Digital corporate autonomy: geo-economics and corporate agency in conflict and competition

Broeders, D.W.J.; Sukumar, A.; Kello, M.; Andersen; Lise H.

Routledge
Taylor & Francis Group

Review of International Political Economy

ISSN: (Print) (Online) Journal homepage: www.tandfonline.com/journals/rrip20

Digital corporate autonomy: geo-economics and corporate agency in conflict and competition

Dennis Broeders, Arun Sukumar, Monica Kello & Lise H. Andersen

To cite this article: Dennis Broeders, Arun Sukumar, Monica Kello & Lise H. Andersen (24 Feb 2025): Digital corporate autonomy: geo-economics and corporate agency in conflict and competition, Review of International Political Economy, DOI: 10.1080/09692290.2025.2468308

To link to this article: https://doi.org/10.1080/09692290.2025.2468308

Published online: 24 Feb 2025.

REVIEW OF INTERNATIONAL POLITICAL ECONOMY
https://doi.org/10.1080/09692290.2025.2468308

Digital corporate autonomy: geo-economics and corporate agency in conflict and competition

Dennis Broeders[a], Arun Sukumar[b], Monica Kello[c] and Lise H. Andersen[a]

[a]Institute of Security and Global Affairs, Leiden University, The Hague, The Netherlands; [b]Department of International Relations, Ashoka University, New Delhi, India; [c]Department of War Studies, King's College London, London, UK

ABSTRACT

Many argue that we have entered a new era of international 'geoeconomic' relations. Looking at western geoeconomic measures in the digital economy, we specifically focus on the role and agency of private companies in relation to geoeconomic policymaking, and take issue with state-centred international relations (IR) theory on geoeconomics that tends to assume company compliance with government policy. We contend that corporate agency is crucial to understanding the dynamics of geoeconomic policymaking and implementation, especially in the digital domain where tech companies have accrued unprecedented power and position. We introduce the notion of Digital Corporate Autonomy as a characteristic of these companies, which is built on their infrastructural power and facilitated by the increasing informality in the international system. Using this framework, we study the involvement of Big Tech companies in the war in Ukraine and corporate manoeuvring in relation to the United States-Japan-Netherlands semiconductor coalition, against the background of rising Sino-American tensions. Our analysis reveals a broad spectrum of government-corporate interaction and a high level of digital corporate autonomy set against the contexts of war – the height of statecraft – and hegemonic rivalry. We conclude that digital corporate autonomy underlines the importance of scholarly attention to corporate agency and behaviour.

ARTICLE HISTORY Received 08 March 2024; Accepted 05 February 2025

KEYWORDS

Geopolitics; geoeconomics; Big Tech; transnational corporations; infrastructure; weaponized interdependence

Introduction

Many scholars have argued that we have entered a new era of international economic and political relations that can be characterised as 'geoeconomic'. In the International Relations (IR) literature, some have spoken of a 'geoeconomic order' (Roberts et al., 2019) or of 'geoeconomics and statecraft' (Blackwill & Harris, 2016). In 1990, Luttwak revived the term of geo-economics and argued that international

CONTACT Dennis Broeders d.w.j.broeders@fgga.leidenuniv.nl Institute of Security and Global Affairs, Leiden University, The Netherlands

tensions will increasingly follow 'the logic of conflict, in the grammar of commerce'. More recent versions of 'the geostrategic use of economic power by nation states' (Wigell, 2016) have emerged in the form of the framework of 'weaponised interdependence' (Drezner et al., 2021; Farrell & Newman, 2019, 2023). Although most of these studies and theories acknowledge that the interests of companies and governments do not always align, they tend to focus on the coercive use of the economy by states in international relations and see companies as merely an extension of state power.

While the study of the relationship between the economy and national security is hardly new (see for example Baldwin, 1985; Blackwill & Harris, 2016; Demarais, 2022; Førland, 1993), the current era of geoeconomic competition, with China-United States (US) rivalry at its centre, merits special attention. Changes in global economic interdependencies and supply chains, the prominence of the digital sphere as one of the main geopolitical and geoeconomic battlefields—and the characteristics of the corporate actors that populate that sphere—point in the direction of a rethink of geo-economic theory. This paper argues that much of the current—especially IR—theory fails to recognise corporate agency in any meaningful sense and sees the role of companies as subordinate and instrumental to states' geopolitical needs. Building on recent critical work on geoeconomics[1] we argue that, especially in the digital domain, transnational multinational corporations (MNCs) have 'corporate autonomy' which they use to serve their own economic and political needs in times of geopolitical tensions and conflict. Corporate autonomy puts the spotlight firmly on the agency that companies employ to navigate geopolitical tensions and the restrictions and opportunities created by states. This rise of corporate agency in the technical domain is supported, firstly, by the rise of informality in the international governance system which creates opportunities for corporate agency and, secondly, by the fact that many MNCs in the digital sphere hold vast infrastructural power that augments their corporate agency.

In recent years, IR scholars have documented a steady but discernible trend towards the decline of formal multilateral organisations and the rise, in their stead, of informal institutions and agreements in various domains of global governance (Roger & Rowan, 2023; Vabulas & Snidal, 2021; Westerwinter et al., 2021). This turn to informality has also created room for corporate actors to take up more space in informal governance and diplomacy and/or by simply creating facts on the ground, not least in the digital sphere (Sukumar et al., 2024). Secondly, the vital importance of networks and infrastructures in the theory of weaponised interdependence underscores and amplifies the corporate autonomy of Big Tech companies that own and operate digital infrastructure and dominate some of the critical supply chains of the global digital economy. Building on recent literature by, amongst others, De Goede and Westermeier (2022), Bueger et al. (2023) and Abels (2024), which seeks to integrate the field of infrastructure studies into IR and argues that infrastructures themselves have (political) agency, we contend that this infrastructural agency augments the agency of Big Tech corporations which dominate the digital domain. 'Nodality' does not just amplify state power (Farrell & Newman, 2019) but also, and perhaps more so, amplifies the power and agency of certain corporate actors in the digital sphere. These combined factors contribute to what this paper calls *digital corporate autonomy*.

The next section discusses the theoretical foundations of digital corporate autonomy. Building on critical geoeconomics literature and literature on informality and infrastructural power in IR, we contend that the latter two characteristics underpin corporate agency in the digital sphere, especially in times of geopolitical tensions. In sections three and four, we examine the nature of digital corporate autonomy in two cases of differing geopolitical intensity: One analysing corporate behaviour during a hot war and one analysing corporate behaviour in the crosshairs of rising geoeconomic rivalry between the US and China. We examine corporate behaviour in Ukraine where companies seem to choose sides autonomously—irrespective of home government requests—while at the same time seeking rewards in terms of reputation and the harvesting of experimental data. The second case centres on ASML, a Dutch company with a monopolistic nodal position in the global manufacturing supply chain of semiconductors, which navigates the geopolitical pressures on its business model as a result of the informal US-Japan-Netherlands 'agreement' to restrict the sale of advanced semiconductor materials to China. The last section draws conclusions.

Beyond state centred geoeconomics: the outlines of digital corporate autonomy

In the early 1990s, neorealist thinkers started to theorise that, although the post-cold war world would perhaps see less open interstate conflict, tensions would (also) take an economic form. Set against the background of a rising Japan, Luttwak (1990) rekindled the terminology of *geo-economics*, arguing that international tensions will increasingly follow 'the logic of conflict, in the grammar of commerce'. Luttwakian geo-economics focuses on the *coercive* use of the economy vis-á-vis rival powers. Or as Huntington (1993), a kindred spirit, phrased it: '[I]n a world in which military conflict between major states is unlikely, economic power will be increasingly important in determining the primacy or subordination of states'. The main *goals* of geoeconomics then, are geopolitical, and sit at the state-to-state level. States are concerned about the threat or the rise of a rival state and seek to counterbalance that threat, and do so through economic means. Often these 'economic means' come in the form of companies, and the question is whether companies are always and easily instrumentalised. At the state-to-state level, governments aim to coerce their adversaries or at least limit their options through the companies that are in their jurisdiction. In addition to coercion (through sanctions, export restrictions etc.) Choer Moraes and Wigell (2022, p. 35) highlighted two additional strategies at the state-to-state level: States can follow a strategy of *geoeconomic binding*—trying to make target states economically dependent on an external power which thereby gains political leverage—or a strategy of *geoeconomic wedging*, i.e. a policy of 'divide and rule' in which the external power offers economic incentives selectively to some targets (a country or coalition of countries), but not to others. Although economic statecraft also entails a positive agenda of investment, innovation, supporting and protecting national champions, most geo-economic theory is about strategic, primarily coercive, power politics in the economic domain within a realist framework.

A recent geoeconomic framework that has gained a lot of traction in policy and academia is that of *weaponised interdependence* (Drezner et al., 2021; Farrell &

Newman, 2019, 2023). This theory's point of departure is that economic interdependence has created global complex systems in the form of asymmetric network structures that can be weaponised. 'Specifically, states with political authority over the central nodes in the international networked structures through which money, goods, and information travel are uniquely positioned to impose costs on others' (Farrell & Newman, 2019, p. 45). In this vision, power derives from the use of manmade infrastructures and supply chains—rather than from natural resources and geographical conditions as the term 'geo' might also suggest (Scholvin & Wigell, 2018). Farrell and Newman (2019, p. 45) point to two strategies for 'nodal' states to gain political advantage: They can 'weaponize networks to gather information or choke off economic and information flows, discover and exploit vulnerabilities, compel policy change, and deter unwanted actions'. The focus in this framework is on the coercive possibilities of the economy as underlined by the subtitle of Farrell and Newman's 2019 article: 'How global economic networks shape state coercion'.

