A Political Economy of Digital Espionage

What are the dynamics of leverage in cyberspace, and who profits?

Ahana Datta

27 November 2024

Centre for Doctoral Training in Cybersecurity,

University College London

A thesis submitted in partial fulfillment of the requirements for a PhD in the Department of Computer Science

Examination Committee:

Primary supervisor: Professor David J. Pym

Secondary supervisor: Professor Madeline Carr

Examiners: Professor Sir Anthony Finkelstein, Professor Tim Watson

'I, Ahana Datta, confirm that the work presented in this thesis is my own. Where information has been derived from other sources, I confirm that this has been indicated in the thesis.'

Abstract:

As an emerging multipolar international order advances strategic competition, cyberspace itself has transformed into a competition domain. To examine the dynamics of leverage in cyberspace, this thesis explores relationships of trust and power between public and private actors, such as nation-states, security researchers, technology platforms, and hacker groups. Using concepts from dynamic international political economy, the central conceptual framework captures the formation of trust-based relationships and how states use cooperation and coercive instruments, in particular, through digital espionage, to achieve strategic objectives and mobilise cyber power. The innovations in the framework outline a multilevel analysis of trust in technological, political, and economic information networks, where interdependence is weaponised as a result of both actor agency as well as constrained by the network structures in which they operate.

In simulating dynamics proposed in the framework by means of a game-theoretic model, which captures long running relationships of collaboration and defection in networks, the thesis motivates a theory of cyber power based on dynamic power relations. Focusing on US-China strategic competition, with espionage taking a central role as a form of statecraft in cyberspace, this thesis finds that great power cyber competition undermines trust in cyberspace. Drawing a link between volatile political behaviour and volatility in information networks, this thesis finds that a structurally volatile cyberspace, resulting from great power cooperative and coercive strategies, can undermine the ability to spy online.

Impact Statement

Thesis title: *A Political Economy of Digital Espionage*

In constructing a political economy of digital espionage, this thesis examines the dynamics of leverage in cyberspace between nation-states and private actors, and asks who profits from these dynamics. Using the topical backdrop of strategic competition between the US and China, the thesis situates the role of digital espionage in cyber statecraft, illustrates how states mobilise cyber power to spy, and discusses the impact on trust in information networks and evolving power structures. The thesis finds that strategies of great power competition undermines trust in cyberspace and, in some cases, the ability of public and private actors to gather intelligence. Actors must cooperate to advance trust-based cyber norms, and actors who can leverage their position in network structures at optimal times can improve their strategic postures to compete.

Academic contributions: Using concepts from dynamic international political economy, this thesis advances a new theory of cyber power where actors continually update their strategies based on their visibility of networks in which they interact. Through this, this thesis makes three salient academic contributions, adding to literature on cyber conflict and cyber power. First, a framework for explicitly linking trust and power in information systems contributes to multidisciplinary perspectives on trust vis-a-vis cyber statecraft. Second, an innovative model that captures collaboration and defection dynamics between using a game theoretic approach that allows for random action and long-running networks. Third, the concept of volatility in cyberspace, which affects the cost-benefit analysis of actors in

offence-defence operations.

Policy impact: For policymakers allocating resources to defend their infrastructure from cyberattacks, and forming strategies to gather intelligence, this thesis lays out the key challenges and identifies future work needed to model the capabilities of adversaries and allies. The academic contributions made can be used in combination with audience-specific methodologies, such as qualitative frameworks assessing cyber power and alternative competing hypotheses used in intelligence assessments, to directly advance policy initiatives concerning domestic and international security. In particular, policymakers may invest resources on advancing trust-based norms in cyberspace.

Real-world relevance: This thesis focuses on the US-China strategic competition dynamic, with reasoning on its impacts to their networked allies, such as key economic actors in global supply chains, as well as middle, rising, and non-aligned powers. Situating the thesis in the current geopolitical climate enables scholars and policymakers to use the concepts introduced here to adapt future responses to their own relevant policy contexts.

