Towards a Framework for Analysing Complex Interdependence in Digital Espionage Markets

Ahana Datta
University College London, UK

ahana.datta.20@ucl.ac.uk

Abstract: Cyber power indices have dominated discourse in recent years as measuring the relative power of nation-states in cyberspace to exercise their cyber capabilities for offensive and defensive purposes. These indices adapt a variety of methodologies, but their effectiveness in mobilising cyber power remains limited. Indices based on dynamic systems frameworks explain power consolidation arising from network-effects, but are too broad to implement due to complexity. In this article, we analyse cyber power through access to digital espionage capabilities, using the theory that states weaponise complex interdependence of information flows. Instead of proposing an index, we set up a case study contrasting the Chinese system, where the state mediates technology vulnerabilities, with the Five Eyes system, where vulnerability disclosures are a common occurrence. The Chinese system exhibits a "chokepoint" effect, in contrast to the Five Eyes' "panopticon" mediation of information flows. Extant cyber espionage analyses range over themes such as economic vis-a-vis open and closed vulnerability markets; legal, in relation to the circulation of tools like spyware; or strategic and case-based. Given this confluence, we posit a framework of information flows between ecosystems of actors. Exploit vendors, state-backed offensive operators, nation-states, and tech platforms are networked through interdependent information flows, consolidating power in private actors. The political economy of a nation-state provides useful heuristics in articulating strategic aims behind its espionage activities, as well as its approach in controlling the flow of knowledge of vulnerabilities between the private actors of which the state may be a customer. In highlighting this tension between nation-states' political economies defining their roles as both mediator and customer, we offer security scholars nuanced considerations in theorising cyber power. We conclude that while this tension amplifies private power, policymakers must intervene to reshape interdependent networks that influence and counter it.

Keywords: Cyber Power, Complex Interdependence, Cyber Espionage, Vulnerability Disclosure

1. Introduction

In over two decades of literature aiming to define, theorise, score, or evaluate national cyber power, some points of consensus emerge. Firstly, that a nation's cyber power projects on to both cyberspace in itself, as well as as an auxiliary instrument to gain leverage in domains outside cyberspace, such as the military. Second, that international relations scholars converge either towards rationalising "cyber power" through longstanding normative theories of power and war in the vein of (Nye, 2010), (Rid, 2013), (Betz and Stevens, 2011) in recent years, (Kuehl, 2009) or (Starr, 2009) before Stuxnet, or through qualitative methods that ultimately set up a scoreboard of cyber capabilities between nation-states.

As such, the first sets up a lens through which cyber power must be appraised more and more comprehensively, covering as many aspects as possible of offensive and defensive domains, revised after any political event of note where cyber-means play a pivotal role. Comparisons of indices are based against supposedly more comprehensive cybersecurity standards, such as NIST (Cifci, 2022). Each successive cyber power model vies for greater comprehensiveness. On the other hand, the second sets up outcomes that typically favour metrics accuracy with little impact on mobilisation (Inkster, 2017) or theoretical consistency at the cost of exposing biases in analysing a strategic competitor's approach. Typical examples are seen in the sample analytical questions that constitute the scoring mechanism, such as those posed by the Belfer Centre index (Voo et. al, 2020), or the more sophisticated IISS version (International Institute for Strategic Studies, 2021): questions such as whether a nation adopts "a whole of society" approach in its cyber governance, or when national documents first mention "cyber" appear to omit political, national security, and cultural considerations in nation-states like Russia, China or North Korea. For example, China and Russia do not linguistically differentiate between information influence and cyber operations; North Korea's disproportionate offensive cyber power belies its economic weaknesses. Furthermore, nation-states such an Iran compensate for the lack of a sophisticated passive surveillance capability through investment in offensive cyber operations; for many states, investing in cyber defence instead is an opportunity cost. This skews the results of any "comprehensive" index, as the analysis is constrained by limited observability of empirical data, attribution, and national perspective.

The divergences in literature, however, show nuanced conclusions. Analyses of mobilising cyber power recognise that non-state actors play a significant role, and any leverage in cyberspace depends on a state's ability to influence and coerce them (Klimburg, 2011). Dynamic systems models of cyber power illustrate nuances such

as an actor's evolving capability, the conception of the state as an actor within a dynamic environment, as well as access to vulnerabilities and capabilities to mature them (Mattila, 2021). A structural analysis demonstrates how the political economy of a bloc like the EU decentralises power over cyber capability to member states, whilst centralising institutional power through common policies, standards and regulatory obligations (Dunn Cavelty, 2018).