Shifting the focus to corporate agency and strategies

Grounded in IR, most geo-economic academic frameworks tend to be largely state-centred: the geopolitical relation and manoeuvring between states is central and companies are represented as policy instruments. But to achieve state-to-state results, governments are dependent on actors that are not part of the state. Or, in the words of Luttwak (1990, p. 22): 'While states occupy virtually all of the world's political space, they occupy only a fraction of the total economic space, and global political-economic trends such as privatization are reducing that fraction even further'. In 2021, Farrell and Newman conceded that their 'original theory did not provide any real independent agency to businesses, treating them as passive transmitters of state policy' (Farrell & Newman, 2021, p. 315). Recently, authors like Norris (2016), Choer Moraes and Wigell (2022), Gjesvik (2023), Chen and Evers (2023) and Abels (2024) have started to challenge the lack of corporate agency in geoeconomic theory. Norris (2016, p. 11) argues that 'scholars engage in an intellectual shorthand when they refer to international economic relations between states' and brings corporate agency into his model as a variable that co-determines the level of state control in economic statecraft. Chen and Evers (2023) analyse system level changes—hegemonic decline and the challenger's rise—to explain why corporations align (the rising challenger) or conflict (the declining hegemon) with the geoeconomic interest of their home states. While a worthwhile effort to predict if corporations will or will not cooperate with their home government, the focus on the hegemonic 'two dog race' makes it difficult to extend the model beyond that frame. However, the insight that high-value MNCs with a central position in the global supply chain are simultaneously crucial for the economic statecraft of their home states if they can be weaponised, as well as more likely to resist that weaponisation—as they have more to lose—is interesting (Chen & Evers, 2023, p. 202) and travels beyond the focus on bi-lateral rivalry. Gjesvik (2023, p. 723) goes a step further and maintains that the framework of weaponised interdependence 'rests on assumptions of alignment between the state and private companies' but it is actually more likely that 'the ability of states to mobilize their domestic companies is eroding in significant areas'.

Using a layered idea of agency, Choer Moraes & Wigell (2022, p. 32) contend that companies have three strategies at their disposal to preserve a 'measure of

autonomy in an economic environment marked by increased state (geoeconomic) intervention'. They identify three types of strategies for market players: First, 'business as usual', in which companies try to limit or push back against state interference in economic relations. Companies seek to discourage measures that balance dependence for fear of 'politicization' of economic relations. Second, 'one company, two systems', whereby companies realise they cannot control balancing dependence measures and seek to adapt their operations in order to play on both sides of the geoeconomic divide. Third, 'patriotic capitalism' where corporate actors either openly side with their governments or advocate the adoption of geoeconomic measures as a way of keeping their country's leadership in a given sector (Choer Moraes & Wigell, 2022, p. 42). All of these strategies have played out in the digital domain. While they are focused on the state, tech companies are increasingly also creating facts on the ground that states in turn have to relate to. We have seen this, for example, in the context of the war in Ukraine, where tech companies waded into the conflict explicitly choosing sides (Lilly et al., 2023), or more below the radar by increasingly capturing the market of the global subsea internet cable network that connects the continents (Kavanagh, 2023).

Informality and digital corporate autonomy

While much of IR theory and international law barely recognises transnational corporations as international actors (Broeders & Taylor, 2017), their relationship with government power and sovereignty plays a more significant role in recent literature. Srivastava (2022, p. 31) maintains that the contemporary sharp public-private distinction obscures the way in which states often work through private, non-state actors to exercise sovereign power. She develops ideal-types of public/private hybrids that highlight different degrees of formality and transparency of the relationship between governments and companies. Hybrid cooperation comes in more and less formal and publicly acknowledged shapes, which is also likely to be the case in geoeconomic policy. With the rising prominence of geo-economics, the relationship between states and corporations is likely to become more characterised by secrecy and obfuscation. A common form of geoeconomic policy is that of states *formally* coercing companies to comply with their interests and demands. This can, for example, be done through sanctions or import- and export controls. For governments there are differences between companies that are legally domiciled and companies that are outside the legal jurisdiction of a state. Only the most powerful states, like the US, will be exerting influence beyond their 'own' companies through (the threat of) secondary sanctions and extraterritorial penalties (Demarais, 2022). But, as Gjesvik (2023, p. 727) contends, even states with a powerful, nodal position in the network still have to negotiate their position with companies in that network and/or operating on that network.

More importantly for this paper is the idea of an *informal* alliance between companies and state authorities. This is usually between companies and their home countries where sometimes public and private interests align. Silicon Valley companies have often been seen as an integral part of America's soft power (Nye, 2011), but also as willing accomplices in US espionage efforts. More recently, they are increasingly contributing to Pentagon projects in the field of (military) AI and cloud services. In the case of China, Big Tech companies like Huawei are often considered to be

tethered to the Chinese government. Moreover, the rise of private actors with global interests and commensurate capabilities—their infrastructural and 'agentic' capacity to shape norms is discussed in the next section—has coincided with and contributed to the rise of informal governance mechanisms. Informal mechanisms lack a treaty—or charter-based constitutive instruments, and function in the absence of a permanent secretariat. They often take the form of multistakeholder arrangements or ad hoc coalitions that offer private actors a seat at the table, as interlocutors alongside states.

Geoeconomic frameworks in the near and medium-term are likely to be influenced by informal governance arrangements for two reasons. Firstly, even as nations, especially advanced economies, revisit their approach towards industrial policy and proclaim geoeconomic ambitions, they will still be mindful of their existing formal commitments at the World Trade Organization (WTO) and other trade arrangements. In the interim, informal arrangements can help prepare the normative ground to reorient principles and frameworks in existing international economic relations (Claussen, 2021). This is especially true of economic security concerns (Paulsen, 2024). Secondly, it is no exaggeration to say that technological advancements are at the front and centre of contemporary geoeconomic debates. States not only want to ensure that they maintain or secure a distinct advantage in the use of emerging technologies such as cyber capabilities and AI, but also to prevent their adversaries from accessing sensitive technologies and attendant production resources. The informal US-Japan-Netherlands agreement on semiconductors, analysed in this paper, is a prime illustration of such a geoeconomics-driven framework. What's notable is that informality is not only on the rise but also 'pervasive' in domains of high politics such as the international security and proliferation threats posed by digital and AI-enabled technologies (Sukumar et al., 2024). Many such informal initiatives are multistakeholder in character and, indeed, necessitate cooperation from globally influential private actors to meet their objectives. They enhance the standing and capacity of private actors to shape state behaviour and compliance with emerging geoeconomic frameworks, and informality therefore is a key driver of digital corporate autonomy.

Infrastructural power and digital corporate autonomy

The focus in this paper is on what the corporate autonomy of digital MNCs consists of, how they use that autonomy to chart their own course to serve their business and political interests, and how they navigate the geoeconomic demands that states place on them. One of the main geo-economic battlefields is that of (emerging) digital technology and the 'cyber commons' they have created (Matania & Sommer, 2023). Many of the transnational companies that populate the digital domain wield vast financial and political power. These companies have great

> 'Freedom to operate as they see fit and to design cyberspace in line with their business, moral, social, economic and political visions. Yet, those seemingly business-oriented decisions by companies have major implications for the national security of almost all the countries in the West and beyond'. (Sommer et al., 2023, p. 148)

Private decisions have public consequences, even though these companies may not have, prioritise or follow public values (Taylor, 2021). Especially Big Tech

companies are sometimes discussed as 'state-like' actors (Harvey & Moore, 2023; Sommer et al., 2023). In terms of economic interdependence, the stakes are arguably higher in the digital domain than anywhere else. The potential leverage for states is high, but the economic actors involved are powerful. That makes the digital sphere a best-case scenario to study digital corporate autonomy as it is home to some of the richest and largest global corporations that are used to navigate different political systems. Many of these companies are also infrastructural companies at a global scale and/or hold key positions in global supply chains, which means they can leverage 'infrastructural power'.

The internet is a global network created, supported and expanded by a mix of private, public and non-profit entities from all corners of the globe. It is these kinds of socio-technical global complex systems and asymmetric network structures that Farrell and Newman (2019, 2023) have in mind when they talk about weaponizing interdependence. The digital economy—in the widest sense—is a dense web of transnational global supply chains at the levels of products, services and infrastructure. Moreover, in the digital realm, civil and military technologies—and with that, civil and military economies—have become increasingly blurred. All modern technology requires semiconductors, and all breakthroughs in general AI or Quantum research will ultimately benefit both the civil and the military domains. In other words, interdependence and blurred lines between civil and military technology are a key feature of the digital domain, at a time when countries seek to disentangle for reasons of geopolitics and national security. Importantly, in this global digital domain, new corporate actors are in positions of immense power. Massive globally operating corporate entities—Big Tech—have shaped the global digital economy, the underlying digital infrastructure and global supply chains, and the way people interact in the digital domain (Gjesvik, 2023; Matania & Sommer, 2023; Sommer et al., 2023; Srivastava, 2023; Srnicek, 2017; Taddeo & Floridi, 2017; Taylor & Broeders, 2015). Digital companies—broadly speaking—are now the largest publicly traded companies and, even though the US is still leading, the field is diversifying in terms of the home countries of 'nodal' companies.

The nodal status of these big internet and tech companies connects well with the recent 'infrastructural turn' in IR literature (Abels, 2024; Bueger et al., 2023; De Goede & Westermeier, 2022; Gjesvik, 2023). In opposition to the rather instrumental IR view of infrastructures, much of this literature calls for a recognition of the 'agentic capacity' of infrastructures themselves (De Goede & Westermeier, 2022, p. 2). Bueger et al. (2023, p. 2) discuss different strands of infrastructure theories but all agree—'implicitly or explicitly—that infrastructures underpin, create, and maintain the structures of international politics'. While most of these theories locate agency in the infrastructures *themselves*, we contend that the power of infrastructure augments, and consolidates, the power and corporate autonomy of big digital companies. Shen and He (2022, p. 2375) argue that the 'rise of private-owned, profit-oriented infrastructuralized platforms on the global Internet' is accompanied by an 'unprecedented corporate control over the basic infrastructure of the global political economy'. Plantin et al. (2018) even speak of a 'platformization' of infrastructures and an 'infrastructuralization' of platforms. Increasingly big platforms build, supply and control key digital infrastructures like the subsea cable networks (Kavanagh, 2023; Liebetrau & Bueger, 2024), satellite infrastructure (Abels, 2024) and global cloud infrastructure (Blancato & Carr,

2024). Abels (2024, p. 3) warns that 'geopolitically relevant infrastructures owned by transnational businesses' have been severely understudied so far. He contends that the geoeconomic interests of these companies are *juxtaposed* with, rather than subordinate to, state interests. The notion of juxtaposition does not imply that states and businesses necessarily compete as their relationship in this line of thinking is dynamic and reciprocal, not strictly hierarchical. To Abels (2024, p. 9) this means that businesses in infrastructure policy have 'their own, partly independent motives and strategies that vary between alignment and autonomy'. In this paper we contend that the corporate autonomy of digital infrastructural companies is not a strategy, but a core 'characteristic' that allows them to decide between alignment and contention for their own business and political reasons.