Acknowledgments

First and foremost, thanks to my supervisors, Professors David Pym and Madeline Carr, for their indefatigable support, humour, encouragement, feedback, and criticisms. David, in particular, for his support throughout the pandemic on a somewhat lonely journey, for insights into adjacent fields and recommending collaborators, and helping me secure research funding for my fellowship. Madeline, for her incisive feedback and inclusion into the RISCS community, and considerably improving my research abilities. Further thanks to Fiona Mannion, Dawn Bailey and Wendy Richards at UCL for critical administrative support.

To Professor Julian Williams, for his patience and energy in collaborating with an ever-changing set of challenges I presented him with, and for welcoming me into the Durham community, and sending me on various adventures, most recently to Ukraine. His friendship, encouragement, and perceptive abilities helped me navigate this journey with ease.

To Professor Helen Nissenbaum and the vibrant community at the Digital Life Initiative at Cornell Tech, who opened up many opportunities across the US East Coast, for feedback and always asking the right questions. In particular, to Michael Byrne, for his unconditional support and always propelling me forward. To Professor Alessandro Acquisti for always offering help and access to his brilliant group at CMU. To Wendy Grossman, Bruce Schneier and the wider Security and Human Behaviours Workshop community, for their interest in my work.

In particular, I am indebted to the late Professor Ross Anderson, for his humour, erudition, perspective, and for always treating me as an equal.

Ross immediately included me into communities at the Cambridge Computer Lab, FIPR, SHB, and at Churchill College, putting me on the spot, and ensuring I swam. I will sorely miss our conversations about which battle to fight next.

My examiners, Professors Sir Anthony Finkelstein and Tim Watson, for taking on a thesis which concerns our mutual interests and enriching it with their considerable experience. Conversations with Sir Anthony have guided this work into the zeitgeist and policy relevance. I thank them both for their enthusiasm.

Many thanks to former government colleagues in central government and the intelligence services, for honing the arguments and patience with my brain dumps. They know who they are, and I am grateful. Further thanks to colleagues at Privacy International and UK Research and Innovation, whose work always shed the right context. This work was supported by EPSRC funding to the UCL Centre for Doctoral Training EP/S022503/1. Further thanks to the wider security research community, anonymous reviewers as well as conference and workshop participants for their feedback.

Finally, I am grateful for the support of my family and friends. They have endured far too many conversations about networks, power, and Chinese hackers. Most of all, to Urban, for giving up his sleep and sanity to care for our newborn so I could write. His love and support lend meaning to all my endeavours.

Contents

Chapter 1

Introduction

In 2005, *Time Magazine* reported that a sole US defence contractor, aliased "Spiderman", had detected a number of hacked American military servers. Detailing the efforts of the FBI and wider US government in expunging from their computer networks a Chinese state-affiliated hacker group, monikered *Titan Rain*, the news report is credited for bringing 'cyber spies' into mainstream disccourse. Spiderman eventually becomes a subject of his own government's investigation, the article concludes, while paying scant attention to how the Titan Rain was able to infiltrate military systems, and exfiltrate aerospace and defence intellectual property in a sustained campaign. Chinese thinking on information warfare and deterrence,[1] consolidated in military analysts Qiao Liang and Wang Xiangsui's 1999 military text, *Unrestricted Warfare*, has evolved into expansive, cross-domain strategic en-

1. D Hodges Stiennon R. et al., *Cyber Warfare: A Multidisciplinary Analysis*, vol. 8 (IEEE Computer Society, 2013), 1210–1213.

gagement.[2]

Spying online is mostly legal,[3] and any strategic value gained from espionage uncertain.[4] As a practice of statecraft, espionage in cyberspace signals strategic intent in fulfilling political and economic national objectives by obtaining intelligence to compete. The ability to spy well, however, is also a function of the state's political and economic characteristics. Not all nation-states have access to the same coercive capabilities; not all nation-states have the ability to project coercive threat credibly, despite possessing the relevant offensive capabilities; not all nation-states have the ability to achieve concessions from an adversary, despite credible threats and relevant offensive capabilities.[5] As such, espionage as a practice has evolved operationally and strategically to both shape, and respond to, political and economic events.

