of-origin-of-tech-components-is-vital/>)

Serkan Ozdemira

a Management Information Systems Department, Bogazici University, Istanbul, Turkey

Email: serkano@metu.edu.tr

Martin Wynnb\*

bSchool of Computing and Engineering, University of Gloucestershire, Cheltenham, UK.

Email: [MWynn@glos.ac.uk](mailto:MWynn@glos.ac.uk)

Bilgin Metina

a Management Information Systems Department, Bogazici University, Istanbul, Turkey

Email: bilgin.metin@boun.edu.tr

# The war in Ukraine has highlighted the significance of knowing the Country of Origin (COO) of technology product components. A single [Iranian drone](https://edition.cnn.com/2023/01/04/politics/iranian-drone-parts-13-us-companies-ukraine-russia/index.html) was found to contain parts made by more than a dozen US and western companies, and digital products can contain hardware components, software elements, and embedded systems and data from a range of countries and computing environments. How can this conundrum best be addressed to support national security? How can the end-consumer be better informed about the origin of digital products he/she is buying? And what are the implications for sustainability and the recyclability of these products?

# Digital products and cybersecurity risk

Even before the Russian invasion of Ukraine, the director of the UK National Cyber Security Centre, [Ciaran Martin](https://www.reuters.com/article/us-kaspersky-cyber-britain/uk-cyber-agency-targets-kaspersky-in-warning-on-russian-%20software-idUSKBN1DV63S), was warning “Russian-made anti-virus software should not be used in systems containing information that would harm national security if it was accessed by the Russian government”. This reference to the Kaspersky anti-virus software product - that was readily available and deployed in the West - highlighted the risks posed by such products when their true origin, purpose and function are unclear. In similar vein, Google decided to withdraw the [licence for the use of the Android mobile operating system](https://indianexpress.com/article/technology/mobile-tabs/google-cancels-android-license-for-huawei-play-store-on-huawei-future-updates-questions-5736694/#:~:text=In%20a%20major%20blow%20to,future%20updates%20to%20Huawei%20phones) in Huawei products, because of the potential threat of information leakage to the Chinese government. And just this month, the US government was moving to ban Chinese social media product TikTok, with the Republican committee chair, Michael McCaul, describing the product as a [“spy balloon in your phone”](https://www.theguardian.com/technology/2023/mar/01/house-committee-advances-legislation-ban-tiktok). Unless every component of a digital product can be identified, and their origin and purpose verified, the product as a whole may constitute a cybersecurity risk.

# Repurposing the COO concept

[Recent research](https://www.mdpi.com/2071-1050/15/1/87) in Turkey has highlighted how the COO concept could be redefined and repurposed to provide a framework that might contribute to addressing such cybersecurity risks. Through a series of workshops and face-to-face interviews with public officials and private sector professionals working on digital products, an initial list of 37 parameters pertaining to digital products was identified. Through further discussion and review with the interviewees, and an online survey of the views of professionals from a range of public sector departments involved in digital projects, the parameters were refined and reduced in number to a final list of 18, classified into the four main categories or “influences” – hardware, software, platforms deployed, and producer of the final product (Table 1).