Digital corporate autonomy

This paper uses the concept of digital corporate autonomy to highlight the economic and political power that digital companies can bring to bear in the geo-economic sphere. While the word autonomy—in the sense of self-governing entities—underlines corporate agency (often overlooked in IR literature), it does not discount the fact that businesses have to contend with other actors. Just as the European Union (EU)'s strategy of 'strategic autonomy' should not be equated with a wish for autarky (Timmers, 2021), digital corporate autonomy is about having the economic and political power to make autonomous choices: Navigating, defying and challenging—as well as complying with—the constraints that other actors put in place. The nodal status of these corporations greatly amplifies that autonomy as they are able to incorporate and put to use their 'infrastructural power'. Especially in situations of conflict and geoeconomic tensions, this autonomy may seriously influence a state's geopolitical ambitions, for better or worse, as already seen in the context of the war in Ukraine. Recognising corporate autonomy means that companies will do more than navigate the wishes and demands of states. It also means that states will increasingly have to negotiate and navigate corporate wishes and demands. Perhaps even more so in the future, as the infrastructural power of these companies grows, rivalling that of—especially smaller—states. However, the exercise of corporate autonomy will not always be clearly visible as some state-company arrangements will be secret and informal.

Digital corporate autonomy asserts that companies make self-governing choices. In the context of geopolitical tensions and conflicts, it allows companies to engage with a conflict *irrespective* of state demands and/or wishes. It may even amount to 'taking sides' in a conflict affecting their business behaviour and bringing companies directly into the mix of political or military conflict. These incursions, in what states usually regard as the ultimate state affair, may be met with (tacit) approval or more mixed reactions from state authorities. In the analysis of the cases, we examine what digital corporate autonomy looks like, and how states and companies interact and move on the spectrum between cooperation and coercion and that between formal and informal interaction.

Digital corporate autonomy in the Ukraine war

Scholars have already noted that the war in Ukraine illustrates the importance of non-state actors in the international system (Bassett, 2024; Grossman et al., 2023).

Technology companies, in particular, have played an outsized role, encroaching into traditional areas of statecraft. It is perhaps the best example of Susan Strange's prediction that, as a result of rapid technological advancement, in conflict, states would increasingly seek allies among foreign companies, rather than other state actors (Strange, 1996, p. 9). Underscoring their nodal status, no state could have provided Ukraine with the kind of services it needed—cloud storage, threat intelligence, satellite communications, and artificial intelligence (AI) for battlefield targeting—at the speed at which they were required. These companies are both the creators and the custodians of 'the cyber commons', swathes of which are proprietary in nature (Matania & Sommer, 2023). Indeed, Ukraine showcases how the immense infrastructural power of technology corporations and informal initiatives at the broader strategic level of corporate operations, as well as between company executives and government representatives, make these companies key autonomous players in an international conflict.

The actions of Microsoft and Amazon have plainly demonstrated their capabilities and infrastructural power. According to Brad Smith, Microsoft's CEO, and Mikhail Fedorov, Ukraine's Digital Transformation Minister, the company is on the 'front lines' of the war (Smith, 2022a). Prior to the Russian invasion, government operations were conducted from servers located in major government buildings in Kyiv. In the event of a missile strike on the buildings, these operations would have been entirely paralysed (Microsoft, 2023). Microsoft was key in ensuring that the data of all Ukrainian government entities, including the military, schools, universities, and hospitals would be moved free of charge to the public cloud, supported by infrastructure distributed across various European data centres, in a service worth US$540 million (Ostiller, 2023). Companies like Kernel, Ukraine's largest producer of sunflower oil; KredoBank, a major bank; and Ukrenergo, a principal energy supplier, are all dependent on Microsoft's cloud to function and continue to conduct business (Microsoft, 2023).

Amazon reacted similarly. Using small data storage units—so-called Snowball devices—it helped the Ukrainian government physically transport millions of gigabytes of critical government data out of Ukraine and into its cloud infrastructure (Amazon Staff, 2022b). Amazon's services were also extended to private entities, including PrivatBank, Ukraine's largest bank, which uses Amazon Web Services to house hundreds of applications and petabytes of client data (Amazon Staff, 2022b). Overall, Microsoft and Amazon have catalysed a monumental digitisation of Ukraine's government. In recognition of their support, in July 2022, Ukraine's government awarded both companies peace prizes for their provision of cloud services to the country (Guest, 2023).

Microsoft and Amazon's access to data through their widely used products and services means that the companies hold unique insights into the cyber threat landscape, and, in turn, their provision of threat intelligence to Ukraine has been key to buttressing the country's cyber resilience. For example, in the early stages of the war, Microsoft alerted the Ukrainian government to a malware campaign—dubbed FoxBlade—that was threatening government systems and worked with it to stop the malware's spread. Soon after, Microsoft established a 24/7 encrypted communications channel to enable faster information sharing with Ukrainian authorities (Lilly et al., 2023, p. 75). Amazon has also shared threat intelligence with aid organisations active in Ukraine (Amazon Staff, 2022a). Indeed, one of the most striking

aspects of Ukraine's digital war has been the speed of information sharing between different entities—private, government, and non-government—involved in the conflict. Overall, the companies have been credited with providing Ukraine with the information and tools to defend itself from over 800 Russian intrusions (Zetter, 2022).

Crucial to Ukraine's war effort has also been a third company, Palantir Technologies, considered controversial by privacy advocates. Its software uses AI to analyse data and imagery from satellites, drones, and ground reports, aiding Ukrainian commanders with battlefield targeting, all free of charge. Ukrainian agencies including the Ministries of Defence, Economy, and Education are also using it for documenting war crimes, de-mining land, and handling refugee movements. Palantir is effectively 'embedded' in the day-to-day work of Ukraine's government (Bergengruen, 2024).

A fourth company heavily involved in Ukraine is SpaceX's Starlink. Its donations to the country, according to its CEO Elon Musk, have amounted to US$80m (Isaacson, 2023). Underscoring Starlink's infrastructural power, the Ukrainian government and military have been wholly reliant upon the company's services for satellite communications, which are 'the essential backbone of communication on the battlefield' (Mykola, a soldier in Ukraine's signal corps, quoted in Farrow, 2023). Starlink's 42,000 terminals have been crucial in helping Ukraine make gains in the war (Horton, 2023). The company's engineers have proven themselves to be the only ones capable of defeating Russian jamming (Isaacson, 2023). Musk is now considered to be the 'dominant power' in strategically-significant satellite internet technology, with no government able to replicate the services provided by Starlink (Satariano & Frenkel, 2022).

However, Ukraine's experience with Starlink has been far from plain sailing, demonstrating the darker side of autonomous corporate behaviour in the operation of a crucial infrastructure in a conflict zone. The company restricted the use of its technology on at least three occasions. In September and October 2022, Ukrainian troops found that Starlink was geofenced and did not function past the front lines as they tried to liberate Russian occupied eastern territories in Kherson, Zaporizhzia, Kharkiv, Donetsk, and Luhansk (Farrow, 2023; Marquardt, 2022). Around the same time, Musk refused to enable Starlink along the coast of Crimea in order to prevent the Ukrainian military from targeting the Russian naval fleet at Sevastopol with drone submarines (Isaacson, 2023). He expressed the personal opinion that enabling the Ukrainian military in this way would lead to a significant escalation in the war (Nawfal, 2023). In February 2023, Starlink again imposed limitations on using its technology for offensive purposes, particularly drone strikes (Foust, 2023). Musk then even tried to propose peace plans for Ukraine (Satariano & Frenkel, 2022).

The unique ownership structure of SpaceX means that Starlink's role in Ukraine is particularly susceptible to the fluctuating opinion of its CEO with very little accountability (Giles, 2023). Musk's volatility, in turn, is spurred at least partially by his reported regular contacts with Russian officials and his other companies'—particularly Tesla's—dependence on China, which opposes the provision of Starlink to Ukraine (Farrow, 2023). Moreover, according to US intelligence reports, Russia has been developing capabilities to sabotage the service (Horton, 2023). China has also previously threatened to take down Starlink satellites (Olcott & White, 2022).

Starlink's nodal status meant that SpaceX was able to pressure the US government into agreeing to pay US$145m for the Ukrainian military's use of the technology.

Exposing the extent to which the company is able to influence government decision-making, a US senior defence official explained that the Department of Defense (US DoD) 'started to get a little panicked … [as] Musk could turn it [Starlink] off at any moment', which would have presented substantial operational problems for the Ukrainian military (quoted in Farrow, 2023). It was only after the story leaked, provoking a public backlash, that Musk appeared to withdraw the request and eventually came to an arrangement with various government agencies, including the US DoD, to share the financial burden of maintaining Starlink and increase its services to the Ukrainian military in the form of Starshield (Isaacson, 2023).

