01/2023

#01

Reducing the Weaponization of Digital Interdependence:

The Overlooked Potential of the EU's New Digital Regulation Package

Felix Garten
Nora Kürzdörfer

DIGITAL DIPLOMACY AND STATECRAFT POLICY BRIEF

GIGA
German Institute for Global and Area Studies
Leibniz-Institut für Globale und Regionale Studien

DIGITAL DIPLOMACY AND STATECRAFT POLICY BRIEF

Authors

Felix Garten is a doctoral researcher at the Hertie School and a PhD candidate at the Berlin Graduate School for Global and Transregional Studies (BGTS). He works for Prof. Daniela Stockmann and within the Cluster of Excellence Contestations of the Liberal Script (SCRIPTS) for *The Challenge to the Challenge* project, which is led by Prof. Amrita Narlikar and Prof. Mark Hallerberg. In his PhD, Felix studies the relationship between Chinese digital platform companies and the Chinese government as well as responses of various countries to the Digital Silk Road. His research interests are global finance, weaponized interdependence, platform regulation and China's political economy.

Nora Kürzdörfer is a doctoral researcher at the German Institute for Global and Area Studies (GIGA) and a student at the Berlin Graduate School for Global and Transregional Studies at Hertie School and Free University Berlin. She works for *The Challenge to the Challenge*, a project by the Cluster of Excellence Contestations of the Liberal Script (SCRIPTS). The project is led by Prof. Amrita Narlikar and Prof. Mark Hallerberg and addresses responses to the Belt and Road Initiative by various actors. In her PhD, Nora studies the Digital Silk Road, e.g. in the European Union and the World Trade Organization. Her research interests include global trade, weaponized interdependence and EU external relations. Currently, Nora is seconded to the German Federal Foreign Office as member of the GIGA knowledge exchange project *Transfer for Transformation* (T4T), funded by the Leibniz Competition and led by Prof. Amrita Narlikar.

Digital technologies are fundamentally transforming societies worldwide. The Global South is an important shaper of this change. "Digital Diplomacy and Statecraft" is a research project funded by the Federal Foreign Office. Under the lead of Prof. Amrita Narlikar, Prof. Jann Lay, and Prof. Christian von Soest, this initiative explores how digitalisation offers new opportunities, challenges, and instruments for foreign policy. Bringing together international experts and identifying prospects and threats of digitalization, the project analyses the drivers and consequences of digitalisation across world regions. Through this research on (and with) Africa, Asia, Latin America, the Middle East as well as global actors, it aims to deliver useful impulses for German foreign policy and timely responses of (digital) diplomacy.

GIGA
German Institute for Global and Area Studies
Leibniz-Institut für Globale und Regionale Studien

Reducing the Weaponization of Digital Interdependence: The Overlooked Potential of the EU's New Digital Regulation Package

Abstract

The Digital Services Act and the Digital Market Act pose an important addition to the EU's toolbox to limit the power of digital companies. The DSA is directed at protecting consumer rights and at enhancing accountability of platforms. The DMA serves to achieve fair competition on the digital market that has taken an oligopoly-like structure. We explain an aspect that is largely overlooked in the debate on the new regulation, its potential to reduce the weaponization of digital dependence. While the DMA helps to reduce the power of single actors, the DSA provides a useful tool to obtain more knowledge about the underlying structure of digital networks. This is crucial to understand what actors are able to exercise coercion over others. Policymakers can cooperate with researchers that are able to inquire platform data under the DSA's transparency regime from 2024 onwards. This will be possible only if companies do not abuse their right to withhold information under specific circumstances. In addition, the weaponization of interdependence has to be acknowledged as systemic risk to ensure that academics working on the issue are able to obtain data. If these conditions are met, researchers and practitioners would benefit jointly.

