The GDPR and DMA Mitigating Vulnerabilities to Weaponized Interdependence in the EU

James Tamim

European Digital Policy Institute

May 3, 2024

Abstract

This paper critically assesses the European Union's vulnerability to weaponized interdependence in the digital sector. The concepts of the "panopticon effect" and "chokepoint effect" from Farrell and Newman's theory of weaponized interdependence are used as criteria to evaluate the EU's lack of autonomy and risk exposure. Key cases like the Snowden revelations and the dominance of US and Chinese tech platforms are analysed. The research finds that the EU is highly vulnerable to the panopticon effect, as evidenced by foreign mass surveillance of EU data with little prospect for improvement despite measures like the GDPR. However, the EU is not significantly vulnerable to the chokepoint effect. This is because no single state currently meets the criteria of having both critical platform dominance in the EU market and strained diplomatic relations that could precipitate a chokepoint scenario. The EU is also taking proactive steps like the Digital Markets Act which will further insulate itself from potential chokepoint vulnerabilities going forward. The paper concludes that EU vulnerability to weaponized interdependence in the digital sector is currently asymmetric, being high for the panopticon effect but low for the chokepoint effect.

Table of Contents

ABSTRACT **2**

INTRODUCTION **4**

DEFINING WEAPONISED INTERDEPENDENCE **5**

THE PANOPTICON EFFECT 6

USING THE PANOPTICON EFFECT TO CRITICALLY ASSESS THE EU'S VULNERABILITY 7

THE CHOKEPOINT EFFECT 7

MASS SURVEILLANCE FROM FOREIGN ACTORS OVER EU DATA **9**

THE SNOWDEN REVELATIONS 9

THE GDPR MITIGATING THE PANOPTICON EFFECT? 10

SURVEILLANCE FROM CHINA 11

IS THE EU VULNERABLE TO THE PANOPTICON EFFECT? 12

DEPENDENCE ON NON-EU PLATFORMS **12**

THE DOMINANCE OF PLATFORMS BASED IN THIRD COUNTRIES 12

IS THE EU VULNERABLE TO THE CHOKEPOINT EFFECT? 13

CONCLUSION **14**

BIBLIOGRAPHY **16**

The GDPR and DMA Mitigating Vulnerabilities to

Weaponized Interdependence in the EU

I will critically assess in what ways the EU is vulnerable to weaponized interdependence in the digital sector. The sector I focus on is highly relevant to weaponised interdependence as it is particularly decentralised on the international stage in part due to its novelty and complexity. I have chosen to limit my research to one specific sector in order to privilege depth of analysis over breadth. Fundamentally, my research critically assesses the lack of autonomy the EU has in the tech sector and the risk this poses while addressing the EU's actions to limit these vulnerabilities. I will first define the concept of weaponised interdependence focusing on the aspects most relevant to my sector of focus. I will then explore its two major effects: the Panopticon Effect and the Chokepoint Effect. Beyond defining key terms, the first sections will also introduce my method by outlining how I will utilise these concepts to assess the EU's vulnerability. After defining key terms and presenting my method, key cases will be outlined. I will then focus the majority of this research paper on using the criteria of assessment to critically assess if the EU is vulnerable to the panopticon and chokepoint effect. I ultimately argue and conclude that in the digital sector, the EU is highly vulnerable to weaponised intercedence when looking at the panopticon effect and the mass collection of EU leaders' and citizens' data with no visible prospect of improvement in the foreseeable future. But the EU is not significantly vulnerable to weaponised intercedence when looking at the chokepoint effect as the case I focus on does not fulfil all necessary criteria for the possibility of the effect to be fully successfully enacted by a third country nor effective.