Importantly, the creeping involvement of technology companies in Ukraine has mostly come about through informal initiatives and meetings between company executives and Ukrainian government representatives. For example, on the day Russia invaded Ukraine, Liam Maxwell, head of government transformation at Amazon Web Services, met with the Ukrainian Ambassador Vadym Prystaiko in London to 'sketc[h] out with pen and paper' what data was most crucial to move into the Amazon cloud (Mitchell, 2022). Microsoft even held a joint press conference at the Web Summit technology conference between its president Brad Smith and Ukraine's digital transformation minister Mykhailo Fedorov, broadcasting its 'digital alliance' with Ukraine (Smith, 2022b). The fast action to stop the spread of FoxBlade came about after direct cooperation between Microsoft and Anne Neuberger, the US Deputy National Security Advisor for Cyber (Sanger et al., 2022). The CEO of Palantir, Alex Karp, personally travelled to meet Ukrainian President Zelensky in Kyiv three months after Russia's invasion, to propose Palantir help Ukraine 'in ways that allow David to beat a modern-day Goliath' (quoted in Bergengruen, 2024). Palantir has subsequently been sending engineers to Ukraine on a regular basis and has also hired a number of local employees to work with government officials.

The arrangements between Starlink and Ukraine have also come about through informal interactions. Fedorov first appealed to Musk for support on Twitter (now X), and two days later posted a photo of satellite dishes entering Ukraine (Bergengruen, 2022). Further discussions of Starlink's support happened over Zoom calls directly between Musk and Zelensky, with Musk haphazardly making decisions over time on increasing Starlink's provisions to Ukraine (Isaacson, 2023). Much of Musk's later volatility, as discussed earlier, came about as a result of informal contacts between him and government leadership in Russia and China. Tensions between Musk and Ukrainian government officials—most notably Ukraine's ambassador to Germany—then publicly unfolded on Twitter, and informal US diplomacy was later required to reach a new agreement with Starlink.

Informal corporate involvement in the Ukraine war has also been enacted through 'self', 'voluntary' or 'corporate' sanctioning (Chief Executive Leadership Institute, 2024; Nicholls, 2022; Parella, 2023). Companies that have engaged in this practice, have gone beyond what is legally required of them in adhering to state sanctions and export controls. For instance, while Microsoft stopped many aspects of its business in line with government sanctions, the company also suspended all new sales of its products and services in Russia (Smith, 2022c). Google, Apple and Meta too have taken a range of actions beyond those stipulated by government through their digital infrastructures, such as blocking access to Russian media outlets, limiting online payment functionalities (Google and Apple) as well as restricting Maps (Apple) (Nicholls, 2022; Timmins, 2022). Halting the sale of not only

military and dual-purpose chips, but also consumer-focused chips, both Intel and AMD implemented blanket approaches in adjusting their sales (Alcorn, 2022).

By restricting their digital services and/or technological components or products beyond that required by law, these companies have voluntarily worked to limit Russia's operational capabilities vis-à-vis its war in Ukraine. In doing so, these companies have informally positioned themselves geopolitically—in this case aligning their activities with the interests of the west. In some instances, this informal alignment has been explicitly communicated—for example, by Microsoft and Intel, who have directly deplored Russia's invasion of Ukraine (Smith, 2022c; White, 2022). In others, it has been implicit—for example, while Apple has taken measures against Russia, it has not specifically condemned the country itself (Higgins, 2022). As these examples demonstrate, informal initiatives at the broader strategic level of corporate operations as well as between company executives and government officials, have been an important feature of corporate involvement in Ukraine.

There are multiple implications of digital corporate autonomy in Ukraine. The most obvious one is Ukraine's dependency on private sector goodwill—the result of a precarious cost-benefit analysis performed by the companies themselves—for national security provision. Another ramification is from an international legal standpoint. Because the companies are demonstrably taking sides in the war, if their engagement in defensive activities is interpreted as involvement in hostilities, then they could be seen by Russia as participants in the conflict and therefore legitimate military targets (Zetter, 2022). This issue is intensified by the fact that the companies are understood to be helping manage not only civilian services but also military assets, for example, the protection of military networks and storage of military data in the cloud (Vignati, 2022).

There are already signs that Russia is retaliating against companies that have taken Ukraine's side in the war. It blocked Microsoft from participating in the Open-Ended Working Group on Cybersecurity at the United Nations (UN) (Lilly et al., 2023, p. 79). Russian officials have also threatened that western commercial satellites could become military targets, provoking the US to promise a reaction if Russia attacks its infrastructure (Reuters, 2022). In response to Meta's decision to permit some expressions of anti-Russian sentiments on its platform, the Kremlin officially labelled the company an extremist organisation—resulting in the freeze of its assets in Russia—and banned access to Facebook and Instagram (Tidy, 2022).

Further repercussions can be found in the companies' impact on Ukrainian digital sovereignty. Spurred by the Russian invasion, in February 2022 Ukraine changed the law so that government data and certain private data no longer needed to be stored in servers on Ukrainian territory, allowing crucial data to be transferred to cloud infrastructure (Mitchell, 2022). Since cloud computing services are provided only by foreign private sector companies—specifically Amazon, Microsoft, Google, and Alibaba (Schroeder & Dack, 2023)—in passing the law and working with Microsoft and Amazon to transfer and store its digital assets, Ukraine ceded a substantial level of control over its critical data to American companies with servers located extraterritorially, under a legal regime different to its own. Ukraine thus effectively traded a proportion of its digital sovereignty for cyber resilience (Editors, 2022). These actions also have sovereignty implications for countries hosting the servers (e.g. Poland), as they become potential Russian targets (Stupp, 2022).

A final implication can be found in what the companies likely see as their greatest gain from their involvement in Ukraine: Data. As Fedorov himself put it, Ukraine has become 'the world's tech RandD lab' (quoted in Bergengruen, 2024). Technology companies have been able to gather enormous amounts of data to train and mature their algorithms, and hone their product offering in a war setting. In other words, they are further increasing their infrastructural power. Learning from the Ukrainian experience, other governments, including Taiwan and the US, have already started working with these companies to prepare for the eventuality of future wars (Bergengruen, 2024). But, unlike government-funded research laboratories, technology corporations are not accountable to the general population, but to shareholders. In a free market, it is likely that at least some of their commercial tools will become available for use by Western adversaries. What we therefore see is a feedback loop, whereby the involvement of corporations in Ukraine increases their infrastructural power, making them indispensable allies in future geopolitical crises for both sides. While outside the scope of this study, it is important to note the potentially transformative implications of private sector algorithmic innovation for the conduct of war and its vast ethical and legal implications (Gould et al., 2024; Taddeo, 2024).

Operationalising economic security: ASML and the US-Netherlands-Japan ad hoc semiconductor coalition

'We have a special position. So that gives us a place at the table. And I have a sense that people are listening [to us]' (Kasteleijn, 2024). These words from Peter Wennink, outgoing CEO of the Dutch semiconductor company ASML, encapsulate the notion of digital corporate autonomy in the articulation and implementation of geoeconomic frameworks. Wennink was referring to ASML's 'special position' not only in the context of its discussions with the Dutch government over issues such as labour, housing, and taxation, but also against the backdrop of a semiconductor agreement between the US, Japan, and the Netherlands that put the company in the crosshairs of international politics. In January 2023, these three states agreed to jointly impose restrictions on the export of advanced semiconductor technology by their companies to foreign actors. The measure was ostensibly directed at constraining China's capacity to pursue advancements in semiconductor-driven, frontier technologies such as AI, as well as catalyse innovations in its own semiconductor industry. The coalition reportedly agreed to restrict the export of lithography equipment integral to manufacturing chips and possibly covers chip design software as well (Swanson, 2023). Multilateral export control regimes are hardly novel in global governance. The US-Netherlands-Japan 'agreement', however, requires closer scrutiny for its form and character, and speaks directly to the challenges of coercing states and inducing compliance from powerful private actors such as ASML for geoeconomic purposes.

Firstly, it is reportedly best characterised as an 'understanding' rather than a 'formal deal', according to US officials (Haeck et al., 2023). The idea behind this US orchestrated informal initiative, is that all three countries, which control critical components in the global semiconductor supply chain, coordinate their domestic policies to limit sensitive exports to China. In other words, the trilateral agreement is non-binding but paves the way for domestic legislation that binds industry

players. Secondly, the arrangement is in the form of an ad hoc coalition of state actors rather than through institutionalised channels of cooperation. Unlike say, the Wassenaar Arrangement—an export control regime (with a permanent secretariat) on sensitive technologies based also on voluntary commitments by states—the semiconductor restrictions do not appear to be driven by regular institutionalised cooperation or dialogue (Haeck et al., 2023). Thirdly, the arrangement itself is a secret. Indeed, its existence can only be deduced from media reports citing unnamed government officials and circumstantial evidence, such as the Dutch and Japanese imposition of domestic semiconductor export controls in the months ensuing it. Neither country's export controls make any reference to the trilateral deal (Inagaki & Lewis, 2023).

These attributes of the US-Japan-Netherlands arrangement on semiconductors are not altogether unique. In 1984, the US similarly steered the creation of an informal and secretive 'Safeguard Plan' with Japan and Canada to limit the export of supercomputers to third-party states (Johnston, 1998). The deliberations of the Wassenaar Arrangement too are kept confidential (The Wassenaar Arrangement, n.d.). However, there is an important difference between these non-proliferation arrangements and the trilateral semiconductor deal in that the latter is driven primarily by economic security considerations. The new semiconductor coalition seeks to generally ensure that China does not become a leader in the design and manufacture of chips, an outcome that could result in many countries becoming heavily dependent on Chinese technologies in most domains of modern economic activity. In September 2022, a month before the US government announced its export controls, National Security Advisor Jake Sullivan argued that the US must 'maintain as large of a lead as possible' on 'foundational […] technologies, such as advanced logic and memory chips' (Sullivan, 2022). Sullivan made his comments even as the US was in the middle of its diplomatic push to forge the trilateral coalition.