Espionage campaigns have ramifications on strategic power competi-

2. Nathan Beauchamp-Mustafanga, "Exploring Chinese Thinking on Deterrence in the Not-So-New Space and Cyber Domains | The National Bureau of Asian Research (NBR)" [in en], in *Modernizing Deterrence: How China Coerces, Compels, and Deters*, ed. Roy D. Kamphausen, People's Liberation Army Conference (The National Bureau of Asian Research, February 2023), https://www.nbr.org/publication/exploring-chinese-thinking-on-deterrence-in-the-not-so-new-space-and-cyber-domains/.

3. M.N. Schmitt, "Cyber operations not per se regulated by international law" [in en], in *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, vol. 2017 (Cambridge University Press), 168–176.

4. Joe Devanny, Ciaran Martin, and Tim Stevens, "On the strategic consequences of digital espionage," Publisher: Routledge _eprint: https://doi.org/10.1080/23738871.2021.2000628, *Journal of Cyber Policy* 6, no. 3 (September 2021): 429–450, ISSN: 2373-8871, https://doi.org/10.1080/23738871.2021.2000628, https://doi.org/10.1080/23738871.2021.2000628.

5. Reid B. C. Pauly, "Damned If They Do, Damned If They Don't: The Assurance Dilemma in International Coercion," *International Security* 49, no. 1 (July 2024): New scholarship on linking threat credibility and coercion investigates scenarios, where ascertaining the costs of credibility in the coercer's assurance are imposed on the target. ISSN: 0162-2889, https://doi.org/10.1162/isec_a_00488, https://doi.org/10.1162/isec_a_00488.

tions, where misinterpretation of intent can lead to conflict escalation.[6] Furthermore, espionage campaigns have effects on the structure of cyberspace itself, as espionage compromises trusted information networks in cyberspace. Nation-states capitalise on insecure technology in partnership with proxy hackers and exploit vendors to develop and mobilise cyber power.[7] Concurrently, nation-states cooperate with, and coerce powerful private actors, such as technology platforms, to reshape global supply chains and secure strategic interests. Balancing the tension in these often contradictory roles inform states' competition strategies in cyberspace. This thesis examines these dynamics through the context of US-China strategic competition.

To address the central research question — what are the dynamics of leverage in cyberspace, and who profits — this thesis uses an integrated approach to international political economy, in considering both actors' agency in strategic competition, as well as the constraints to agency arising from limited visibility of the structures in which they operate, to construct a dynamic theory of cyber power. Other components of the integrated approach are also used; in particular, a multi-level concept of trust, power, cooperation and competition at global, national, regional and individual levels, interdisciplinary perspectives on trust and system stability, dynamism in interactions, and a focus on the interplay between domestic

6. Seumas Miller, "Cyberattacks and "Dirty Hands": Cyberwar, Cybercrime, or Covert Political Action?," in *Binary Bullets: The Ethics of Cyberwarfare*, ed. Fritz Allhoff, Adam Henschke, and Bradley Jay Strawser (Oxford University Press, March 2016), 0, ISBN: 978-0-19-022107-2, https://doi.org/10.1093/acprof:oso/9780190221072.003.0012, https://doi.org/10.1093/acprof:oso/9780190221072.003.0012.

7. Paul W. Thurner et al., "Network Interdependencies and the Evolution of the International Arms Trade" [in en], Publisher: SAGE Publications Inc, *Journal of Conflict Resolution* 63, no. 7 (August 2019): Using concepts in political economy have analytical precedents in assessments of arms trade evolution. ISSN: 0022-0027, https://doi.org/10.1177/0022002718801965, https://doi.org/10.1177/0022002718801965.

and global dynamics, which may be synthesised into policy outcomes.