Defining Weaponised Interdependence

As used in this research paper, the term weaponised interdependence was introduced by Henry Farrell and Abraham Newman in 2019 (Farrell and Newman, 2019). Networks which are asymmetrical in nature, create a condition where certain favourably placed actors can use their position to exert power over other less favourably placed actors through their interdependent relationship. This phenomenon, in essence, is the definition of weaponised interdependence in its simplest sense. Through their domestic institutions or by acting more directly, states could exploit networks in two distinct ways: first, by collecting valuable data which could significantly advance their geopolitical position, putting them at an advantage, and second, by blocking crucial flows of data or economic activity to targeted enemy states. These two dynamics underpin the constitutive elements of weaponised interdependence, each of which is given the term "Panopticon effect" and "Chokepoint effect" by the authors (Farrell and Newman, 2019 p. 45) which we will further explore later. These two effects guide our assessment of the EU's vulnerability to weaponised interdependence.

Since weaponised interdependence as a concept explains the dynamics in asymmetrical networks, it is most useful to apply in cases where certain actors have more power than others. In the case of Networks, an actor represented as a node is considered to have more sway if it possesses more relational connections to other nodes. Therefore, the asymmetry we are referring to within a network describes a hierarchy of actors, the most powerful of which has the most relational connections, the least powerful having the least connections. Global networks, notably in the case we explore, have centralised nodes. In theory, actors with the most connections within an interdependent network have a bigger opportunity to exert their power through the panopticon or chokepoint effect (Drezner 2021). To provide a simplified representative example, let us consider a transit system such as the London Underground. When looking at a network map of the London Underground, one can observe that there are

super hubs, certain stations being better connected than others, some having more lines passing through them such as King's Cross St Pancras tube station. Hypothetically, if this tube station which links six out of the eleven lines were to unexpectedly shut down, not letting lines pass through it anymore, the entire network would be severely disrupted (Silva et al, 2015) and potentially entirely dysfunctional. This, of course, cannot be said for smaller stations with fewer connections. Therefore, some nodes are more crucial than others.

The Panopticon Effect

The panopticon effect refers to the ability of external states to view and collect crucial information in a network based on their advantageous position within it. Originally, the panopticon was a concept described by Bentham, later further developed and used metaphorically by Foucault (Foucault, 1977). It originally referred to a prison which has a central point which has a clear view of all prisoners (Bentham, 1791).

As noted earlier, decentralised networks tend to have nodes which bear more importance than others based on the number of connections it has. Within a decentralised network, political actors (states in our case) who have control or access over these central hub nodes have the ability to view activity passing through them. Controlling these important nodes, therefore, puts certain states at a significant advantage. “Controlling” a node, in our case, means that a state has jurisdiction over or has physical access to a node. Since hub nodes are difficult to avoid in a decentralised network, it can be almost impossible for actors to send and receive information without passing through them. One may at first think of this concept in the context of an advanced, modern globalised system, in particular in the context of technology (which we will focus on). But, examples of the panopticon effect can be found throughout history, for example, in the 19th and early 20th centuries, the UK used its advantageous position as a central

hub for finance and trade to gain critical information leading them to have a clearer understanding of global trade compared to other states (James, 2014, p. 53 - 54).

Using the Panopticon Effect to Critically Assess the EU's Vulnerability

In the context of digital platforms, the panopticon effect will be one of the two perspectives used to understand how, why, and to what degree the EU is vulnerable to weaponised interdependence. I will do so qualitatively using secondary evidence by answering: how much of the data of EU citizens and officials are vulnerable to foreign actors? The Snowden revelations will be used as a key case study here. This includes outlining the NSA's targeted spying of EU leaders, and citizens. I will also use evidence such as the Schrems' complaints. Additionally, I will also address a more recent case on the Chinese side regarding espionage from ByteDance, the company that owns TikTok. Although this specific ongoing ByteDance case is very recent and therefore lacks evidence to be used in order to provide an in-depth assessment, I will explore the EU's recent direct response to ban TikTok from civil servants' devices as a counterargument. My main counterargument to the EU's vulnerability within the panopticon effect relates to the introduction of key legislation to protect itself. I will critically assess whether the GDPR has been effective in limiting this vulnerability or if alternative systems to circumvent data protection regulations like the EU–US Privacy Shield crystalises the EU's vulnerability. This is evidence, at the very least, that EU institutions are aware of this vulnerability but raises questions on the degree of action taken.