Policy Implications

- Under the DSA, researchers with a university or research institute affiliation can obtain access to platform data. This has the positive side-effect of fostering cooperation between academics and practitioners. Partnerships between policymakers and researchers would be of mutual benefit, by **enhancing impactful research** and informing policy choices.
- Data access is granted only for research addressing systemic risks of platforms. Researchers interested in weaponized interdependence can help **identifying what counts as systemic risk**. It remains to be seen whether or not researchers will be able to obtain network data in the interest of public security.
- In particular, it will be crucial that platforms do not abuse their right to invoke exceptions based on security of services, confidential information, or trade secrets. This requires **prioritizing security over commercial interests**.
- The threshold determining which platforms are subject to both the DSA and the DMA is met by a number of US companies. However, the package can help promote the **understanding that not only US platforms can exercise coercion.** Chinese companies that are expanding under the Digital Silk Road also need to adhere to the regulation. Considering that securitization aspects gained importance in the debate on Chinese technology, it would be interesting to obtain data on Chinese firms in order to be able to analyze whether their network position and structure promotes weaponized interdependence or not.

Consumer protection and fair market conditions: The Digital Services Act and the Digital Markets Act

The European Union's (EU) General Data Protection Regulation (GDPR) enhancing individual and privacy rights is widely celebrated as gold standard of data protection. While some problems related to the implementation and enforcement remain, the regulation has proven useful as "one-stop shop for regulatory oversight (…) and to minimize regulatory arbitrage" (Jang & Newman, 2022, p. 285). In 2022, the EU added a new set of digital regulations to its portfolio, the Digital Services Act (DSA) and the Digital Markets Act (DMA). Similar to the GDPR, both the DSA and the DMA apply to companies offering services inside the European Economic Area (EEA), regardless of their location (European Commission, 2022b, 2022a). The Digital Services Act aims to reduce harm and risk for online consumers and requires all digital services to comply with transparency obligations. The range of obligations rises in proportion to the role and size of platforms. Very large online platforms (VLOCs) with more than 45 million users have the most comprehensive duties. The Digital Market act addresses the unfair advantage large online platforms have due to their market share. They are able to create bottlenecks for smaller actors by favoring their own services, e.g. through restricting access to their app stores or preventing the installment of applications from other companies. Gatekeeper companies falling under the DMA are defined by an annual turnover that amounts to €7.5 billion or more for the past three financial years, more than 45 million monthly end users, and an entrenched and durable position (European Commission, 2022b, 2022a). In April 2023, the Commission announced 17 platforms and two search engines meeting the threshold of the DSA (European Commission, 2023).[1] It is likely that many of these companies will also fall under the DMA, resulting in additional obligations.

Security implications of digital platforms

The EU's ambition to decrease the power of digital platforms responds to the shifting paradigm of global trade. As the Russian invasion of the Ukraine has shown, the liberal promise of interdependence as generator not only of economic prosperity but also of peace does not hold. Like dependence on natural resources including gas, dependence on digital platforms and infrastructure is also prone to be weaponized. The oligopoly-like position of many tech companies has generated a hierarchical structure of digital networks. A few firms, mostly from the US and now joined by Chinese competitors, are in the possession of large amounts of data. Under the

[1] The list includes Alibaba's AliExpress, Amazon Store, Apple's AppStore, Booking.com, Facebook, Google Play, Google Maps, Google Shopping, Instagram, LinkedIn, Pinterest, Snapchat, TikTok, Twitter, Wikipedia, YouTube, and Zalando, as well as Bing and Google Search.

right institutional set-up, the state where the platform originates can gain access to this information and use it for coercive actions against other actors (Farrell & Newman, 2019; Tusikov, 2021). Farrell and Newman (2019) who developed the concept of weaponized interdependence refer to this as panopticon effect. A prominent example poses the US National Security Agency's access to data from telecommunications providers like AT&T for surveillance purposes. Next to collecting data, platforms can also restrict access or services for other actors or states. This type of coercion, referred to as chokepoint effect, can lead to severe economic repercussions for the targeted actor, also referred to as bottleneck. The Chinese government for example pressured Alibaba and Tencent to ban US basketball broadcasts and merchandise on their e-commerce platforms in response to solidarity with the pro-democracy protests in Hong Kong voiced by the manager of an NBA team (Tusikov, 2021). India has set a precedent by banning more than 100 Chinese apps, including TikTok due to concerns about the security implications of digital platforms. Other countries such as the US are taking steps to follow suit (Times of India, 2023). In the EU, the debate on limiting platform power is related more to the protection of consumers and fair competition than to national security. Nonetheless, as we explain below, the Union's regulations also have the potential to protect against the weaponization of digital networks.