This article presents cyber power as a relative phenomenon in a wider ecosystem of actors, each of which act to accrue, consolidate, diffuse or disperse it. In the digital espionage ecosystem, the promise of achieving political, economic, trade, or innovation-based strategic objectives can lead nation-states to exert significant resources and capabilities in acquiring, developing, deploying, and storing offensive cyber capabilities. Depending on a nation-state's strategic objectives, this may well outweigh the priority placed on defensive cyber capabilities or the resilience of institutions that maintain its security, which motivates our scrutiny on crucial offensive cyber capabilities. Our research process adopts as an analytic tool the theory of 'new structuralism', which argues that states entrench power asymmetries by weaponising complex interdependence of information flows. We use a single, interpretive case study, where recent Chinese legislation requiring technology platforms to report vulnerabilities in their systems to the government within days of discovery acts as a break point, allowing us to present the Chinese system as a global "chokepoint" of vulnerabilities, in contrast to the Five Eyes, where vulnerability disclosures are more common. Our sourcing relies on a synthesis of government documents, news reports, peer-reviewed literature such as journal articles, researcher reports, and testimony of actor perspectives in the form of blogs or interviews.

We construct an ecosystem of four types of actors, namely, nation-states; tech platforms; third-party offensive cyber groups (often called mercenaries, proxies, etc) who may act independently, or on behalf of a state. Third-party cyber groups are sometimes indistinguishable from the state, as seen in the case of many Advanced Persistent Threat groups, who are linked to state security and intelligence agencies but not directly employed. Finally, we include a fourth actor in the form of exploit vendors on the legitimate or illegitimate vulnerability market, who may also assist nation-states or mercenaries with offensive cyber operations when such actors need to procure and develop offensive cyber tools. Each actor is connected by a demand-supply relationship with another for a service that provides or develops a capability. We discuss how the interdependence of information flows between these actors entrench established power dynamics, by consolidating two types of private power: that accumulated by tech platforms, and that exercised by exploit vendors. To do so, we turn to weaponised complex interdependence of information flows described by (Farrell and Newman, 2019) and (Oatley, 2018). Given demand and supply relationships between public, private, and "in between" actors in the vulnerability market, coercive power within private actors grows. Political economies of states that help reshape these information flows, or states that have the capability to exercise coercion over private power are most able to mobilise cyber power. (Betz, 2012) and (Maurer, 2018) use actor-network models to appraise coercive power in mercenary hackers, (Harvey and Moore, 2023) analyse Meta's statecraft-like private power.

In Section 2, we justify using digital espionage as an angle to theorise cyber power; in Section 3, we introduce the ecosystem of actors, connectivity and the complex interdependence framework of information flows, and outline the case study; in Section 4, we discuss implications of private power and its coercive abilities on states and other actors, and vice versa; in Section 5 we present concluding remarks on translating digital espionage into strategic advantage for states, and future directions for policymakers considering reshaping private power.

2. Digital Espionage as an Angle For Analysing Cyber Power

Cyber espionage has been defined as "an attempt to penetrate an adversarial computer network system … for the purpose of extracting sensitive information" (Rid, 2013). Natural questions arise: who does it, why, and how? Some perspectives deal mainly with intelligence operations conducted by states for political objectives (Lindsay, 2021), but absent the effect of mercenaries' independent actions, the analyses can seem incomplete. Many IR scholars may point out that political and commercial espionage are perceived differently, particularly in legal terms, but the targets of alleged Chinese state-sponsored espionage transcend such distinctions in terms of technical methodologies, for example, the Volt Typhoon advisory (Joint Cybersecurity Advisory with Microsoft Threat Intelligence, 2023). When we speak of digital espionage markets, we are concerned with the capabilities — the tools and services — offered on open or closed markets to any customer, regardless of the customer's objective as a strategic actor — at least in the first instance.