The Chokepoint Effect

The Chokepoint effect refers to the ability of states to cut off other actors' access to crucial nodes in a network (Tusikov, 2021). As the name implies, it is therefore the act of actors using nodes as chokepoints. In the definition we use, the chokepoint effect also includes cases where actors are entirely cut off from a network (not just cut from one or more nodes). When

utilised offensively, the chokepoint effect can be particularly disruptive to a state as they may suddenly no longer has access to international markets or information in the global system, but may also be disruptive domestically as the links between actors within a state may be disrupted (Mastanduno, 2021, p. 67). This is because, in many cases, two actors within a state may be reliant on a node which is controlled by a foreign actor. As a demonstrative simplified hypothetical scenario, a citizen who may need to purchase a product from a company based domestically via the internet may need to do so through a digital platform (intermediary) based in a different continent. In this case, if the foreign actor who controls the intermediary decided to no longer operate in the market in question, the national economy would be affected as a crucial link between sellers and buyers would be lost.

Using the Chokepoint Effect to Critically Assess the EU's Vulnerability

In the context of digital platforms, the panopticon effect will be the second way we can understand the EU's vulnerability to weaponised interdependence. My assessment of the threat via the chokepoint effect will require similar information I will use in my panopticon effect assessment, but, since no clear cases have yet unfolded in the EU when looking at digital platforms, I will need to explore cases outside the EU and need to consider the plausibility of hypothetical scenarios on the continent. This will be done by assessing the EU's reliance on foreign digital platforms. In particular, I will outline the monopolistic powers of the Chinese "BATX" and the US "Big Five" within the EU also considering the lack of credible domestic platforms. Once again, to counter this point, I will look at the legislative steps the EU took to counter this by assessing if regulations like the Digital Markets Act (DMA) are sufficient to address this vulnerability. Additionally, I will heavily question the plausibility of certain key actors exiting the EU.

Mass Surveillance From Foreign Actors Over EU Data

The Snowden Revelations

What unfolded during Edward Snowden's revelations provide significant evidence regarding the mass surveillance present in the European Union. It can be argued that his revelations present the salience of the panopticon effect and the EU's vulnerability in this context. Edward Snowden, an employee of the United States National Security Agency (NSA) publicly leaked information about PRISM in 2013. PRISM was an NSA program which enabled the agency to collect data from large technology platforms. The NSA legally pressured large tech companies based in the United States to hand over information they held (Greenwald and MacAskill, 2013). The information in question which matters in our case is the data generated outside the US which includes the European Union. For example, AT&T, the American mobile phone network provider was heavily leveraged by the NSA. AT&T's customers are almost entirely based in the US, but, the NSA explicitly stated that it partnered with them because they have relationships with other international providers (The Intercept, 2018). This gave the agency the opportunity to collect data from EU citizens. Beyond citizens' valuable data being extracted by the NSA, the PRISM program also targeted EU commissioners, European heads of state, ministers, government buildings, and major European businesses (Poitras et al, 2013) (Glanz and Lehren, 2013) (Ball and Hopkins, 2013) (BBC News 2021).

In a more concrete sense, much of the EU's external communication will pass through the US for two reasons, first simply due to its geographical location, as an example we can think about the trajectory information needs to take to get from the EU to Japan. And secondly, because major telecommunication platforms are based there. The NSA describes this as the "home-field advantage" (Gallagher and Moltke, 2018).

It should be noted that the EU, before these revelations, had seemingly robust legal protection which would prevent cases like these, but these NSA programs unfolded regardless. Max Schrems highlighted this through the complaint he made to the Irish Data Protection Commissioner against Facebook (Sanghani, 2013). The law in the EU legally ensured that EU data would not be transferred to external states as per the Data Protection Directive unless significant protection could be guaranteed. The International Safe Harbor Privacy Principle introduced by the European Commission guaranteed that the US would be a safe location for the data of EU citizens to be stored in, processed in, or passed through. This was overturned by the European Court of Justice in 2015, 15 years later (CJEU, 2015).