Effective mobilisation of cyber power is necessary to mount espionage campaigns for intelligence gathering and strategic competition. As military, economic, political, and diplomatic competition domains are increasingly cyber-assisted, strategic competition occurs both in and through the cyber domain. Whether cyberspace is a legitimate competition domain, or merely a medium for facilitating competition in more traditional domains, is contested in literature. In Chapter 2, by developing some aims of statecraft in cyberspace, this thesis addresses whether claims that cyberspace as a competition domain are exaggerated, by presenting a view of cyberspace as a domain where ambiguous signalling may be manipulated for strategic advantage, and cyber power projection does not occur in a vacuum.

Connectivity of information flows in cyberspace requires actors to establish at least dyadic relations in a network, such that a communication channel can support the information flow. As such, a rudimentary form of trust must be established between senders and recipients of information. The use of technological capabilities necessary to subvert and control trusted information flows take on an economic character, as the knowledge of software vulnerabilities and commercial hacking and surveillance tools are in demand by public actors, and developed in partnership with, or supplied by, private actors. Competition in accessing and deploying these capabilities, as well as cooperation necessary in developing them, are necessary strategies of cyber power projection.

Specifically, the dynamics of leverage raise four research questions that this thesis seeks to answer (Figure 1.1). First, what is the role of trust in information networks in evolving interdependent power structures? Sec-

ond, what are the dynamics between public and private actors that enable strategic competition? Third, what is the role of private actors in developing offensive cyber capabilities necessary for nation-states to mobilise cyber power and conduct espionage? Fourth, what is the effect of power competitions, where espionage is used as a tool of cyber statecraft, on trust in information networks?

The thesis argues that nation-states form trust relationships with allies and private actors based on their domestic polities and economic structures, enabling coercion in cyberspace. Through a central conceptual framework linking trust and power in information systems, and examining causal relationships by means of an illustrative game-theoretic model, the thesis finds while leveraging trust relationships allows nations to compete, strategic competition undermines trust and creates volatility in information networks in cyberspace, contrary to expectations of Internet fragmentation. As such, the answer to who profits as a consequence of these dynamics, is contextual and counterintuitive, as the actors capable of manipulating volatile information networks in their strategic favour are best placed to compete, but volatility can make competition costlier.

The contributions made through this thesis are understood in the context of significant evolutions in the international political, economic, and technological domains. In twenty years since the public attribution of *Titan Rain*, Chinese offensive cyber activity has evolved over a backdrop of numerous geopolitical and economic shocks, and technological advancements. Campaigns such as GhostNet (2009), Aurora (2010), RSA (2011), APT-1 compromise of the US Office of Personnel Management (2014), to the APT-31 hack on the UK Electoral Commission (2024) amongst other Five

Eyes, South East Asian, European, African and Latin American targets,[8] are testament to China's growing national cyber power.

Significant international and domestic political events have contributed to the rise of China: its divergence with the West in the aftermath of the 2008 Global Financial Crisis, the global reach of the Belt and Road Initiative, influence-building through foreign policy, such as infrastructure investments in the South American and African continents, and trade conflicts with the US, have added a significant political dimension to its pervasive economic espionage initiatives.[9] With new and numerous public and private targets, the strategic, operational, and tactical characteristics of spying have evolved, with some analysts attributing over 50 APT groups as presently affiliated with the Chinese state,[10] despite its 2015 detente agreements with the Obama administration.

In three decades, the World Wide Web, envisioned as a distributed and decentralised communication system, has transformed into centralised but interdependent nodes of power, where end-point devices relay information flows to dominant platforms for social networking and payment systems. The techniques, tactics and procedures (TTPs) of offensive cyber activity aimed at controlling these information flows engage critical points of interdependence in global supply chains. These critical points, which have attractive economic or political properties to coercers as a result of their

8. Lior Rochberger and Daniel Frank, *Operation Diplomatic Specter: An Active Chinese Cyberespionage Campaign Leverages Rare Tool Set to Target Governmental Entities in the Middle East, Africa and Asia*, accessed October 30, 2024, https://unit42.paloaltonetworks.com/operation-diplomatic-specter/.