How the DSA helps addressing weaponized interdependence

The DMA's purpose of deterring companies from creating bottlenecks for other actors certainly matters to reduce the possibility of weaponized interdependence. If actors can choose between providers, it becomes more difficult to restrict access to a digital network. However, the DSA could take an even more practical role. In order to be able to understand why economic coercion is possible and which actors are equipped to perform weaponized interdependence it is crucial to explore the structure of economic networks. As Farrell and Newman (2022) explain, interdisciplinary research is necessary to analyze how global supply-chains are connected, what security risks they entail and how actors in a network relate to each other. The DSA can become a powerful tool for this endeavor, as it provides researchers with the ability to analyze VLOPs, their network position, and how they interact with their stakeholders and competitors. The regulation's transparency regime is the first mechanism that allows for accessing internal platform data, including their algorithms and large network sampling.[2] It is thus not surprising that the various drafts of the regulation as well as the final version have attracted a vivid debate even though the

[2] For more details, see Algorithmwatch (2022): A guide to the EU's new rules for researcher access to platform data

transparency regime will not be up and running before 2024. We add to the debate by focusing on those aspects of the regulation that are related to its potential in addressing weaponized interdependence:

1. ***Enhancing impact-driven research:*** In order to be able to file a request for data access, researchers need to be affiliated with a university or a research institute with scientific research as primary goal. In addition, they need to be independent from commercial interests and able to adhere to confidentiality requirements (Directive (EU) 2019/790, 2019; Regulation (EU) 2022/2065, 2022). At a first glance, this can be interpreted as a restriction for research by civil society organizations, journalists, and national government authorities. The first two groups are more difficult to accredit and to demarcate from commercial interests than academics. However, they can still benefit from the transparency regime by entering into cooperation with vetted researchers. This also applies to government authorities. As Farrell and Newman (2022) outline governments have realized that addressing weaponized interdependence requires understanding economic networks as well as their underlying algorithms. Government units, including policy-planning departments of ministries, would benefit from cooperating with researchers using the DSA to explore the structure of digital networks. Unintentionally, the regulation responds to the need for partnerships between academics and policymakers, moving research out of the ivory tower and leading to better-informed policymaking (Narlikar, 2022).
2. ***Identifying what counts as systemic risk:*** In line with Article 40 of the regulation, in order to obtain data access, the research has to contribute to detecting, identifying, and understanding "systemic risks". Article 34 further defines that systemic risks are illegal content, negative effects for fundamental rights, on civic discourse, on elections and public security, on public health, on minors, on physical and mental well-being as well as on gender-based violence (Regulation (EU) 2022/2065, 2022). In light of this wording, it is not surprising that much of the debate on the DSA focuses on questions of counterfeit products, violent images as well as misinformation and manipulation. At a first glance, it appears difficult to relate the article directly to the risks of weaponized interdependence. Even though coercive action via digital platforms arguably entails systemic risks, the only category that could immediately fit is that of "public security". It remains to be seen whether researchers interested in weaponized interdependence will be able to convince DSCs and platforms of their endeavor.
3. ***Prioritizing security over commercial interests:*** Not only does the DSA restrict who can access data and for what purpose it also gives platforms the ability to deny access due to security of service and confidentiality, including the protection of personal data and trade secrets

(Regulation (EU) 2022/2065, 2022). Whistleblower Frances Haugen and other activists raised their concerns about this exception, especially with regard to trade secrets. Meta e.g. has a history of abusing privacy law to deny data access. The provision of trade secret exemptions certainly runs the same risk (Albert, 2022; Albert & Spielkamp, 2022; Leerssen, 2021; Prettner & Andrew, 2021). In response to this criticism the final version of the regulation now states that commercial interests cannot be used to invoke the exception (Regulation (EU) 2022/2065, 2022). Research on weaponized interdependence, e.g. on how algorithms can create bottlenecks, may indeed require data related to trade secrets. Whether or not platforms will be allowed to withhold such data will ultimately be a political question, i.e. whether commercial interests will continue to outweigh security interests.