The GDPR Mitigating the Panopticon Effect?

Some may argue that since the Snowden revelations and Schrems' first complaint in 2013, things might have changed. In particular, one could assume that since then, the EU is less vulnerable to the panopticon effect since the introduction of the GDPR and the revocation of The International Safe Harbor Privacy Principle. This is a reasonable assumption since many academics argue that the Snowden revelation encouraged and shaped the Regulation introduced in 2016 (Rossi 2018) (Coyne 2019). The GDPR, legally requires that EU data only be transferred to third countries (like the US) if the state can guarantee high levels of data protection and privacy (GDPR, 2016, Chapter V). Before moving forward, we should note that there is little evidence to indicate that the United States has changed its practices regarding mass surveillance and the collection of data entering its territory since the Snowden revelations (Gallagher, 2018).

Data transfers from the EU to the US remain largely unchanged in this regard since it was replaced with the EU–US Privacy Shield. This means in practice that data can largely be exported to the US, in a similar way to how it did before 2015 under the Safe Harbor Principle

(Schrems, 2016). The Privacy Shield was later similarly declared invalid in 2020 (BBC News 2020) but is expected to be replaced by the EU-US Data Privacy Framework to once again facilitate the transfer of data from the EU to the US (Politico, 2022).

Surveillance From China

For my assessment of the cases which utilises the panopticon effect to assess the EU's vulnerability to weaponised interdependence, it would not be reasonable not to address recent accusation regarding Chinese surveillance of EU citizens. ByteDance, the Chinese company that owns the social media platform TikTok outlined in 2022 where data from EU citizens was transferred and stored (Milmo, 2022). Elaine Fox, the head of privacy for TikTok in Europe officially stated that they: "store European user data in the U.S. and Singapore" […] "we allow certain employees within our corporate group located in Brazil, Canada, China, Israel, Japan, Malaysia, Philippines, Singapore, South Korea, and the United States remote access to TikTok European user data." (Fox, 2022).

This is another case where the panopticon effect is taking place in the EU and this example clearly shows the extent of the global network of data. Interestingly this case explicitly includes multiple countries where EU citizens' data is being stored and accessed. An assumption can be made that the Chinese government is making tactical use of EU citizens' data being transferred to third countries through this platform because multiple EU institutions banned the app from work-related devices (Goujard, Wax and Haeck, 2023). The extent and nature of the Chinese government's use of EU citizen's data it collects is inconclusive, but this ban from the EU Parliament, EU Council, and Commission indicates that EU institutions may hold undisclosed evidence that the panopticon effect may be in full effect from China against the EU.

Is the EU Vulnerable to the Panopticon Effect?

These cases are highly relevant to weaponised interdependence and the panopticon effect for two reasons. First, they demonstrate that the network of information worldwide was in fact highly dependent and centralised around very few hubs. These central hubs were large technology companies such as AT&T, Facebook, Google, and TikTok. These cases perfectly echo Farrell and Newman's emphasis on the potential for asymmetrical networks in particular to be leveraged. Secondly, the PRISM case shows the importance of the geographical location these key actors are based in. They may, to some degree, appear to operate in a broad and decentralised manner, but are in fact fundamentally beholden to the jurisdiction of the state they are based in: intelligence agencies have easy and legal access to data held by companies based within their jurisdiction as their cooperation shows. Using the panopticon effect as our criteria of assessment and the Snowden revelations as our main case study, the EU is vulnerable to weaponized interdependence. Beyond being potentially vulnerable we have demonstrated that the EU has been and still is the victim of the panopticon effect.