9. Alex Younger, *We must confront China over security — but co-operate with it too*, September 2023, https://www.ft.com/content/b01a5e6a-1a59-4eb1-8add-415e64dbda37.

10. Insikt Group, *Charting China's Climb as a Leading Global Cyber Power'* [in en], Recorded Futures. Available at: 2023, https://www.recordedfuture.com/charting-chinas-climb-leading-global-cyber-power.

structural positions, either serve as a direct target, or as a cheaply compromised indirect entry point. The emergent trend of using vulnerable networks rather than targeting resourceful actors directly has made network exploitation more accessible to coercers. Techniques of lateral movement, such as Chinese actors 'living off the land' after initial network access,[11] scale up the scope for data exfiltration at lower cost, as they use tools already available in the network, compromising unintended targets and escalating privileges gained from initial access to reach an intended target.

States target adversaries, such as strategic competitors, directly, or by targeting valuable private actors in global supply chains. The resulting complexity of offense-defence relations has spawned an industry that supports espionage, comprised of open and closed markets, and non-market information flows for selling offensive cyber capabilities and knowledge of unpatched vulnerabilities. Nation-states, proxy hackers, security researchers and exploit vendors, and tech platforms are all participant actors with agency operating in their own complex ecosystems. Each ecosystem has political and economic dynamics of its own that nation-states must manipulate to obtain resources necessary for espionage in order to successfully impose security costs onto their adversaries.

States must balance coercing private actors with incentivising them. This strategic balance varies between state actors, based on domestic political institutions, economic, and foreign policies. Systems of government with centralised power, like China, can coerce rapidly and risk stability, as they seek to suppress domestic dissent. At the same time, such gov-

11. *Joint Cybersecurity Advisory: People's Republic of China State-Sponsored Cyber Actor Living off the Land to Evade Detection*, technical report Ver 1.1 (Five Eyes, June 2023), accessed July 17, 2023, https://media.defense.gov/2023/May/24/2003229517/-1/-1/0/CSA_PRC_State_Sponsored_Cyber_Living_off_the_Land_v1.1.PDF.

ernments have more reason to spy, as they do not historically possess the entrenched passive surveillance capabilities of intelligence allies, such as the Five Eyes. Yet analysts suggest that Western governments were, until recently, the biggest consumers of spyware.[12]

These dynamics lend espionage with political and economic operational properties. As a coercive competition strategy, espionage foremost aims to reduce information asymmetries about an adversary or impose new asymmetries, in contrast to cybercrime, which intends to sabotage or extort, or fraud. Coercion in cyberspace can act as a low intensity signal of power projection in cyberspace, suffering reprisal that may contain escalation in other domains. As an intelligence methodology, espionage reduces information asymmetries created by the adversary to enable a coercer to project power in military, political, or economic domains. By creating or aggravating information asymmetries in its own favour, the coercer imposes the cost of correcting the resulting imbalance upon its target, if the target has the resources to detect and respond. In enacting a counter-espionage strategy, the coercer hopes to reduce long-term defensive costs it incurs itself. The coercer may achieve this advantage by either encouraging proxy actors to intervene on its behalf, or by procuring or developing offensive cyber capabilities in partnership with national security allies or on its own. The operational logic of coercion lends espionage its economic character.

Operationally, the offensive cyber capabilities needed to sustain an espionage campaign concerns some economic good: a commodity that private actors develop or exploit on behalf of the public actor, such as commercial

12. S.F. Kot and Brian, *Why Does the Global Spyware Industry Continue to Thrive? Trends, Explanations, and Responses, Carnegie Endowment for International Peace* [in en], Available at: 2023, https://carnegieendowment.org/2023/03/14/why-does-global-spyware-industry-continue-to-thrive-trends-explanations-and-responses-pub-89229.

spyware, or the knowledge of an unpatched vulnerability in target infrastructure cultivated by a public actor into a 'vulnerability equity', to be disclosed, developed, or deployed. Disclosure makes the knowledge public, and contains the risk of the adversary exploiting the vulnerability. However, the competition to control information flows may not directly leverage cyber power, but use other tools of statecraft, such as legal, regulatory, and diplomatic tools. These tools open up the potential for collaboration and cooperation between allies, drawing on collective effort to compete. Internet governance proposals at multilateral levels, tools of economic coercion, such as the export control of spyware, or legal regimes, such as the mandatory disclosure of software vulnerabilities, require collaboration domestically as well as with intelligence allies. As such, cyberspace, having long acted as a conduit for leverage across military, diplomatic, technological, and other competition domains, is itself a legitimate power competition domain.