US efforts to stitch this coalition together have not been easy, and speak to the challenges of going it alone. The Netherlands has generally supported the US in its geoeconomic goals and endorsed the need to have 'sovereignty and self-confidence [in] vital technologies' (Sterling, 2023). However, as Rasser and Wolf (2022) note, the economic considerations that motivate the US government's approach to export controls were 'too indirect a threat' for the Netherlands to consider imposing unilateral sanctions on the export of advanced semiconductors used 'overwhelmingly […] in commercial products'. They also note that Japan had 'no incentive to move forward' with export controls without Dutch commitment. The Netherlands is a critical cog in this arrangement because of the role and influence of one company: ASML. The geoeconomic objectives of the plan have been challenged by ASML, which has flexed its 'infrastructural' muscles, pushing against the informal framework to pursue its objectives as an autonomous economic actor.

ASML is one of the few global manufacturers of Deep Ultraviolet Lithography (DUV) machines, and the sole purveyor of advanced Extreme Ultraviolet Lithography (EUV) equipment, both of which are needed to manufacture high-computing chips of ever-decreasing size (The Economist, 2020). ASML has announced it intends to comply with Dutch export controls that were announced following the creation of the ad hoc coalition (ASML, 2023). However, the company has also communicated to states that it intends simply to follow the 'letter of the agreement', or in other words, only limit the sale of the most sensitive or

advanced lithography equipment to China (Koc et al., 2024). Indeed, Chinese entities began swiftly concluding purchases of 'more mature' lithography equipment with ASML prior to Dutch licensing restrictions taking effect, prompting the US to exert pressure both on the Dutch government as well as the company to stop sales immediately (Koc & Jacobs, 2024). The Dutch approach in turn has been strongly influenced by ASML's interests, with its current CEO saying 'there will be more push-back' against the trilateral deal, with the claim that the deal was about national security becoming harder to maintain (Sterling, 2023).

The former co-president of ASML has said that one could 'openly question whether the Dutch government has effectively leveraged its position'. 'In the long run', he said, 'I do dare say that an export freeze to China is not going to help us' (Van Leemput, 2024). What is the source and scope of ASML's agentic capacity that allows it to pushback against this informal arrangement? Firstly, with ASML being an exclusive manufacturer of lithography equipment, it can singularly move the global semiconductor market. While the US has levers of concrete control that it can exercise against ASML—including finance, supply chain, and talent restrictions (Malkin & He, 2024)—the company is so central to global chipmaking that the future of critical American industry players (e.g. Intel) are all directly or indirectly dependent on it. So, the US too has to approach its policies with a fair degree of calibration.

Secondly, this is not the first time that ASML has waded into geoeconomics. In 2019, ASML bought another Dutch company, Mapper, which used an alternative technique to manufacture lithography equipment. ASML bought the company not because it was interested in the technology—in fact, ASML had no use for it and repurposed the technique for another aspect of its operations—but because the Dutch and US governments did not want the financially troubled Mapper to fall into Chinese hands (Hijink, 2023). In this scenario, ASML exercised its digital corporate autonomy to *favour* geoeconomic goals because it had the financial wherewithal and more importantly market competence to make such an acquisition. With the ability to shape market trajectories in this manner, i.e. through corporate manoeuvres outside of its manufacturing prowess, ASML has also demonstrated its ability to channel political pressure.

Finally, ASML has significant bargaining power against the Dutch government as a source of frontier technological advancement, revenue, and national prestige for the Netherlands. For some time, ASML and the Dutch government have been engaged in negotiations over the availability of foreign talent and affordable employee housing in Eindhoven, the company's headquarters. In 2024, the Netherlands allocated US$2.5 billion (bn) to boost infrastructure and educational resources in the Eindhoven region to ameliorate ASML's concerns and prevent it from relocating major operations abroad (Government of the Netherlands, 2024). These issues may seem a remit of domestic policy, but they are deeply entangled with geoeconomics. ASML executives have spoken of the need to access foreign labour and commercial markets in the same breath, as part of the company's desire to maintain its competitive edge (Eppinga, 2023). The presence of Chinese students in Eindhoven University of Technology, a 'feeder' educational institute for ASML in which the company has made major investments, has become a source of major political controversy. In 2023, the US ambassador flagged the 'large number' of Chinese students at the institute with the university's president, illustrating how local issues of education and recruitment are intertwined with geoeconomic

considerations (Koc, 2024). As domestic and international issues become ever more fused, ASML too is arguably able to leverage issues in discussions with the Dutch government. Moreover, in 2025 ASML hired Bruno Le Maire as strategic advisor to its board, to safeguard its interests in Europe. Le Maire is a former diplomat and politician, who, during his tenure as French minister of Finance, challenged the US government and companies like Meta and Apple. His experience will help ASML articulate and channel its own geoeconomic position (Waarlo, 2025).

The question remains whether ASML has indeed been able to pursue its autonomous interests in the shadow of this trilateral arrangement. The US has had to unilaterally ratchet up the stringency of its own sanctions in the aftermath of the deal (Hijink, 2023). At the time of writing, the export of any advanced semiconductor equipment that uses American components, is restricted by the US government, which also affects ASML. Dutch policymakers and politicians have meanwhile bristled against increasingly severe US restrictions (Kasteleijn, 2024). Dutch officials even advised their US counterparts to reach out to ASML directly to limit any sales before January 2024 (Kasteleijn, 2024), indicating the company's autonomous agency as well as the limits of their own influence. Any further joint restrictions imposed on China should 'watch out very specifically for the economic interests of ASML', Dutch Prime Minister Dick Schoof has stated (Reuters, 2024). The Dutch government has also sought to shore up support for the coalition's export control measures within the EU, because it wants to prevent European suppliers from catering to Chinese demands—an outcome that would weaken not only sanctions but the global market share of ASML itself (Van Gerven, 2023).

Finally, the form and character of the US-Netherlands-Japan semiconductor initiative arguably allowed for a powerful corporate actor like ASML to exert its influence beyond that possible in closed, multilateral settings. The trilateral 'understanding' had to be informal in nature, arguably to preserve room for flexibility in the implementation of domestic measures within these three states. Just as importantly, an arrangement that is primarily economic in character must consider the existence of formal, multilateral commitments that the US, Japan and Netherlands have already made on international trade. Unsurprisingly, China has invoked the WTO dispute settlement mechanism both in response to the October 7 US export controls, and the purported creation of the ad hoc coalition (Aizhu & Wang, 2023; World Trade Organization, 2022). Similarly, the arrangement is secretive arguably because its parties not only want to be bound by such arrangements but also do not wish for it to affect their economic relations with China on other issues. Economic interdependence can be weaponised, but its consequences and potential spillover effects may not be fully in control of the 'weaponisers'. Secret negotiations and unofficial announcements offer room for plausible deniability, limit scope for tit-for-tat retaliations by say, a China-led coalition, and leave no possibility for a legal assessment of the document, if one exists. China's request for the coalition to report its plans to the WTO reflects its counter-strategy: Were the WTO dispute settlement bodies to find the coalition's measures to be violative of WTO commitments, China would be free to adopt proportional countermeasures in any domain of trade.

Its secrecy and informality have, however, focused discussions about the semiconductor deal on the technological infrastructure that is intended to be restricted, which makes ASML the centrepiece of the conversation. Debates on the arrangement are less about states' legal obligations, and more about the scope of the

measures themselves. For example, the sanctions are considered to have become more restrictive since 2023, because DUV exports are also now covered under it. ASML may be the key player manufacturing DUVs and EUVs, but it is easy to forget that an entire supply chain is also implicated through such measures. The focus on the ultimate infrastructure—the finished product, i.e. lithography equipment—attracts heightened political attention on the Dutch company. But as this section has shown, ASML too can, and has, used its importance to the geoeconomic deal, to highlight its business interests.

Conclusion

While IR based geoeconomic frameworks tend to focus on state-to-state competition and coercion and consider companies as subordinate and instrumental, the empirical reality of 'doing geo-economics' unfolds as much at the level of companies as it does at the state level. In this paper, we argue that big technology companies have significant 'digital corporate autonomy'. We build the notion of digital corporate autonomy firstly, on the recent literature on infrastructural power, arguing that the power ascribed to infrastructures themselves transcends to the corporations that run large digital infrastructure or take up nodal positions in international digital supply chains. The second pillar, supporting the notion of digital corporate autonomy, is the informalisation of international relations that grants corporations more room to manoeuvre and 'juxtaposes' (Abels, 2024) their own corporate interests with state geoeconomic interests. In the current age, the role of tech companies is central as digital technologies are integral to almost all aspects of economic, social, political and military life. Moreover, digital empires are being built by internet companies that boast global userbases of billions and financial resources surpassing that of many countries, while other tech companies sit at crucial intersections of global supply chains, such as semiconductor manufacturers like NVIDIA and ASML. To understand digital corporate autonomy in empirical reality this paper analysed two cases.

The autonomous behaviour of tech companies in the context of the war in Ukraine reveals that a number of—primarily, but not exclusively—American tech companies have aligned themselves with the Ukrainian cause at a very deep level. Even to the point that some commentators began to wonder about their non-combatant status. Their infrastructural power—cloud operation, satellite infrastructure, network analysis—were instrumental in their cooperation with the Ukrainian government, which in most cases is open to public view, but not transparent in terms of the scope and depth of their cooperation. The informality also extends to relations with their home government. As far as is known, the US government did not 'request' the type of aid that Microsoft and Amazon provided to Ukraine, but did step in informally when Starlink CEO Elon Musk, unilaterally curtailed the use of his satellite infrastructure to align with his personal ideas of geopolitical necessity and business interests. Informality and infrastructural power explain why these companies are able to intervene but do not explain why they do so. While intrinsic motivation and expected reputational gains provide some insight, there are also gains that are more clearly aligned with 'business as usual'.