Dependence on Non-EU Platforms

The Dominance of Platforms Based in Third Countries

In order to address the threat of the Chokepoint effect, we must first look at the reliance the EU has on platforms based in non-EU states. Much is often said about the dominance of American and Chinese tech monopolies. They are often referred to as "the big five" in the case of American companies representing Microsoft, Alphabet, Apple, Meta, and Amazon (Sen, 2017). In the case of Chinese large platforms, they are referred to as "BATX", an acronym for Baidu, Alibaba, Tencent, and Xiaomi (Braun, 2020). Some academics have referred to their dominance in the EU as a form of "digital colonisation" (Iteanu, 2021). Using recent data leveraged from the introduction of the Digital Services Act which requires large companies to

disclose their user numbers (DSA, 2022 article 24, section 2), we can observe that the dominance of foreign-based tech platforms in the EU is substantial. As the regulation requires, the European Commission published a list of "Very Large Online Platforms" (VLOPs) and "Very Large Online Search Engines" (VLOSEs) which includes services that surpass 45 million monthly active users (European Commission, 2023). The two lists collectively identify 19 services. Out of those 19, 15 are US based, 2 are Chinese-based, and 2 are based in the EU.

Is the EU vulnerable to the chokepoint effect?

Although this point is important to assess the EU's vulnerability to the chokepoint effect, it does not fully answer our question. We must take the concept of the chokepoint effect to its end and ask what the risk of states removing their platforms from the EU's market is and how important of an impact could this have. In the case of US platforms, the impact on the EU would be significant since they hold 79% of the large platforms used in the EU. But, the long and relatively cohesive history of EU-US relations remains stable compared to other EU diplomatic relationships despite occasional calls for further autonomy (Goujard, 2023). The Chinese case is the opposite. If Chinese-based technology planforms were to leave the EU market, this would be much less significant since they currently only hold 2 of the 19 large services. But, compared to the US, the prospect of Chinese companies leaving the EU market is higher, considering growing tensions, although still uncertain (Bruegel, 2023).

In order for the Chokepoint effect to be a threat to the EU, two criteria should be filled by a third state: first, platforms based in the third state should represent a high level of dominance in the EU (this is only the case of the US), and second diplomatic relations must be at risk (this is only possibly the case in EU-China relations). Since no single non-EU state clearly fulfils both criteria, we can conclude that the EU is not vulnerable to the Chokepoint effect in the case of digital platforms. Furthermore, the EU is taking new precautions for these

two criteria not to be met: first by introducing legislation to discourage further growth of large tech platforms (the majority of which are currently foreign-based) through the enforcement of the Digital Markets Act (Cabral *et al.*, 2021). Secondly, the EU is actively working towards ensuring healthy diplomatic relations in the context of technology through the creation of so-called "Trade and Technology Councils", in particular for EU-US and EU-India trade relations (European Commission 2021) (Goujard, 2023). Through these forums, the EU is consequently positioning itself as a central hub node with more and stronger connections. Additionally, the likeliness for US or Chinese actors to leave the EU is low since the EU's market is considerably large, further cementing my argument that today, the EU is broadly not vulnerable to the Chokepoint effect when looking at digital platforms.

Conclusion

As I have demonstrated in this article, I have found that in the digital sector, the EU is vulnerable to the panopticon effect. I have argued that the Snowden revelations show the importance of the geographical location of where major technology firms are based as they can be leveraged by third countries to collect vast amounts of data from EU citizens and leaders. This echoes Newman's initial argument. The case of the PRISM program and the Chinese ByteDance case demonstrates that the panopticon effect makes the EU more than vulnerable to weaponised interdependence, the EU is already a target. As we have seen the GDPR did little to prevent this, and the EU is therefore still actively a target of weaponised interdependence when using the panopticon effect as a criterion.

On the other hand, I have argued that the EU is not vulnerable to the chokepoint effect for several reasons despite initial assumptions. First, because the prospect of US companies leaving the EU's market is unlikely based on the relatively healthy EU-US diplomatic relationship and due to the value of being present in the EU's market. Secondly, because the

prospect of China leaving the EU's market, although more likely, would not have as high an impact on the EU's economy. I also demonstrate that the EU is actively taking additional precautions to limit its potential vulnerability to the chokepoint effect through the DMA and the introduction of Trade and Technology Councils.