To avoid confusion with combined methods such as HUMINT, we speak of digital espionage as espionage conducted by digital means on digital targets. Extracting sensitive information may not entail information

exfiltration from a computer network, merely passive surveillance; we look at services and technologies used to establish surveillance and/or computer network exploitation (CNE) as the main methods of digital espionage. Surveillance may help establish CNE, and vice-versa, but unlike CNE, surveillance need not be covert. Further, the type of digital target motivates the tactics, techniques, and processes (TTPs) engaged for penetration. For example, in telecommunications and Internet service providers (ISPs), intelligence sharing networks such as the Five Eyes have established passive surveillance capabilities (SIGINT). In contrast, mass market technology endpoints, such as smartphones can be penetrated by exploiting a vulnerability in the application layer, operating systems, firmware and/or hardware. A canonical example is the spyware Pegasus, aimed at exploiting a vast number of iPhone firmware versions for full access at 0-click target engagement.

Espionage and counterespionage may be intended for offensive or defensive cyber operations. State may use intelligence about adversarial cyber capabilities, obtained from surveillance or CNE or other sources, to develop counter capabilities of their own, to deter the adversary by disclosing their capabilities, or to patch their own high-risk vulnerabilities. As a precursor to meeting a political or commercial strategic objective — which scholars may find hard to deduce and study until some instance of public attribution — the act of mounting an espionage operation itself can be indicative of adversarial cyber power. Factors include how much the adversary invests in the cybersecurity of its digital assets, its purchasing power in accessing sophisticated capabilities, and the resources required to acquire, develop, stage or deploy an exploit. The same questions that analysts in a state's intelligence agency must answer in mounting a digital espionage operation are then necessary in evaluating its offensive cyber power.

Throughout the planning and execution stages of an operation, answers to operational questions are indicative of some facet of cyber power: Are the targets (adversary's digital assets) connected to the Internet; is the target a proprietary technology or mass-market, and if so, are exploits already available on the market or in-house for vulnerabilities in the target; has the state developed its own exploits, or does it have already established relationships with third-party vendors who might be able to provide such capabilities, and at what cost; can the state afford to acquire and develop these exploits, and turn them into "intelligence equities" (Ben-Gad and Finkelstein, 2022); is it best for the state's strategic objective to deploy the equity on to the target (and risk discovery, closure of that attack vector, and rebuttal) or to disclose the equity to the tech platform that can patch the underlying vulnerability or to trade the equity with an intelligence ally for some other utility; how long must penetration be maintained after initial CNE, and is that affordable resource-wise and strategically; how quickly the target reacts to discovering the CNE, if at all; how viable are other attack vectors to the target and for how long.

This is by no means an exhaustive list of the analyst's considerations, but illustrative that in large part, the business of conducting digital espionage is just that — a business. This is the key economic dimension that many cyber power narratives omit. Like any business, the state actor's relationships with other actors in the ecosystem, such as tech platforms, mercenaries, exploit vendors, and intelligence allies are rooted in the ability to negotiate, control, or influence; such forms of coercion is the source of its power. This ability is derived from the political economy of the state itself, which determines its response to private actors, as well as who it views as an ally or adversary (in some contexts, both). Given its relationships and political economy, the state can take on the role of intermediary, consumer, regulator, or some combination of those roles in the vulnerability market. In liberal democracies, the state has lower control over private enterprises in market-based economies, with some ability to regulate information flows in the market, in contrast to more authoritarian systems, where the state acts as an effective ceiling to accrued private power. The UK, as a member of the Five Eyes, for example, admits that its preference towards handling intelligence equities is disclosure wherever possible, and subject to internal governance (Levy, 2018), and this is also reflected in United States policy (Trump White House Archives, 2017).

We are not suggesting that this implies that authoritarian systems must be disproportionately large consumers in the vulnerability market, however, current empirical data suggests quite the opposite — democratic countries appear to be the biggest buyers of spyware globally (Feldstein and Kot, 2023). The aim of interdependence is to discuss the extent of control that states can or cannot exert over private power — for offensive or defensive purposes — which form much of its cyber capability, even as they might play the roles of customers and mediators simultaneously.