|  |  |  |  |
| --- | --- | --- | --- |
| **Category/**  **Influence** | **Parameter** | **Definition** | **Significance** |
| **Hardware** | Hardware Production Place | Measures the percentage of hardware elements within a product produced in any one country. For example, 60% in USA; 40% in Turkey. | Indicates the amount of direct investment in a country and thus the domesticity of the product. |
|  | Hardware Assembly Place | Measures where the hardware elements of a product were assembled. For example, 15% in USA; 85% in Turkey. | Indicates investment in assembly factories and workshops in any one country and thus domesticity. |
|  | Content Rate of Component Parts (Raw Materials and Spare Parts Origin) | Provides the content rate for component parts and spare parts origin deployed in hardware manufacture and maintenance. For example, 70% from USA; 15% from China; 15% from Turkey. | The provision of component parts and spare parts from within the user country reduces the import dependency and on-going cost. |
| **Software** | Software Production Place | Measures the percentage of software elements within a product developed or produced in any one country. Must consider if outsourced. | Provides an indication of domesticity of the product. |
|  | Capability of On-going Software Development and Maintenance | Measures country capability for software development and maintenance using country-based personnel. | Capability to manage software updates and on-going maintenance increases the domesticity rating. |
|  | Compliance with International Standards | Assesses compliance with international standards and thus eligibility for subsequent foreign export. | Meeting necessary international compliance standards establishes the software competence and indicates potential security, privacy, and quality issues. |
|  | Open Source Code Ratio | Measures ratio of software that is developed in open source environment | Using open source code makes it easier to solve problems rather than rely on proprietary products. |
|  | Software Producer Headquarter Location | Measures software producer’s domesticity ratio, including for outsourced products | Inbound headquarter location for suppliers has a positive impact on domesticity |
| **Platforms Deployed** | Software Development Platform Location | Denotes location of platform upon which software deployed.  May be in the Cloud via SaaS | Supplying software development platforms with domestic resources reduces foreign dependency and increases domesticity |
|  | Data Storage Location | Measures domesticity rate based on location for data storage. Maybe in the Cloud via IaaS, PaaS or SaaS. | Storing data inside the country reduces the risk of data breach and increases the country’s information security, improving data confidentiality, integrity, and availability. |
|  | Open Source Database Availability | Measures the level of database usage with open source resources | Open source database prevents data breach possibility and increases domesticity |
|  | Communication Infrastructure Origin | Measures the domesticity level of communication infrastructure (e.g. Base station) | Supplying communication infrastructure and necessary data transfer technology inside the country increases data privacy and national data security |
|  | Open Platform Ratio | Measures the ratio of software developed in an open platform environment | An open platform will use open standards and documented APIs, and is likely to reduce dependencies between development teams and certain application components. |
| **Producer of the Final Product** | Headquarter Location of Manufacturer of Final Product | Measures domesticity in terms of headquarter location | Inbound headquarter location for the producer has a positive impact on domesticity |
|  | Domestic Capital Rate | Measures domesticity of capital used to finance the producer company. | Financing the producer capital with domestic investors should increase the domesticity |
|  | Tax Payment to Domestic Country | Measures domesticity in terms of tax payment to domestic country | Paying taxes to the country it operates should increase the domesticity |
|  | Investment Revenue Costs in Domestic Country | Measures all investment costs in domestic country, including R&D. | Spending more in the country should increase the domesticity |
|  | Employment Contribution | Measures employment contribution level in the country | Contributing to the labour force it operates means selecting domestic labour and should increase the domesticity |

Table 1. Final parameter list for digital product COO evaluation

A key point is that some products, which may appear to be made in a domestic country, are in fact not made there in large part, and this is not reflected in the current COO assessment. Today, the most commonly used parameters for COO determination are, in general terms, production place, headquarter location and domestic capital deployment. This is replicated in many of the COO regulations used in different countries to assess tariff calculations rather than to determine the true domesticity of products. This means the “Made in…” labelling may be at best misleading, and at worst plain wrong.

**The Xiaomi smartphone example**

In Turkey, there are three main parameters used for assessing digital product domesticity - production place, content rate and certification of the manufacturer in the Turkish industrial registry. If a product satisfies two of these three conditions, it is classified as a Turkish product. As an illustration, Xiaomi Corporation, a Chinese designer and manufacturer of consumer electronics and related software, has [a factory in Turkey](https://www.aa.com.tr/en/economy/chinese-tech-giant-xiaomi-opens-factory-in-turkey/2191361) employing 2000 staff producing smartphones – the production place of the smartphone is thus Turkey. Content rate is considered a negative since all of the component parts are imported via Xiaomi’s international subsidiaries. But Xiaomi has an industry registry certificate, which was granted to allow company legal transactions in Turkey. It is thus considered a [Turkish product](https://www.dailysabah.com/business/tech/made-in-turkey-xiaomi-phones-to-go-on-sale-in-april), as it appears to meet two of the three criteria.

|  |  |  |
| --- | --- | --- |
| **Category/Influence** | **Parameter** | **Domesticity Assessment** |
| **Hardware** | Hardware Production Place | No |
|  | Hardware Assembly Place | Yes |
|  | Content rate of component parts (raw materials) and spare parts origin | No < 50% |
| **Software** | Software Production Place | No |
|  | Capability of on-going software development and maintenance | No |
|  | Compliance with International Standards | Yes. It is allowed to export the product to other countries |
|  | Open Source Code Ratio | No. < 50%. The operating system is Android which is open source but the other software products are produced by Xiaomi itself. |
|  | Software Producer Headquarter Location | Not in Turkey |
| **Platforms Deployed** | Software Development Platform Location | Not in Turkey |
|  | Data Storage Location | Not in Turkey |
|  | Open source database availability | No |
|  | Communication Infrastructure Origin | Not in Turkey |
|  | Open Platform Ratio | Low |
| **Producer of the Final Product** | Headquarter location of manufacturer of final product | Not in Turkey |
|  | Domestic capital rate | 0%. Total Chinese investment |
|  | Tax payment to domestic country | Yes. Corporate tax, value-added-tax, income tax. However, the amount is not explicitly given |
|  | Investment rate in domestic country | Yes. Building and factory. $30 million |
|  | Employment Contribution | Yes. 2000 personnel |

Table 2. COO Evaluation of Xiaomi mobile phone using proposed parameter list

However, an assessment of the same smartphone using the proposed COO parameters would show the majority of parameters are negative (Table 2), which would almost certainly preclude a “Made in Turkey” labelling. The use of such a scale for COO assessment could lessen import dependency. At the same time, governments could introduce subsidies and incentives for domestic companies to develop products with a certain threshold of domesticity in order to compete with global technology manufacturers.