The second case is set against the background of the rising geopolitical and geoeconomic tensions between the US and China and highlights the role of ASML, a Dutch company with a strategic, nodal position in the global supply chains for

semiconductors. The American initiated US-Netherlands-Japan 'agreement' to restrict Chinese access to high end semiconductors is informal—even secret—and creates its own dynamic in geoeconomic policymaking and digital corporate autonomy. While there is no public document to scrutinise, the (scarce) public reactions from, for example, the Dutch government and ASML, indicate, at best, a reluctant compliance with American wishes. ASML basically indicated that it would follow the letter of what is a secret arrangement, trying to preserve business continuity as much as possible. ASML's nodality works in two ways: It makes the company vital for US geo-economic policy making, but also exposes American industry's dependence on the company, augmenting its leverage. The nodality of ASML—also vis-á-vis its own and the US government—and the informality of the agreement gives the company some room to manoeuvre and push back against the geoeconomic restrictions.

The cases highlight the relevance of digital corporate autonomy in geopolitical times and underline that geoeconomics cannot be studied in isolation from corporate behaviour. In the context of the war in Ukraine, digital corporate autonomy should carry a warning sign for western states, as there is likely to be a clear difference between their short term and long term appraisal of such corporate behaviour. From a western perspective, corporate autonomy in this specific conflict is relatively unproblematic, as it has a clear good and bad side. However, as this case has been uncritically applauded, it sets a precedent that will make it harder to criticise and condemn (western and non-western) autonomous corporate behaviour in less clear-cut future conflicts. In time, corporate autonomy will raise many more questions on the legal limits of corporate political and perhaps even military behaviour, but the concept underlines the importance of giving much more scholarly attention to corporate behaviour in the context of geoeconomic competition and policymaking.

The Trump administration has shifted the political context for *American* digital corporate autonomy as it emboldens US Big Tech companies to use the 'America First' movement to reformulate and aggressively push for their interests. The CEOs of many Big Tech companies were present at Trump's inauguration and were even seated in front of the designated cabinet ministers. Elon Musk has effectively dropped any distinction between politics and business by being part of Trump's inner circle, using his platform to influence politics abroad (in Germany and the UK, for example) while growing his business profits. Meta's CEO Zuckerberg did not lose any time in using the MAGA momentum to drop costly content moderation and announce that he will work with president Trump 'to push back on governments around the world, that are going after American companies and pushing to censor more'.[2] Under the banner of free speech—in an absolutist American version—Meta claims to 'fight censorship' but also urges Trump to go after the EU's competition policy, comparing its antitrust penalties to tariffs, saying that Brussels is 'screwing with' American industry (Hernandez-Morales, 2025). This is a highly aggressive form of the 'patriotic capitalism' strategy, emboldened by a belligerent US administration: So corporate autonomous behavior should also not be studied in isolation from government (geo) politics. However, especially for digital platforms like Meta and X, these policy shifts are not without risk as they serve a global user base spread over many jurisdictions that may not all respond favorably to an explicit US centered interpretation of free speech and capitalism.

Under the Trump presidency informality is likely to increase as well. The Biden administration had already taken a calibrated approach to export controls on ASML,

being mindful of close ties with the American semiconductor market. In the final days of the Biden administration, more Chinese chipmakers were brought under the ambit of US export controls, but the Netherlands and Japan were exempted from those additional restrictions (Freifeld & Shepardson, 2024). Clearly, the US prefers informal agreements with states and companies that have geoeconomic clout, away from the scope of formal controls and regulations. The turn to informal arrangements and 'deals' is true for US governments across the political spectrum, but it was especially notable during the first Trump administration (Bradley et al., 2023, p. 1284). While this Trump administration will be more aggressive in targeting Chinese competition, it will likely be sensitive to the pulls and pressures of American technology companies that rely on ASML equipment. Consequently, even as it gets further drawn into the thicket of geoeconomics and coercive arrangements, ASML may still retain its ability to exert autonomy and influence in various client markets. If nothing else, the start of the Trump administration shows that American big technology companies have no trouble recognizing political momentum that they can use to their own (perceived) advantage, while others recognise the political winds that need to be sailed.

Notes

1. See for example: Norris (2016); Choer Moraes and Wigell (2022); Gjesvik (2023); Chen and Evers (2023) and Abels (2024).
2. Video message of Mark Zuckerberg, 7 January 2025, see https://about.fb.com/news/2025/01/meta-more-speech-fewer-mistakes/.

Acknowledgements

This article was originally written as a discussion paper for a research seminar on 'Economic Security and Cyberspace: Politics, Policy and Practice' that took place in November 2023 in the Hague and was organised as part of the EU-funded EU Cyber Direct project and The Hague Program on International Cyber Security, funded by the Dutch Ministry of Foreign Affairs. The authors would like to thank the participants of that seminar for the lively discussion and their valuable comments and suggestions. We would also like to thank the organisers and participants of the conference 'The Political Economy of Cyber Conflict' that was held at ETH Zürich in October 2023 where we also presented an earlier version of the paper. Finally, we wish to thank the three anonymous reviewers of this journal whose substantial and insightful comments led to an extensive overhaul of the text and – in our view – a better paper.

Disclosure statement

No potential conflict of interest was reported by the author(s).

Funding

This work was supported by the European Commission [EU Cyber Diplomacy Initiative]; Ministerie van Buitenlandse Zaken [The Hague Program on International Cyber Security].

Notes on contributors

Dennis Broeders is Full Professor of Global Security and Technology at the Institute of Security and Global Affairs (ISGA) of Leiden University, the Netherlands. He is the Senior Fellow of The

Hague Program on International Cyber Security. His research focuses on the interaction between security, technology and policy, with a specific interest in international cyber security governance.

Arun Sukumar is Assistant Professor of International Relations at Ashoka University, India. His recent research highlights how multilateral institutions are evolving to address the security and governance of emerging technologies.

Monica Kello is a Lecturer in Cyber Security at the Department of War Studies, King's College London. Her research focuses on international cyber conflict and the strategic implications of new technologies.

Lise H. Andersen is a Postdoctoral Research Fellow at the Institute of Security and Global Affairs (ISGA) based at Leiden University. Her research focuses on the management of knowledge and expertise informing multilateral diplomatic negotiations, specifically in the scientific and technological space.

References

Abels, J. (2024). Private infrastructure in geopolitical conflicts: The case of Starlink and the war in Ukraine. *European Journal of International Relations*, *30*(4), 842–866. https://doi.org/10.1177/13540661241260653

Aizhu, C., & Wang, J. (2023, April 5). China urges stronger WTO monitoring of US-led chip export curbs. *Reuters*. https://www.reuters.com/technology/china-urges-wto-sift-us-led-chip-export-curbs-2023-04-05/

Alcorn, P. (2022, March 4). AMD and Intel Halt Processor Sales to Russia and Belarus Updated). *Tom's Hardware*. https://www.tomshardware.com/news/intel-amd-nvidia-tsmc-russia-stop-chip-sales-ukraine-sanction

Amazon Staff. (2022a, March 1). How Amazon is assisting in Ukraine. *Amazon*. https://www.aboutamazon.com/news/community/amazons-assistance-in-ukraine

Amazon Staff. (2022b, June 9). Safeguarding Ukraine's data to preserve its present and build its future. *Amazon*. https://www.aboutamazon.com/news/aws/safeguarding-ukraines-data-to-preserve-its-present-and-build-its-future

ASML. (2023, June 30). Statement regarding Dutch government's export control regulations. *ASML*. https://www.asml.com/en/news/press-releases/2023/statement-regarding-export-control-regulations-dutch-government

Baldwin, D. A. (1985). *Economic Statecraft*. Princeton University Press.

Bassett, L. (2024). Silicon shadow: The influence of big tech in Russo-Ukrainian cyber warfare. Cambridge Journal of Political Affairs, *8*(Easter), 70–104.

Bergengruen, V. (2022, March 15). 'It's our home turf.' The man on Ukraine's digital frontline. *Time*. https://time.com/6157308/its-our-home-turf-the-man-on-ukraines-digital-frontline/

Bergengruen, V. (2024, February 8). How tech giants turned Ukraine into an AI war lab. *Time*. https://time.com/6691662/ai-ukraine-war-palantir/

Blackwill, R., & Harris, J. (2016). *War by other means: Geoeconomics and statecraft*. Harvard University Press.

Blancato, F. G., & Carr, M. (2024). The trust deficit: EU bargaining for access and control over cloud infrastructures. *Journal of European Public Policy*, *2024*, 1–32. https://doi.org/10.1080/13501763.2024.2441418

Bradley, C., Goldsmith, J., & Hathaway, O. A. (2023). The rise of nonbinding international agreements: An empirical, comparative, and normative analysis. *University of Chicago Law Review*, *90*. https://live-chicago-law-review.pantheonsite.io/sites/default/files/2023-09/01_Bradley_ART_Final.pdf

Broeders, D., & Taylor, L. (2017). Does great power come with great responsibility? The need to talk about corporate political responsibility. In M. Taddeo & L. Floridi (Eds.), *The responsibilities of online service providers* (pp. 315–323). Springer.

Bueger, C., Liebetrau, T., & Stockbruegger, J. (2023). Theorizing infrastructures in global politics. *International Studies Quarterly*, *67*(4), sqad101. https://doi.org/10.1093/isq/sqad101

Chen, L., & Evers, M. (2023). 'Wars without gun smoke': Global supply chains, power transitions, and economic statecraft. *International Security*, *48*(2), 164–204. https://doi.org/10.1162/isec_a_00473

Chief Executive Leadership Institute. (2024, January 28). *Over 1,000 companies have curtailed operations in Russia – But some remain*. Yale School of Management. https://som.yale.edu/story/2022/over-1000-companies-have-curtailed-operations-russia-some-remain

Choer Moraes, H., & Wigell, M. (2022). Balancing dependence: The quest for autonomy and the rise of corporate geoeconomics. In M. Babić, A. D. Dixon, & I. T. Liu (Eds.), *The political economy of geoeconomics: Europe in a changing world*. Palgrave Macmillan. https://doi.org/10.1007/978-3-031-01968-5_2

Claussen, K. (2021). Trade's mini-deals. *Virginia Journal of International Law*, *62*, 315.