3. Complex Interdependence and a Case Study

Weaponised interdependence argues that networks, as sociological structures that place limits on an actor's agency, tend to entrench and amplify existing asymmetries in power relationships over time. Where power is initially centralised, network effects of interdependence such as globalisation will ensure power is only further centralised as these structures evolve, and networks become "highly resistant to change", best visualised as hub-and-spoke models. In particular, Farrell and Newman characterise weaponisation in the guise of "chokepoints" and "panopticons": the former is an actor's ability to limit the access of other actors to an information hub; and the latter is an actor's ability to observe information flows passing through key hubs. In the case of globalised, interdependent information networks, such as the Internet, they observe that American institutions such as ICANN and policies of tech self-regulation allowed online business models to extract and monetise user content, thus first enabling, then entrenching centralised power over digital markets in tech platforms such as Google, Amazon and Facebook. Platform monopolies and the national security apparatus force a disproportionate amount of global Internet traffic to pass through an American hub such as in Virginia. Through the PRISM programme, the US government was able to then exploit this "panopticon" setup and weaponise its dominance over Internet traffic hubs to create extensive surveillance capabilities in cooperation with private partners and intelligence allies such as the Five Eyes.

As a theoretical tool, 'new structuralism' has been applied to other areas of security analyses. (Farrell and Newman, 2019) adapt weaponised complex interdependence to privacy, surveillance, and its governance.(Segal, 2021) applies weaponised interdependence to the 5G rivalry between the US and China, arguing that the exclusion of ZTE from the US supply chain eventually led to ZTE's exclusion from Western tech supply chains, and through restrictions on Huawei, controlling the critical chokepoint of the advanced semiconductors design and manufacturing market, the US prevented Huawei from leveraging diversified markets. (Tusikov, 2021) contextualises states coercing tech platforms into enacting chokepoints for Internet services globally, noting that states need to have considerable structural, legal and economic capacity to coerce the private sector, not just domestically but internationally. She contrasts US weaponisation of its tech platforms' international influence with their Chinese counterparts expanding to catch up and fulfil China's political economy objectives with the state overseeing industrial expansion; China's weaponisation of chokepoints is highlighted in suggested future work, which adds to our motivation.

We use a similar network construction to discuss the case of offensive cyber capability. Our framework consists of actors such as nation-states and tech platforms, but also exploit vendors, and hackers groups, mercenaries, or proxies. Each actor operates in its own 'ecosystem' (Adner, 2017), with tech platforms such as Alibaba, Meta, Amazon, Alphabet, etc offering the most visible examples of multiple product offerings that keeps their customers information walled in. On the other hand, the Lighthouse and Haaretz investigations into exploit vendors also suggest an ecosystem of actors working towards each stack of the technology they target and build offensive capabilities from (Lighthouse Reports, 2022). Each actor interacts with another within its own ecosystem, or in another ecosystem, through information buying and selling relationships. On the other hand, ecosystems are not always cleanly differentiated. Even in the digital espionage ecosystem construct, it is not always possible to distinguish an offensive cyber operation led and owned solely by the nation-state, as opposed to a joint or sponsored effort with a mercenary, enabled by a trusted vendor, or in concert with other intelligence allies, but rather, it depends on what role the actor takes vis-a-vis its requirement to buy or sell a service.

However, to conduct CNE, the offensive actor needs access to a specific information commodity, namely, vulnerabilities in the digital target, the knowledge or use of which may be bought and sold with any degree of technological sophistication, ranging from digital footprints on databases, to exploits that must be used in concert in a wider attack (spearphishing for network penetration, then malware lateral movement is a common example), to packaged and point-and-deploy malware such as Predator or Pegasus. Given the range of expertise and resources needed to facilitate discovery of vulnerabilities and their development into commoditised offensive tools or weapons, the exploit vendors operate in an ecosystem of their own, with different actors focusing on different technology stacks or business development, for example. Vulnerabilities don't necessarily have to be 0-days; simply identifying that the target is vulnerable and an exploit can be made available in fulfilling a broader objective. Each actor has a specific role in the circulation of these commodities over the Internet. Tech platforms produce digital endpoints such as smartphone software or hardware, server and network infrastructures that inevitably have security vulnerabilities, and at the same time must detect and patch these vulnerabilities in a timely manner. The resulting window between any actor detecting such a vulnerability in digital targets and its closure allows actors such as exploit vendors, mercenary groups, and nation-states to develop CNE and data exfiltration capabilities.