First, establishing cyber norms for espionage conflict with state secrecy,[13] allowing great powers to intensify their offensive campaigns. Political behaviour and strategic stability then impacts the stability of information networks in cyberspace. Misinterpreting intent to espionage could escalate conflict or risk reprisal through other domains. Second, the offensive capabilities deployed require some prior intelligence of the target's

13. Sebastian Harnisch and Kerstin Zettl-Schabath, "Secrecy and Norm Emergence in Cyber-Space. The US, China and Russia Interaction and the Governance of Cyber-Espionage," Publisher: Routledge _eprint: https://doi.org/10.1080/17419166.2022.2097074, *Democracy and Security* 19, no. 1 (January 2, 2023): 82–110, ISSN: 1741-9166, https://doi.org/10.1080/17419166.2022.2097074, https://doi.org/10.1080/17419166.2022.2097074; Martin Libicki, "The coming of cyber espionage norms," in *2017 9th International Conference on Cyber Conflict (CyCon)*, ISSN: 2325-5374 (May 2017), 1–17, https://doi.org/10.23919/CYCON.2017.8240325, https://ieeexplore.ieee.org/abstract/document/8240325.

defensive posture, likelihood of discovery, and risk of failure to deploy to the target or to exfiltrate data. Developing and deploying such capability signals the coercer's resources of time and resources to mitigate against the underlying vulnerability in the target technology being patched. Credible espionage campaigns can be assessed as a more faithful representation of offensive national cyber power.

Third, espionage campaigns are mounted with an intent to close some leverage deficit. Where the coercer lacks resources in economic or military domains to mount a credible deterrent or threat, cyber espionage campaigns may signal to the target confirmation of the coercer's leverage deficit, and as a result, vulnerabilities in its wider competitive arsenal. Fourth, while it is difficult to attribute strategic success in any domain explicitly or solely due to an espionage campaign, it can nonetheless contribute to erosion in a target's sources of national power by targeting critical and public infrastructure[14]regardless of eliciting concessions.

This thesis contributes to a growing literature on power competitions and stability in cyberspace as a domain of strategic significance[15] by contributing a dynamic international political economy perspective on cyber power. Realist and structuralist political economy theorise conflict in cyberspace. The 'cybersecurity dilemma'[16] examines the value of a state's offensive cyber attacks in order to defend itself, at the risk of undermining 'system stability'. The dilemma grows weaker or stronger based on the context of strategic competition, but the defensive realist methodology

14. R.J. Harknett and M. Smeets, "Cyber campaigns and strategic outcomes" [in en], *Journal of Strategic Studies* 45, no. 4 (2022): 534–567.

15. David V Gioe and Margaret W Smith, *Great Power Cyber Competition: Competing and Winning in the Information Environment* (Taylor & Francis, 2024).

16. B. Buchanan, "The Cybersecurity Dilemma: Network Intrusions" [in en], in *Trust, and Fear in the International System, in King's* (College London, 2016).

overlooks structural effects as a result. On the other hand, US-China leverage their structural advantage to coerce interdependent information flows in static networks, according to 'weaponised interdependence',[17] yet this approach is limited in explaining how networks evolve dynamically as interdependence changes, which may explain real-world scenarios of strategic choice.