In conclusion, the EU is highly vulnerable to weaponised intercedence when looking at the panopticon effect and the mass collection of EU leaders' and citizens' data with no visible prospect of improvement in the foreseeable future, but the EU is not significantly vulnerable to weaponised intercedence when looking at the chokepoint effect in the digital sector.

Bibliography

Ball, J. and Hopkins, N. (2013) 'GCHQ and NSA targeted charities, Germans, Israeli PM and EU chief', *The Guardian*, 20 December. Available at: https://www.theguardian.com/uk-news/2013/dec/20/gchq-targeted-aid-agencies-german-government-eu-commissioner.

BBC News (2020) 'EU-US Privacy Shield for data struck down by court', 15 July. Available at: https://www.bbc.com/news/technology-53418898.

BBC News (2021) 'NSA spying row: Denmark accused of helping US spy on European officials', 30 May. Available at: https://www.bbc.com/news/world-europe-57302806.

Bentham, J. (1791) *Panopticon: Postscript: Part II: Containing a Plan of Management for a Panopticon Penitentiary-house. By Jeremy Bentham,* T. Payne.

Braun, E. (2020) 'Macron's EU tech agenda version 2.0', *POLITICO*, 7 February. Available at: https://www.politico.eu/article/macrons-eu-tech-agenda-version-2-0/.

Bruegel (2023) *A change of tack on EU-China relations*. Available at: https://www.bruegel.org/comment/change-tack-eu-china-relations.

Cabral, L.M.B. *et al.* (2021) 'The EU Digital Markets Act: A Report from a Panel of Economic Experts'. Rochester, NY. Available at: https://papers.ssrn.com/abstract=3783436.

CJEU (2015) 'The Court of Justice declares that the Commission's US Safe Harbour Decision is invalid', *Court of Justice of the European Union*.

Coyne, H. (2019) 'The Untold Story of Edward Snowden's Impact on the GDPR', *The Cyber Defense Review*, 4(2), pp. 65–80.

Drezner, D.W. (2021) 'Introduction: The Uses and Abuses of Weaponized Interdependence', in D.W. Drezner, H. Farrell, and A.L. Newman (eds) *The Uses and Abuses of Weaponized Interdependence*. Brookings Institution Press, pp. 1–16. Available at: https://www.jstor.org/stable/10.7864/j.ctv11sn64z.3.

DSA (2022) Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act) (Text with EEA relevance)

European Commission (2021) *EU-US Trade and Technology Council Inaugural Joint Statement*.

European Commission (2023) *Digital Services Act: Commission designates first set of Very Large Online Platforms and Search Engines*. Available at: https://ec.europa.eu/commission/presscorner/detail/en/IP_23_2413.

Farrell, H. and Newman, A.L. (2019) 'Weaponized Interdependence: How Global Economic Networks Shape State Coercion', *International Security*, 44(1), pp. 42–79. Available at: https://doi.org/10.1162/isec_a_00351.

Foucault, M. (1977) *Discipline and punish: the birth of the prison*. 1st American ed. New York: Pantheon Books.

Fox, E. (2022) *Sharing an Update to our Privacy Policy*, *Newsroom | TikTok*. Available at: https://newsroom.tiktok.com/en-eu/sharing-an-update-to-our-privacy-policy.

Gallagher, R. and Moltke, H. (2018) *The NSA's Hidden Spy Hubs in Eight U.S. Cities*, *The Intercept*. Available at: https://theintercept.com/2018/06/25/att-internet-nsa-spy-hubs/.

Gallagher, S. (2018) *The Snowden Legacy, part one: What's changed, really?*, *Ars Technica*. Available at: https://arstechnica.com/tech-policy/2018/11/the-snowden-legacy-part-one-whats-changed-really/.

GDPR (2016) Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance)

Glanz, J. and Lehren, A.W. (2013) 'N.S.A. Spied on Allies, Aid Groups and Businesses', *The New York Times*, 20 December. Available at: https://www.nytimes.com/2013/12/21/world/nsa-dragnet-included-allies-aid-groups-and-business-elite.html.