The offensive security researcher Maor Schwartz provides a look into exploit vendor actors and the wider industry (Schwartz, 2023). As tech platforms have invested more into the cybersecurity of their products, the availability of an arsenal of vulnerabilities has become rarer and more expensive, reshaping the supply pool. Offensive security researchers have overcome the difficulty of selling the vulnerabilities they do find by establishing trust-based relationships with nation-states through middlemen such as brokers, or by being employed to "end-to-end companies". Schwartz asserts that the market peaked before 2020 with many competing vendors selling the same vulnerabilities, but dipped between 2020-2021 due to a combination of increased media coverage, export control laws on spyware, new regulatory paradigms on cybersecurity, the economic shock of the pandemic, and legal challenges brought by tech platforms to vendors exploiting their products. After 2021, vendors sought R&D investments from nation-states and private equity directly, and recouped their costs by selling the same vulnerabilities to multiple states. In particular, nation-states that appear on US sanctions lists have no legal or affordable purchasing power from vendors supplying to the Five Eyes due to export control and price discrimination, and such states struggle to develop similar capabilities in-house. They must seek alternatives domestically, or amongst their allies and their markets. It is evident that the domestic institutional power, norms, and jurisdictions that form a necessary condition for weaponising complex interdependence in Farrell and Newman's theory are also present in the case of the Five Eyes, and particularly the US, in accessing part of the digital espionage market and isolating adversaries from it. This "panopticon" role is an evolution of the same structural and topological asymmetry as information flows vis-a-vis Internet traffic and surveillance capabilities.

In contrast, China has its own network architecture, derived from and in service to its political economy, that routes information flows in its own favour. Former FBI agent Adam Kozy notes in his testimony to the US-China Economic and Security Review Commission that a part of the Chinese Ministry of State Security (MSS) has been "getting early access to software vulnerabilities for twenty years". In September 2021 vulnerability disclosure by tech platforms and wider industry to the databases of the Ministry of Industry and Information Technology (MIIT) was made legally mandatory within 2 days of discovery, isolating foreign platforms from knowledge of vulnerabilities in mass technology, ostensibly adding to Chinese offensive cyber capability. The Atlantic Council (Cary and Del Rosso, 2023) uses the Chinese CERT data as a primary source to report the role of the MIIT as an intermediary for vulnerability disclosure. The report indicates that new, post-regulation information flows leverage academia, tech platforms, national infrastructure such as telecoms, and the state in bolstering China's offensive cyber capability. They cite the increase in high-severity vulnerabilities reported on its central database as evidence of regulatory success. This apparent sharp increase in the hoarding of 0-days since 2021 is corroborated by Microsoft as well as Recorded Future's reports into the rise of China as a "leading global cyber power," finding that 85% of digital targets were public, Internet-facing appliances (Insikt Group, 2023). They imply that Chinese digital espionage has expanded to mass-market consumer tech products, from firewalls to email infrastructure. The report also describes China's cyber capability evolution as rapid, scaled up, focused, and aligned "…with China's military, political, economic, and domestic security priorities." Formalising the 2021 regulation, coercing industry and cornering the vulnerability market turned an existing norm into legal leverage, with the Chinese state weaponising vulnerabilities and centralising access to an ever-growing database, at the exclusion of foreign tech platforms, as a "chokepoint". As Farrell and Newman observe, "… states that fear they will be targeted … reshape networks so as to minimise their vulnerabilities."

Restrictions on the availability of, and access to, vulnerabilities and exploits in globally used tech products impact the creation and development of intelligence equities. In turn, this affects the ability to mount espionage campaigns, and so the ability to exert cyber power for strategic leverage. The asymmetric relationship between decentralised disclosures led by industry in the Five Eyes case, and centralised mediation by the state in the Chinese case, on what are likely similar vulnerabilities in underlying tech platforms, is reflective of their respective political economies. Liberal democracies must simultaneously welcome scrutiny and answer to the same institutions that enable them levers such as mobilising and exerting cyber power; autocracies have no such checks and balances. The authoritarian state has a bigger threat than an international adversary to contend with, in the form of domestic dissent. The investment in mitigating internal threat through increased surveillance, or other digital means — including the role of "domestic panopticon" through a vast national firewall — will be as much, if not more, of a priority than foreign and economic policy initiatives outlined in the Belt and Road Initiative, for example. Simply collecting more vulnerabilities than a strategic adversary is not the final word in a nation-state's digital espionage capabilities, or the extent of its "cyber power". Vulnerability markets represent one of the key hubs to which privileged states need sustained access, in order to maintain structural dominance, as well as institutional power that enables them to weaponise these interdependences, fostered by the dominant tech platforms' products and the topology of the Internet. Coercing the tech platform private actor

directly (using regulatory or legislative levers, or by targeting its customers) or indirectly (by targeting its products and forcing vulnerability remediation) then requires partnership with other private actors such as exploit vendors and mercenaries.