4. ***Understanding that not only US platforms can exercise coercion*:** Only very large online platforms with more than 45 million active users in the EU are subject to the DSA's transparency regime. Considering that the majority of firms falling under this category are from the US, industry groups in the US went as far as describing the DSA "as written to target US companies" (Satariano, 2022). While US platforms indeed have a high market share in the EU, European companies like Spotify and Zalando are also subject to the DSA. For questions related to weaponized interdependence, it is interesting to see that Chinese companies expanding under the Digital Silk Road (DSR), the digital component of China's Belt and Road Initiative, also fall under the scope of the DSA. In its 2022 annual report, Alibaba Group already identifies the DSA and the DMA as regulatory challenges (Alibaba Group, 2022). TikTok, which is currently widely debated with regard to data sensitivity concerns, is among the VLOPs, too. In the discussion of US companies' power, the focus is usually on unfair practices due to their large market share. The discussion on Chinese tech firms is much more securitized. Even though not all companies are state-owned, under China's state-capitalist system they are to varying degrees at least state-led (Babić & Dixon, 2022; Erie & Streinz, 2021; Otero-Iglesias & Weissenegger, 2020). The "crackdown" on China's tech giants shows that the Chinese government increases the control of its tech champions to align them more with the official party line (Creemers et al., 2023). State regulators use "golden shares" in private tech companies to influence decision making and have developed a new regulatory environment that forces private actors to work closer with the government to avoid more punishments. Due to the Chinese government's ability to influence commercial actors there is an increased fear that cooperation with Chinese firms results in weaponized interdependence (Drezner et al., 2021; Farrell & Newman, 2019). This includes concerns about Digital Authoritarianism, assuming that the DSR does not expand Chinese technologies only, but also influences data

governance by exporting non-democratic values and practices to other countries. Erie and Streinz (2021) reject the notion of Digital Authoritarianism as too broad and too generalized. At the same time, they explain that the Beijing Effect allows for the export of Chinese data regulations across borders, if the country hosting Chinese firms has a weak regulatory framework and is in need of digital infrastructure. Obtaining data on Chinese platform companies through the DSA, including Alibaba Group which is present in Europe not only through its market platform but also through wider services offered by its electronic World Trade Platform, would be a novelty. So far, it has not been possible to obtain access to network and algorithm data, making it more difficult to determine whether the expanse of the DSR enables companies to exercise coercion or not.

Outlook

Over the next months, the 19 companies meeting the threshold of the DSA will need to adhere to a new set of rules and obligations. Before the end of the year, the Commission will announce the companies falling under the DMA as well. For the limitation of coercion via digital networks, the DSA will play an especially important role. By equipping researchers and policymakers with more knowledge about leading platform companies it will become easier to identify systemic risks and to protect against the weaponization of digital interdependence. The success of the DSA's transparency regime hinges on two factors. First, weaponized interdependence has to be identified as systemic risk for public security. Second, companies may not abuse their right to withhold information for alleged trade secrets or confidentiality purposes. If these factors are fulfilled, the regulation package poses a valuable addition to the EU's toolbox to achieve greater strategic autonomy.

Bibliography

Albert, J. (2022, December 7). A guide to the EU's new rules for researcher access to platform data. *AlgorithmWatch*. https://algorithmwatch.org/en/dsa-data-access-explained/

Albert, J., & Spielkamp, M. (2022, June 30). Time for Europe to turn the tables on Big Tech. *Context - Thomson Reuters Foundation*. https://www.context.news/big-tech/opinion/digital-services-act-time-for-europe-to-turn-the-tables-on-big-tech

Alibaba Group. (2022). *Alibaba Group Holding Limited—Fiscal Year 2022—Annual Report*. https://data.alibabagroup.com/ecms-files/886023430/c330302f-bfdd-4c79-a5ac-614446292e68.pdf