Goujard, C. (2023) 'Charles Michel: Europe warming up to Macron's "strategic autonomy" push away from US', *POLITICO*, 11 April. Available at: https://www.politico.eu/article/europe-warming-up-to-macrons-strategic-autonomy-push-says-charles-michel/.

Goujard, C. (2023) 'EU and India launch Trade and Technology Council', *POLITICO*, 6 February. Available at: https://www.politico.eu/article/eu-and-india-launch-trade-and-technology-council/.

Goujard, C., Wax, E. and Haeck, P. (2023) 'Brussels banned TikTok. Europe has questions', *POLITICO*, 3 March. Available at: https://www.politico.eu/article/eu-brussels-ban-tiktok-europe-has-questions/.

Greenwald, G. and MacAskill, E. (2013) 'NSA Prism program taps in to user data of Apple, Google and others', *The Guardian*, 7 June. Available at: https://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data.

Iteanu, O. (2021) ‘La colonisation digitale’, *Constructif*, 58(1), pp. 18–21. Available at: https://doi.org/10.3917/const.058.0018.

James, H. (2014) ‘Cosmos, chaos: finance, power and conflict’, *International Affairs*, 90(1), pp. 37–57. Available at: https://doi.org/10.1111/1468-2346.12094.

Mastanduno, M. (2021) ‘Hegemony and Fear: The National Security Determinants of Weaponized Interdependence’, in D.W. Drezner, H. Farrell, and A.L. Newman (eds) *The Uses and Abuses of Weaponized Interdependence*. Brookings Institution Press, pp. 67–83. Available at: https://www.jstor.org/stable/10.7864/j.ctv11sn64z.5.

Milmo, D. (2022) ‘TikTok tells European users its staff in China get access to their data’, *The Guardian*, 2 November. Available at: https://www.theguardian.com/technology/2022/nov/02/tiktok-tells-european-users-its-staff-in-china-get-access-to-their-data.

Poitras, L. *et al.* (2013) ‘Secret Documents: NSA Targeted Germany and EU Buildings’, *Der Spiegel*, 1 July. Available at: https://www.spiegel.de/international/world/secret-documents-nsa-targeted-germany-and-eu-buildings-a-908609.html.

Politico (2022) US expected to publish Privacy Shield executive order next week’, 27 September. Available at: https://www.politico.eu/article/us-expected-to-publish-privacy-shield-executive-order-next-week/.

Rossi, A. (2018) ‘How the Snowden Revelations Saved the EU General Data Protection Regulation’, *The International Spectator*, 53(4), pp. 95–111.

Sanghani, R. (2013) *Facebook 'PRISM' decision to be reviewed by Irish High Court*. Available at: https://www.telegraph.co.uk/technology/facebook/10401419/Facebook-PRISM-decision-to-be-reviewed-by-Irish-High-Court.html.

Schrems, M. (2016) 'The Privacy Shield is a Soft Update of the Safe Harbor Foreword', *European Data Protection Law Review (EDPL)*, 2(2), pp. 148–150.

Sen, C. (2017) 'The "Big Five" Could Destroy the Tech Ecosystem', *Bloomberg.com*, 15 November. Available at: https://www.bloomberg.com/opinion/articles/2017-11-15/the-big-five-could-destroy-the-tech-ecosystem.

Silva, R., Kang, S.M. and Airoldi, E.M. (2015) 'Predicting traffic volumes and estimating the effects of shocks in massive transportation systems', *Proceedings of the National Academy of Sciences*, 112(18), pp. 5643–5648. Available at: https://doi.org/10.1073/pnas.1412908112.

The Intercept, 'FAIRVIEW overview with notes' (2018). Available at: https://theintercept.com/document/2018/06/25/fairview-overview-with-notes/.

Tusikov, N. (2021) 'Internet Platforms Weaponizing Choke Points', in D.W. Drezner, H. Farrell, and A.L. Newman (eds) *The Uses and Abuses of Weaponized Interdependence*. Brookings Institution Press, pp. 133–148. Available at: https://www.jstor.org/stable/10.7864/j.ctv11sn64z.9.