4. Private Power and State Coercion

In order to weaponise complex interdependence to any sustained degree structurally — by controlling chokepoints that are critical to offensive cyber capability, amplifying data flows through new and existing surveillance hubs, and creating legal and regulatory frameworks that entrench these power asymmetries — the nation-state must coerce to its advantage three types of private power: that of tech platforms, hacker groups, and exploit vendors.

These so-called private actors operate in ecosystems of their own. Hacker groups' relationship with the state, for example, may be semi-private: ideological proxies can form trust-based relationships with the state until a desirable political inertia lasts. Economically motivated mercenaries may act of their own agency, mounting subversive ransomware attacks. Public attribution can muddy the waters. Hacker groups are at times useful for the nation-states' deniability of an offensive operation, but also a potential nuisance or deterrent when acting upon their own initiative — their power, only semi-private where funded by the state, shapes the digital espionage market by leveraging unsophisticated cyber attacks, or burning vulnerabilities. (Sheldon and McReynolds, 2015) assess the policy implications of civil-military integration in Chinese "information warfare militias", and their predictions of the Chinese state leveraging academia and industry in contributing to espionage campaigns, targeting telecommunications and global supply chains have been proved correct. The vast literature on hacker groups and mercenaries does not reach a consensus on the entrenched power in the longer term of any single group, even of any particular Advanced Persistent Threat; in the aftermath the US Office of Personnel Management 2014 breach, for example, APT-1 was publicly attributed. Identified individuals, rather than the state, were sanctioned by the US. The effectiveness of such sanctions as a deterrent to espionage campaigns is debatable, but has remained the one of the few legitimate ripostes where political attribution is fruitless.

Where power is even more private, nearly opaque, in the case of exploit vendors for example, states struggle to create lasting coercive instruments due to complex domiciles and overlapping incentives. As alluded to previously, the joint Lighthouse-Haaretz reportage identifies the vendor of the Predator spyware, Intellexa, and its European connections with the Israeli spy firm; Haaretz also notes in a separate report the involvement of a Swiss actor enabling spyware firms rout regulations through vulnerabilities in the international mobile system (Black and Benjakob, 2023). The scandal of the Pegasus spyware, proliferation and use in EU member states, and legal frameworks on "dual-use" has been covered extensively elsewhere. Additionally, the US Executive Order strengthening export control laws on spyware through a moratorium has drawn criticism at its ability to protect the free press from surveillance, and if this instead strengthens American offensive cyber capability. On the other hand, given its political economy, the Chinese state uses its legal chokepoint to leverage its offensive cyber ecosystem in systematic ways — as seen in researchers' analysis of the recent Anxun ('I-Soon') leaks — which suggest, through new insight these leaks reveal about the group APT-41, that the offensive cyber ecosystem in China is similar to that of its Western counterparts (Bernsen, 2024).

Tech platform power, exploitation, and digital market monopolies are extensively covered in academic literature where 'private power' is invoked; the phrase applies much less to power accrued by exploit vendors and other third-parties. However, nation-states' coercive strategies are now aimed at securing and manipulating private power to build resilience in, or conversely spy on, global supply chains. To achieve meaningful coercion, states must leverage security policies that apply to every actor in the ecosystem both internationally and domestically, and tech platforms can be an obvious target. The US Securities and Exchange Commission response to alleged Russian espionage, resulting in the 2020 SolarWinds breach, has triggered legal action against SolarWinds company staff. Targeting platforms provides easy access into any global supply chain, given increased dependence on cloud infrastructure. Leveraging platform vulnerabilities, such as the 2024 targeting of senior Microsoft leadership by Russian-sponsored Midnight Blizzard, appears to be an emerging pattern in the competition for control of global supply chains (UK National Cyber Security Centre, 2024). The Five Eyes in particular, have suggested policies to "de-risk" their critical infrastructure from that of its strategic competitors, but have to overcome the realities of complex interdependence for this to work.