These gaps motivate the trust-interdependence-power framework, which is the key conceptual development used to develop a dynamic theory of cyber power. The innovation is in a dynamic network game-theoretic set up, that enables actors to enact strategic intent with varying levels of effort. The second conceptual development is using the concept of volatility through network defections, that links strategic stability with cyberspace stability. Power competitions undermine trust in cyberspace, resulting in actors unable to anticipate security costs of network defections, and a 'structurally volatile' cyberspace. The thesis concludes with arguing that a volatile cyberspace may not support espionage, and simultaneously intensify offensive cyber activity and decrease trust. The conceptual contributions may assist security and international studies scholars in reasoning about cyber power given the context of a nation-state's allied and adversarial relationships. Policymakers may use these concepts to allocate offence-defence resources in a strategic manner, propagate trust-building cyber norms, and adapt the strategic logics presented here to their policy contexts.

17. Henry Farrell and Abraham L. Newman, "Weaponized Interdependence: How Global Economic Networks Shape State Coercion," *International Security* 44, no. 1 (July 1, 2019): 42–79, ISSN: 0162-2889, accessed July 17, 2023, https://doi.org/10.1162/isec_a_00351, https://doi.org/10.1162/isec_a_00351.

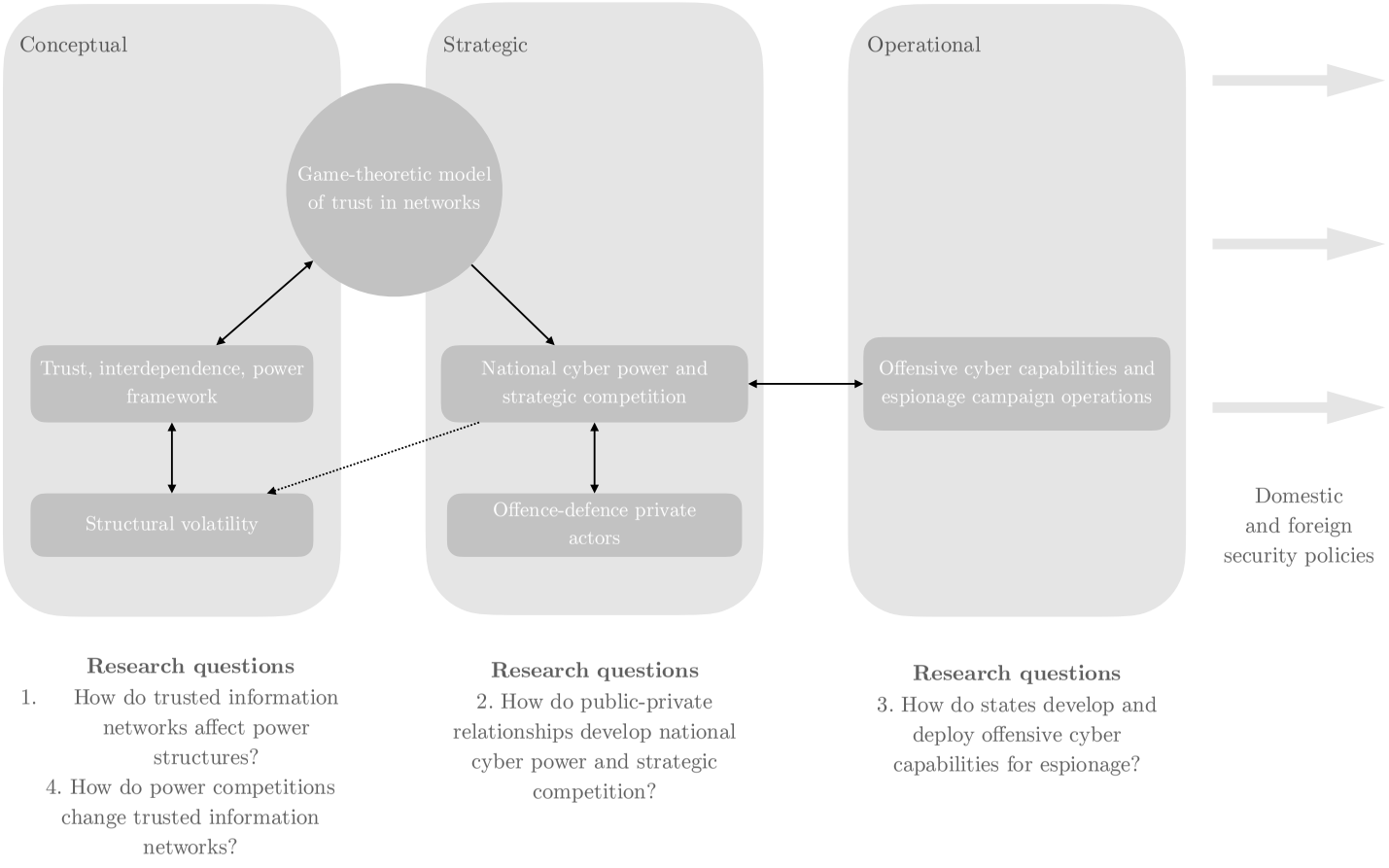


Figure 1.1: Research overview: What are the dynamics of leverage in cyberspace?

1.1 Methodology and sources

Governments struggle with effective responses to destabilising cyber attacks for many reasons; discerning attacker intent, mitigating risks to networked actors, and constructing reprisal framework that minimise costs imposed to the attacker on their own security owing to interdependence, are key considerations in exercising restraint.[18] Nonetheless, the damaging effects of cyber-attacks result in decreasing societal trust may be longer-term than the immediate effects of sabotage or infrastructure downtime.[19] Yet, while these cases motivate some causal relations between compromised technological trust and erosion of social and political trust, explicit links between different theoretical conceptions of trust remain to be made.

Long-established concepts in cybersecurity, international relations, and political science have now found application overlaps in state cyber operations. To seek insight into how states spy online requires scrutiny of the underlying dynamics in their relationships with other states, as well as with and between private actors. Multidisciplinary trust concepts must reconcile political trust between states, with trust in their societies, through technological trust in information systems. The links between strategic and cyberspace stability through trusted information flows are yet to be made explicit. The dynamic evolution of network structures, and their role in