Babić, M., & Dixon, A. D. (2022). Is the China Effect Real? Ideational Change and the Political Contestation of Chinese State-Led Investment in Europe. *The Chinese Journal of International Politics*, *15*(2), 111–139. https://doi.org/10.1093/cjip/poac009

Creemers, R., Costigan, J., Triolo, P., Nunlist, T., Dudley, L., Danowski, M., Chorzempa, M., Lucero, K., & Huang, S. (2023, January 25). Is China's Tech 'Crackdown' or 'Rectification' Over? *Digi China*. https://digichina.stanford.edu/work/is-chinas-tech-crackdown-or-rectification-over/

Drezner, D. W., Newman, A. L., & Farrell, H. (2021). *The Uses and Abuses of Weaponized Interdependence*. Brookings Institution Press.

Erie, M. S., & Streinz, T. (2021). The Beijing Effect: China's "Digital Silk Road" as Transnational Data Governance. *New York University Journal of International Law and Politics (JILP), Forthcoming*, 61.

European Commission. (2023). *Gesetz über digitale Dienste: Sehr große Online-Plattformen und Suchmaschinen.* https://ec.europa.eu/commission/presscorner/detail/de/ip_23_2413

European Commission. (2022a). *The Digital Markets Act: Ensuring fair and open digital markets*. https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/digital-markets-act-ensuring-fair-and-open-digital-markets_en

European Commission. (2022b). *The Digital Services Act: Ensuring a safe and accountable online environment*. https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/digital-services-act-ensuring-safe-and-accountable-online-environment_en

Directive (EU) 2019/790 of the European Parliament and of the Council of 17 April 2019 on copyright and related rights in the Digital Single Market and amending Directives 96/9/EC and 2001/29/EC (Text with EEA relevance.), 130 OJL (2019). https://eur-lex.europa.eu/eli/dir/2019/790/oj

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), 277 OJ L (2022). http://data.europa.eu/eli/reg/2022/2065/oj/eng

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

Farrell, H., & Newman, A. L. (2022). Weak links in finance and supply chains are easily weaponized. *Nature*, *605*(7909), 219–222. https://doi.org/10.1038/d41586-022-01254-5

Jang, W., & Newman, A. L. (2022). Enforcing European Privacy Regulations from Below: Transnational Fire Alarms and the General Data Protection Regulation*. *JCMS: Journal of Common Market Studies*, *60*(2), 283–300. https://doi.org/10.1111/jcms.13215

Leerssen, P. (2021). Platform research access in Article 31 of the Digital Services Act: Sword without a shield? *Verfassungsblog*. https://doi.org/10.17176/20210907-214355-0

Narlikar, A. (2022). How not to negotiate: The case of trade multilateralism. *International Affairs*, *98*(5), 1553–1573. https://doi.org/10.1093/ia/iiac063

Otero-Iglesias, M., & Weissenegger, M. (2020). Motivations, security threats and geopolitical implications of Chinese investment in the EU energy sector: The case of CDP Reti. *European Journal of International Relations*, *26*(2), 594–620. https://doi.org/10.1177/1354066119871350

Prettner, C., & Andrew, S. (2021, November 30). Trade secrets don't trump our rights. *Www.Euractiv.Com*. https://www.euractiv.com/section/digital/opinion/trade-secrets-dont-trump-our-rights/

Satariano, A. (2022, March 24). E.U. Takes Aim at Big Tech's Power With Landmark Digital Act. *The New York Times*. https://www.nytimes.com/2022/03/24/technology/eu-regulation-apple-meta-google.html

Times of India. (2023, January 23). US may go the "India way" on TikTok. *Times of India*. https://timesofindia.indiatimes.com/gadgets-news/us-may-go-the-india-way-on-tiktok/articleshow/97394184.cms

Tusikov, N. (2021). Internet Platforms Weaponizing Choke Points. In D. W. Drezner, A. L. Newman, & H. Farrell (Eds.), *The Uses and Abuses of Weaponized Interdependence* (pp. 133–148). Brookings Institution Press.

DIGITAL DIPLOMACY AND STATECRAFT POLICY BRIEF