De Goede, M., & Westermeier, C. (2022). Infrastructural geopolitics. *International Studies Quarterly*, *66*(3), 33. https://doi.org/10.1093/isq/sqac033

Demarais, A. (2022). *Backfire: How sanctions reshape the world against US interests*. Columbia University Press.

Drezner, D., Farrell, H., & Newman, A. (Eds.) (2021). *The uses and abuses of weaponised interdependence*. Brookings Institution Press.

Editors. (2022, September 8). How Does War in Ukraine Impact the EU's Digital Sovereignty? *Directions*. https://eucyberdirect.eu/blog/how-does-war-in-ukraine-impact-the-eu-s-digital-sovereignty

Eppinga, A. (2023, September 6). ASML's CEO warns for impact of migration restriction and isolating China. *Innovation Origins*. https://innovationorigins.com/en/asmls-ceo-warns-for-impact-of-migration-restriction-and-isolating-china/

Freifeld, K., & Shepardson, D. (2024, December 3). Latest US clampdown on China's chips hits semiconductor toolmakers. *Reuters*. https://www.reuters.com/technology/latest-us-strike-china s-chips-hits-semiconductor-toolmakers-2024-12-02/

Farrell, H., & Newman, A. (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. (2021). Weaponized interdependence and networked coercion: A research agenda. In D. Drezner, H. Farrell, & A. Newman (Eds.), *The uses and abuses of weaponised interdependence* (pp. 305–322). Brookings Institution Press.

Farrell, H., & Newman, A. (2023). The new economic security state: How de-risking will remake geopolitics. *Foreign Affairs*, *102*, 106–122.

Farrow, R. (2023, August 21). Elon Musk's shadow rule. *New Yorker*. https://www.newyorker.com/magazine/2023/08/28/elon-musks-shadow-rule

Foust, J. (2023, February 9). Shotwell: Ukraine 'weaponized' Starlink in war against Russia. *SpaceNews*. https://spacenews.com/shotwell-ukraine-weaponized-starlink-in-war-against-russia/

Førland, T. (1993). The history of economic warfare: International law, effectiveness, strategies. *Journal of Peace Research*, *30*(2), 151–162. https://doi.org/10.1177/0022343393030002003

Van Gerven, P. (2023, January 16). Dutch demand Europe-wide implementation of semi equipment export controls. *BitsandChips*. https://bits-chips.nl/artikel/dutch-demand-europe-wide-implementation-of-semi-equipment-export-controls/

Giles, K. (2023, September 12). Tech giants hold huge sway in matters of war, life and death: That should concern us all. *Guardian*. https://www.theguardian.com/commentisfree/2023/sep/12/tech-giants-war-elon-musk-ukraine-starlink

Gjesvik, L. (2023). Private infrastructure in weaponized interdependence. *Review of International Political Economy*, *30*(2), 722–746. https://doi.org/10.1080/09692290.2022.2069145

Gould, L., Hoijtink, M., Jaarsma, M., & Davies, J. (2024). Innovating algorithmic warfare: Experimentation with information manoeuvre beyond the boundaries of the law. *Global Society*, *38*(1), 49–66. https://doi.org/10.1080/13600826.2023.2261466

Government of the Netherlands. (2024). *The Netherlands to invest €2.5 billion to strengthen business climate for chip industry in Brainport Eindhoven*. Government of the Netherlands. https://www.government.nl/latest/news/2024/03/28/the-netherlands-to-invest-%E2%82%AC2.5-billion-to-strengthen-business-climate-for-chip-industry-in-brainport-eindhoven

Grossman, T., Kaminska, M., Shires, J., & Smeets, M. (2023). *The cyber dimensions of the Russia-Ukraine war*. ECCRI.

Guest, P. (2023, October). *Mykhailo Fedorov is running Ukraine's war against Russia like a startup*. Wired UK. https://www.wired.co.uk/article/ukraine-runs-war-startup

Haeck, P., Bordelon, B., & Scott, M. (2023, January 27). US, Netherlands strike deal on blocking chip exports to China. *Politico*. https://www.politico.eu/article/us-dutch-officials-meet-to-hammer-out-chips-control-deal-export-blocks-china/

Harvey, C., & Moore, C. (2023). The client net state: Trajectories of state control over cyberspace. *Policy & Internet*, *15*(1), 133–151. https://doi.org/10.1002/poi3.334

Hernandez-Morales, A. (2025, January 11). Zuckerberg urges Trump to stop the EU from fining US tech companies. *Politico*. https://www.politico.eu/article/zuckerberg-urges-trump-to-stop-eu-from-screwing-with-fining-us-tech-companies/

Higgins, T. (2022). Apple says it has stopped all product sales in Russia. *Wall Street Journal*. https://www.wsj.com/livecoverage/russia-ukraine-latest-news-2022-03-01/card/apple-says-it-has-stopped-all-product-sales-in-russia-Fl1qBYwvPtks66KYYaKW

Hijink, M. (2023, October 17). VS leggen strengere exportrestricties naar China op aan ASML. *NRC*. https://www.nrc.nl/nieuws/2023/10/17/vs-leggen-strengere-exportrestricties-naar-china-op-aan-asml-a4177595

Van Leemput, A. (2024, September 9). Farewell interview Martin van den Brink and Peter Wennink: 'ASML Remains a Very Dutch Company'. *Management Scope*. https://managementscope.nl/en/interview/martin-van-den-brink-peter-wennink-asml-farewell-interview

Horton, A. (2023, September 19). Whatever the fuss over Elon Musk, Starlink is utterly essential in Ukraine. *Washington Post*. https://www.washingtonpost.com/world/2023/09/08/elon-musk-starlink-ukraine-war/

Huntington, S. (1993). Why international primacy matters. *International Security*, *17*(4), 68–83. https://doi.org/10.2307/2539022

Inagaki, K., & Lewis, L. (2023). March 31). Japan to restrict semiconductor equipment exports as China chip war intensifies. *Financial Times*. https://www.ft.com/content/768966d0-1082-4db4-b1bc-cca0c1982f9e

Isaacson, W. (2023, September 7). Opinion: 'How am I in this war?': The untold story of Elon Musk's support for Ukraine. *Washington Post*. https://www.washingtonpost.com/opinions/2023/09/07/elon-musk-starlink-ukraine-russia-invasion/

Johnston, R. (1998). U.S. export control policy in the high performance computer sector. *The Nonproliferation Review*, *5*(2), 44–59. https://doi.org/10.1080/10736709808436706

Kasteleijn, N. (2024, January 24). ASML verkocht veel chipmachines aan China, ondanks beperkingen. *NOS*. https://nos.nl/artikel/2506021-asml-verkocht-veel-chipmachines-aan-china-ondanks-beperkingen

Kavanagh, C. (2023). Wading murky waters: Subsea communications cables and responsible state behaviour (Report). *United Nations Institute for Disarmament Research (UNIDIR)*. https://unidir.org/wp-content/uploads/2023/05/UNIDIR_Wading_Murky_Waters_Subsea_Communications_Cables_Responsible_State_Behaviour.pdf

Koc, C. (2024, July 15). ASML-backed university caught in middle of US-China chips war. *Bloomberg*. https://www.bloomberg.com/news/articles/2024-07-15/us-pressure-on-dutch-china-links-reaches-asml-funded-university

Koc, C., King, I., & Baazil, D. (2024, January 25). ASML's China sales surged despite secret Dutch deal with US. *Bloomberg*. https://www.bloomberg.com/news/articles/2024-01-25/asml-s-china-sales-surged-despite-secret-dutch-deal-with-us

Koc, C., & Jacobs, J. (2024, January 1). US pressured Netherlands to block China-bound chip machinery. *Bloomberg*. https://www.bloomberg.com/news/articles/2024-01-01/us-pushed-asml-to-block-chinese-sales-before-january-deadline

Liebetrau, T., & Bueger, C. (2024). Advancing coordination in critical maritime infrastructure protection: Lessons from maritime piracy and cybersecurity. *International Journal of Critical Infrastructure Protection*, *46*(September), 100683. https://doi.org/10.1016/j.ijcip.2024.100683

Lilly, B., Geers, K., Rattray, G., & Koch, R. (2023). Business@war: The IT companies helping to defend Ukraine. In T. Jančárková, D. Giovannelli, K. Podinš, & I. Winther (Eds.), *2023 15th International Conference on Cyber Conflict: Meeting Reality (CyCon)* (pp. 71–83).

Luttwak, E. (1990). From geopolitics to geo-economics: Logic of conflict, grammar of commerce. *National Interest*, *20*, 17–24.

Malkin, A., & He, T. (2024). The geoeconomics of global semiconductor value chains: Extraterritoriality and the US-China technology rivalry. *Review of International Political Economy*, *31*(2), 674–699. https://doi.org/10.1080/09692290.2023.2245404

Marquardt, A. (2022, October 13). Exclusive: Musk's SpaceX says it can no longer pay for critical satellite services in Ukraine, asks Pentagon to pick up the tab. *CNN*. https://www.cnn.com/2022/10/13/politics/elon-musk-spacex-starlink-ukraine/index.html

Matania, E., & Sommer, U. (2023). Tech titans, cyber commons and the war in Ukraine: An incipient shift in international relations. *International Relations*, *2023*, 500. https://doi.org/10.1177/00471178231211500

Microsoft. (2023, January 20). How technology helped Ukraine resist during wartime. *Microsoft CEE Multi-Country News Center*. https://news.microsoft.com/en-cee/2023/01/20/how-technology-helped-ukraine-resist-during-wartime/

Mitchell, R. (2022, December 15). How Amazon put Ukraine's 'government in a box'—and saved its economy from Russia. *Los Angeles Times*. https://www.latimes.com/business/story/2022-12-15/amazon-ukraine-war-cloud-data

Nawfal, M. (2023, September 7). @ MarioNawfal There was an emergency request from government authorities to activate Starlink all the way to Sevastopol. The obvious intent being [Post]. Twitter (X). https://twitter.com/elonmusk/status/1699917639043404146

Nicholls, R. (2022, March 6). The power of tech giants had made them as influential as nations: Here's how they're sanctioning Russia. *Conversation*. https://theconversation.com/the-power-of-tech-giants-has-made-them-as-influential-as-nations-heres-how-theyre-sanctioning-russia-178424

Norris, W. (2016). *Chinese economic statecraft: Commercial actors, grand strategy, and state control*. Cornell University Press.