5. Conclusion

Any strategic leverage derived from digital espionage is not homogenous (Devanny et al, 2021). We have argued that it may depend on several factors such as structural advantages, national objectives, political economies, proportional responses, and legal instruments available to the state. By taking a political economy approach to digital espionage markets, we have constructed a framework of actor ecosystems and their interplay. We identify, in particular, two forms of private power vis-a-vis the role of the state: exploit vendors, where the state may act as a consumer; and tech platforms, where the state acts as regulator. Yet, at the nexus of these actors, the state strives to be an intermediary, and the resulting tension creates an area of future scrutiny. There is growing momentum in cyber espionage literature for such analyses that juxtapose the state's assumed rôle versus its political, economic and security objectives; a recent example highlights the difficulty in establishing espionage norms between Russia, China and the West due to conflicts in this juxtaposition (Harnisch and Zettl-Schabath, 2023). Our proposed approach for theorising cyber power using 'new structuralism' as an analytical tool, states consolidate cyber power by weaponising the complex interdependence of information flows online, exploiting structural asymmetries in accessing digital espionage markets and coercing private actors. Our case study compares the Chinese and Five Eyes approaches to vulnerability disclosures to show how structural asymmetries are embedded using levers of state power.

Even one aspect of mobilising cyber power, in the form of access to offensive tooling needed to conduct digital espionage, is a dynamic and interdependent phenomenon, and comprehensive indices forego nuances. The digital espionage case illustrates that in future models of cyber power, each selection criterion must be considered in both absolute and relative terms; for example, interdependences that affect defending a state's digital assets, or within its civil society vis-a-vis incident response preparedness, and other interdependences.

Digital espionage is mostly motivated by a desire to decrease information asymmetries, and counter-espionage is motivated by maintaining or even increasing them. Its methods originate from, and are a response to, technological innovation that primarily arise from private actors. Future research on factors that increase or limit innovation in an era of systemic competition would be beneficial in understanding the persistence of national cyber power. In particular, while authoritarian systems have greater coercive capabilities on private actors, democratic systems may enable innovation through freer markets. Emerging risks must also be factored into policymakers models aiming to reshape network interdependence. (Tusikov, 2021) points out, for example, that the network structure of the Internet is shifting towards the Pacific due to increased private power in tech platforms serving the BRICS nations. A plausible shift in the global political economy away from democratic capitalist systems will change the nature of interdependent information flows; particularly in the capacity for weaponisation, and thus, cyber power. Future policy frameworks analysing cyber power must be sensitive to these dynamics.

Finally, we posit to the cyber power theory community that the capability of a state to mobilise its cyber capabilities to enhance its "national power" is not merely limited to its absolute technological, institutional, and structural advantages. It is equally a test of it arbitrates and conducts domestic and foreign trust relationships in the long term, and the quality of leadership that decides how best to project it.

Acknowledgments

Thanks to Madeline Carr and David Pym for their feedback. This work was supported by EPSRC grant EP/S022503/1.

References

Adner, R. (2017). Ecosystem as Structure: An Actionable Construct for Strategy. Journal of Management, 43(1), 39-58.

Ben-Gad, M., Finkelstein, A. (2022) 'On Intelligence Equities'. Draft. (0.9.1)

Bernsen, W. (2024) Same Same, but Different, Margin Research. Available at: https://margin.re/2024/02/same-same-but-different/.

Betz, D. (2012) 'Cyberpower in Strategic Affairs: Neither Unthinkable nor Blessed', Journal of Strategic Studies, 35(5), pp. 689–711.

Betz, D.J. (2017) 'Cyberspace and the State: Towards a Strategy for Cyber-Power'. Routledge.

Black, C. and Benjakob, O. (2023) 'How a Secretive Swiss Dealer Is Enabling Israeli Spy Firms', Haaretz.