# Security and sustainability aspects

A repurposed COO assessment would allow greater scrutiny of security aspects alluded to above. If the storage of data produced from an imported product is managed in the cloud via an unvetted third-party, there is an obvious risk that the data may be leaked or hacked. If the COO assessment confirms this to be the case, then organizations and governments who wish to safely store strategic data would clearly be reluctant to use such products. Data related security considerations may affect a product's value and potential use, given the spiralling costs of [data security breaches](https://digitalguardian.com/blog/whats-cost-data-breach-2019). The COO parameters put forward here allow a fuller assessment of related data security issues.

There are also implications for the sustainability of the digital supply chain and the wider circular economy. Clarifying the origin and make-up of different digital technology components can facilitate an assessment of their sustainability and recyclability. [Reuter](https://link.springer.com/article/10.1007/s11663-016-0735-5) noted that “metallurgy is a key enabler of a circular economy; its digitalization is the metallurgical Internet of Things. In short: metallurgy is at the heart of a circular economy, as metals all have strong intrinsic recycling potentials”. This demands consideration of a wide range of measures and systems to assess the resource efficiency and reusability of digital product parts. This, in turn, requires clarity on the origin of the component parts and software elements contained in digital products, and an accurate and realistic COO assessment would be a step towards this end.

# Conclusion

# A new and more realistic COO assessment could provide the basis for implementing policies aimed at excluding, or imposing higher levies on, non-domestic digital products, whilst at the same time supporting the development of home-grown technology companies. At the same time, digital products from companies or countries considered a threat to security could be more effectively screened through such a revised set of COO parameters. Further research could refine and adapt the parameters put forward here, and additional criteria and formulas should be tried, not least in the identification of recyclable or non-recyclable materials. Linkages to other research, notably that regarding assessment of [circular economy product assessment](https://ellenmacarthurfoundation.org/material-circularity-indicator), could be explored to combine security and sustainability concerns in a revamped COO assessment of digital products.

**Reference**

Ozdemir, S., Wynn, M., and Metin, B. (2023) Cybersecurity and Country of Origin: Towards a New Framework for Assessing Digital Product Domesticity. *Sustainability*, *15*(1). Art 87. doi:10.3390/su15010087

**Serkan Ozdemir** is Research Assistant in the Information Systems Department in the Institute of Informatics at the Middle East Technical University, Ankara, Turkey. He attained his Master’s degree from Bogazici University, Istanbul, Turkey. His current PhD studies focus on time series prediction with artificial intelligence models.

ORCID: <https://orcid.org/0000-0002-8635-3311>

LINKED IN: <https://www.linkedin.com/in/serkan-%C3%B6zdemir-30938b13a>

SCOPUS: <https://www.scopus.com/authid/detail.uri?authorId=57208127727>



**Martin Wynn** is Associate Professor in Information Technology in the School of Computing and Engineering at the University of Gloucestershire. Having gained his PhD at Nottingham Trent University, he was appointed Research Fellow at East London University, and then spent 20 years in industry at Glaxo Pharmaceuticals and HP Bulmer Drinks, now part of Heineken UK, before returning to academia in 2002. His research interests include digitalisation, information systems, sustainability, project management and urban planning. His latest book, *Handbook of Research on Digital Transformation, Industry Use Cases, and the Impact of Disruptive Technologies,* was published in 2022. (<https://www.igi-global.com/book/handbook-research-digital-transformation-industry/265448>).

ORCID: <https://orcid.org/my-orcid?orcid=0000-0001-7619-6079>

LINKED IN: <https://www.linkedin.com/in/martin-wynn-79296a2/?originalSubdomain=uk>

SCOPUS: <https://www.scopus.com/authid/detail.uri?authorId=7005117935>



Dr Martin Wynn

**Bilgin Metin** is head of the Management Information Systems Department, and of the Cybersecurity Centre at Bogazici University. After receiving his Ph.D. degree at Bogazici University in 2007, he was appointed assistant professor in the Management Information Systems Department at the university, becoming Associate Professor in 2014 and Professor in 2021. His multi-disciplinary research interests include cybersecurity, information technology and privacy governance, and electronic design for information and communication systems. He has more than 100 publications in international journals and conferences. He holds OSCP (Offensive Security Certified Security Professional), CISA (Certified Information Systems Auditor), CDPSE (Certified Data Privacy Solution Engineer), and ISO 27001 Lead Auditor qualifications.

ORCID: https://orcid.org/0000-0002-5828-9770

LINKED IN: https://www.linkedin.com/in/bilginmetin

SCOPUS: https://www.scopus.com/authid/detail.uri?authorId=6507573592



Prof. Bilgin Metin