Nye, J. (2011). *The future of power*. Public Affairs.

Olcott, E., & White, E. (2022, June 21). Elon Musk's Starlink aid to Ukraine triggers scrutiny in China over US military links. *Financial Times*. https://www.ft.com/content/df032357-51e7-4635-baaa-f053dcc0c4c1

Ostiller, N. (2023, November 29). Minister: Microsoft to provide free cloud services to Ukrainian government for another year. *Kyiv Independent*. https://kyivindependent.com/minister-microsoft-to-provide-free-cloud-services-to-ukrainian-government-for-another-year/

Parella, K. (2023). Corporate foreign policy in War. *Boston College Law Review*, *63*, 1–50. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4223298

Paulsen, M. (2024). The past, present, and potential of economic security (Forthcoming). *Yale Journal of International Law*, *50*.

Plantin, J.-C., Lagoze, C., Edwards, P. N., & Sandvig, C. (2018). Infrastructure studies meet platform studies in the age of Google and Facebook. *New Media & Society*, *20*(1), 293–310. https://doi.org/10.1177/1461444816661553

Rasser, M., & Wolf, K. (2022, December 13). The right time for chip export controls. *Lawfare*. https://www.lawfaremedia.org/article/right-time-chip-export-controls

Reuters. (2022, October 27). White House vows response if Russia attacks U.S. satellites. *Reuters*. https://www.reuters.com/world/white-house-vows-response-if-russia-attacks-us-satellites-2022-10-27/

Reuters. (2024, August 30). Netherlands to weigh ASML's interests in China export restriction decision, PM says. *Reuters*. https://www.reuters.com/markets/netherlands-weigh-asmls-interests-china-export-restriction-decision-pm-says-2024-08-30/

Roberts, A., Choer Moraes, H., & Ferguson, V. (2019). Toward a geoeconomic order in international trade and investment. *Journal of International Economic Law*, *22*(4), 655–676. https://doi.org/10.1093/jiel/jgz036

Roger, C., & Rowan, S. (2023). The new terrain of global governance: Mapping membership in informal international organizations. *Journal of Conflict Resolution*, *67*(6), 1248–1269. https://doi.org/10.1177/00220027221139431

Sanger, D. E., Barnes, J. E., & Conger, K. (2022, March 1). As tanks rolled into Ukraine, so did malware: Then Microsoft entered the war. *New York Times*. https://www.nytimes.com/2022/02/28/us/politics/ukraine-russia-microsoft.html

Satariano, A., & Frenkel, S. (2022, February 28). Ukraine war tests the power of tech giants. *New York Times*. https://www.nytimes.com/2022/02/28/technology/ukraine-russia-social-media.html.

Schroeder, E., & Dack, S. (2023, February 27). A parallel terrain: Public-private defense of the Ukrainian information environment. *Atlantic Council*. https://www.atlanticcouncil.org/in-depth-research-reports/report/a-parallel-terrain-public-private-defense-of-the-ukrainian-information-environment/.

Scholvin, S., & Wigell, M. (2018). Power politics by economic means: Geoeconomics as an analytical approach and foreign policy practice. *Comparative Strategy*, *37*(1), 73–84. https://doi.org/10.1080/01495933.2018.1419729

Shen, H., & He, Y. (2022). The geopolitics of infrastructuralized platforms: The case of Alibaba. *Information, Communication and Society*, *25*(16), 2363–2380. https://doi.org/10.1080/1369118X.2022.2128599

Smith, B. (2022a, June 23). *Countering foreign information operations: Developing a whole society approach to build resilience* [Video]. YouTube. https://www.youtube.com/watch?v=m_R1jbYoxkI.

Smith, B. (2022b, November 3). Extending our vital technology support for Ukraine. *Microsoft On the Issues*. https://blogs.microsoft.com/on-the-issues/2022/11/03/our-tech-support-ukraine/

Smith, B. (2022c, March 4). *Microsoft suspends new sales in Russia. Microsoft On the Issues.* https://blogs.microsoft.com/on-the-issues/2022/03/04/microsoft-suspends-russia-sales-ukraine-conflict/.

Sommer, U., Matania, E., & Hassid, N. (2023). The rise of companies in the cyber era and the pursuant shift in national security. *Political Science*, *75*(2), 140–164. https://doi.org/10.1080/00323187.2023.2278499

Srnicek, N. (2017). *Platform capitalism*. Polity Press.

Srivastava, S. (2023). Algorithmic governance and the international politics of big tech. *Perspectives on Politics*, *21*(3), 989–1000. https://doi.org/10.1017/S1537592721003145

Srivastava, S. (2022). *Hybrid sovereignty in world politics*. Cambridge University Press.

Sterling, T. (2023, January 13). Dutch PM Rutte denies U.S. pressure over chip export policy. *Reuters*. https://www.reuters.com/world/dutch-pm-rutte-denies-us-pressure-over-chip-export-policy-2023-01-13/

Strange, S. (1996). *The retreat of the state: The diffusion of power in the world economy*. Cambridge University Pres.

Stupp, C. (2022, June 14). Ukraine has begun moving sensitive data outside its borders. *Wall Street Journal*. https://www.wsj.com/articles/ukraine-has-begun-moving-sensitive-data-outside-its-borders-11655199002

Sukumar, A., Broeders, D., & Kello, M. (2024). The pervasive informality of the international cybersecurity regime: Geopolitics, non-state actors and diplomacy. *Contemporary Security Policy*, *45*(1), 7–44. https://doi.org/10.1080/13523260.2023.2296739

Swanson, A. (2023, January 28). Netherlands and Japan said to join U.S. in curbing chip technology sent to China. *New York Times*. https://www.nytimes.com/2023/01/28/business/economy/netherlands-japan-china-chips.html

Taddeo, M. (2024). *The Ethics of Artificial Intelligence in Defence*. Oxford University Press.

Taddeo, M., & Floridi, L. (Eds.) (2017). *The responsibilities of online service providers*. Springer.

Taylor, L. (2021). Public actors without public values: Legitimacy, domination and the regulation of the technology sector. *Philosophy & Technology*, *34*(4), 897–922. https://doi.org/10.1007/s13347-020-00441-4

Taylor, L., & Broeders, D. (2015). In the name of development: Power, profit and the datafication of the global South. *Geoforum*, *64*, 229–237. https://doi.org/10.1016/j.geoforum.2015.07.002

The Economist. (2020, February 29). How ASML became chipmaking's biggest monopoly. *Economist*. https://www.economist.com/business/2020/02/29/how-asml-became-chipmakings-biggest-monopoly

Tidy, J. (2022, October 11). Russia confirms Meta's designation as extremist. *BBC News*. https://www.bbc.com/news/technology-63218095

The Wassenaar Arrangement. (n.d.). *About us*. The Wassenaar Arrangement: On Export Controls for Conventional Arms and Dual-Use Goods and Technologies. https://www.wassenaar.org/about-us/

Sullivan, J. (2022, September 16). Remarks by National Security Advisor Jake Sullivan at the Special Competitive Studies Project Global Emerging Technologies Summit [Speech transcript]. *The White House*. https://bidenwhitehouse.archives.gov/briefing-room/speeches-remarks/2022/09/16/remarks-by-national-security-advisor-jake-sullivan-at-the-special-competitive-studies-project-global-emerging-technologies-summit/

Timmers, P. (2021, July 23). Debunking strategic autonomy. *Directions Blog*. https://directionsblog.eu/debunking-strategic-autonomy/

Timmins, B. (2022). Apple, Nike and Google join brands limiting services. *BBC News*. https://www.bbc.com/news/technology-60579641

Vabulas, F., & Snidal, D. (2021). Cooperation under autonomy: Building and analyzing the informal intergovernmental organizations 2.0 dataset. *Journal of Peace Research*, *58*(4), 859–869. https://doi.org/10.1177/0022343320943920

Vignati, M. (2022, November 10). LABScon replay: Are digital technologies eroding the principle of distinction in war? [Video]. *YouTube*. https://www.youtube.com/watch?v=0190oHf8zEA

Waarlo, N. (2025, January 3). ASML zet kleurrijk zwaargewicht in. *de Volkskrant*. https://www.volkskrant.nl/economie/asml-zet-politiek-zwaargewicht-in-de-kleurrijke-franse-oud-minister-bruno-le-maire~bc8b0b11/?referrer=https%3A//www.bing.com/

Westerwinter, O., Abbott, K. W., & Biersteker, T. (2021). Informal governance in world politics. *The Review of International Organizations*, *16*(1), 1–27. https://doi.org/10.1007/s11558-020-09382-1

World Trade Organization. (2022). *United States – Measures on certain semiconductor and other products, and related services and technologies: Request for consultations by China* (WT/DS615/1). https://docs.wto.org/dol2fe/Pages/SS/directdoc.aspx?filename=q:/WT/DS/615-1.pdfandOpen=True

White, M. J. (2022). *Intel joins list of companies to halt shipping to Russia*. Digitaltrends. https://www.digitaltrends.com/computing/intel-stops-shipping-to-russia-and-belarus/

Wigell, M. (2016). Conceptualizing regional powers' geoeconomic strategies: Neo-imperialism, neo-mercantilism, hegemony, and liberal institutionalism. *Asia Europe Journal*, *14*(2), 135–151. https://doi.org/10.1007/s10308-015-0442-x

Zetter, K. (2022, December 7). *Security firms aiding Ukraine during war could be considered participants in conflict*. Zero Day. https://zetter.substack.com/p/security-firms-aiding-ukraine-during?publication_id=312238andutm_medium=emailandaction=shareandisFreemail=true