Cary, D. and Del Rosso, K. (2023) 'Sleight of hand: How China weaponizes software vulnerabilities', Atlantic Council, 6 September.
Cifci, H. (2022) 'Comparison of National-Level Cybersecurity and Cyber Power Indices: A Conceptual Framework' pre-print (2022).
Devanny, J., Martin, C. and Stevens, T. (2021) 'On the strategic consequences of digital espionage', Journal of Cyber Policy, 6(3), pp. 429–450.
Dunn Cavelty, M. (2018) 'Europe's cyber-power', European Politics and Society, 19(3), pp. 304–320.
Farrell, H. and Newman, A.L. (2019) 'Of Privacy and Power: The Transatlantic Struggle over Freedom and Security', in Of Privacy and Power. Princeton University Press.
Farrell, H. and Newman, A.L. (2019) 'Weaponized Interdependence: How Global Economic Networks Shape State Coercion', International Security, 44(1), pp. 42–79.
Harnisch, S. and Zettl-Schabath, K. (2023) 'Secrecy and Norm Emergence in Cyber-Space. The US, China and Russia Interaction and the Governance of Cyber-Espionage', Democracy and Security, 19(1), pp. 82–110.
Harvey, C.J. and Moore, C.L. (2023) 'Cyber statecraft by net states: the case of Meta, 2016–2021', Journal of Cyber Policy, 0(0), pp. 1–21.
IISS. (2021), 'A methodology for assessing the cyber power of states'. Available at: https://www.iiss.org/research-paper/2021/06/cyber-power-methodology/
Inkster, N. (2017) 'Measuring Military Cyber Power', Survival, 59(4), pp. 27–34.
Insikt Group. (2023) 'Charting China's Climb as a Leading Global Cyber Power' , Recorded Futures.
Klimburg, A. (2011) 'Mobilising Cyber Power', Survival, 53(1), pp. 41–60.
Kot, S.F., Brian (Chun Hey) (2023) Why Does the Global Spyware Industry Continue to Thrive? Trends, Explanations, and Responses, Carnegie Endowment for International Peace.
Levy, I. (2018) 'Equities Process'. Available at https://www.ncsc.gov.uk/blog-post/equities-process
Lighthouse Reports (2022), 'Flight of the Predator'. Available at: https://www.lighthousereports.com/investigation/flight-of-the-predator/
Lindsay, J.R. (2021) 'Cyber Espionage', in P. Cornish (ed.) The Oxford Handbook of Cyber Security. Oxford University Press.
Lindsay, J.R., Cheung, T.M. and Reveron, D.S. (2015) China and Cybersecurity: Espionage, Strategy, and Politics in the Digital Domain. Oxford University Press.
Miller, S. (2016) 'Cyberattacks and "Dirty Hands": Cyberwar, Cybercrime, or Covert Political Action?', in F. Allhoff, A. Henschke, and B.J. Strawser (eds) Binary Bullets: The Ethics of Cyberwarfare. Oxford University Press.
Mattila, J.K. (2022) 'A Model for State Cyber Power: Case Study of Russian Behaviour', European Conference on Cyber Warfare and Security, 21(1), pp. 188–197.
Maurer, T. (2018) Cyber Mercenaries. Cambridge University Press.
Oatley, T. (2019) 'Toward a political economy of complex interdependence', European Journal of International Relations, 25(4), pp. 957–978..
Rid, T. (2013) Cyber War Will Not Take Place. Oxford, UNITED STATES: Oxford University Press, Incorporated.
Segal, A. (2021) 'Huawei, 5G, and Weaponized Interdependence', in D.W. Drezner, H. Farrell, and A.L. Newman (eds) The Uses and Abuses of Weaponized Interdependence. Brookings Institution Press, pp. 149–166.
Sheldon, R. and McReynolds, J. (2015) 'Civil-Military Integration and Cybersecurity: A Study of Chinese Information Warfare Militias', in J.R. Lindsay, T.M. Cheung, and D.S. Reveron (eds) China and Cybersecurity: Espionage, Strategy, and Politics in the Digital Domain. Oxford University Press.
Shwartz, M. (2023) 'The boom, the bust and the adjust', Medium, 20 June. Available at: https://medium.com/@maor_s/the-boom-the-bust-and-the-adjust-ea443a120c6.
Trump White House (2017) Vulnerabilities Equities Policy and Process for the United States Government.
Tusikov, N. (2021) Internet Platforms Weaponizing Chokepoints. In D. Drezner, H. Farrell, and A. Newman, eds. The Uses and Abuses of Weaponized Interdependence. (pp. 133-148). Washington, DC: Brookings Institute Press.
UK National Cyber Security Centre. (2024) SVR cyber actors adapt tactics for initial cloud access. Available at: https://www.ncsc.gov.uk/news/svr-cyber-actors-adapt-tactics-for-initial-cloud-access.
Voo, J. et al. (2020) 'National Cyber Power Index 2020: Methodology and Analytical Considerations', China Cyber Policy Initiative Reports [Preprint].