18. Monica Kaminska, "Restraint under conditions of uncertainty: Why the United States tolerates cyberattacks" [in en], *Journal of Cybersecurity* 7, no. 1 (February 2021): tyab008, ISSN: 2057-2085, 2057-2093, https://doi.org/10.1093/cybsec/tyab008, https://academic.oup.com/cybersecurity/article/doi/10.1093/cybsec/tyab008/6162971.

19. Ryan Shandler and Miguel Alberto Gomez, "The hidden threat of cyber-attacks – undermining public confidence in government," Publisher: Routledge _eprint: https://doi.org/10.1080/19331681.2022.2112796, *Journal of Information Technology & Politics* 20, no. 4 (October 2023): 359–374, ISSN: 1933-1681, https://doi.org/10.1080/19331681.2022.2112796, https://doi.org/10.1080/19331681.2022.2112796.

enabling strategic engagement is central to domain power. This is the reason for proposing a novel conceptual framework for assessing the dynamics of leverage, over adapting any single, field-specific theory.

This thesis adopts mixed methods. Chapter two uses concepts from dynamic international political economy to develop a framework which presents trust as a process, rather than a property, necessary to connect information flows and establish network interdependence. The central claim made in this chapter is that states exploit trusted information flows to enact strategies of cooperation and coercion vis-a-vis competitors and ecosystems of private actors, and the methods of exploitation are based in national objectives determined by their domestic political economies. The framework synthesises realist concepts, such as the cybersecurity dilemma, and structuralist concepts, such as weaponised interdependence, to fill gaps in both theories; specifically, the strategic nature of actor interaction substantiated through network structure, and the dynamic evolution of these network structures, respectively. The chapter concludes by arguing that fragmentation outcomes in cyberspace need to be mitigated through trust-building in political and information systems, where weaponising interdependence to project power is reliant on public-private actor relationship configurations.

Chapter three validates this framework by providing a richer, contextual simulation of network evolution through game theoretic models of cooperation and defection in information networks. The innovative features of these games reflect nuances in the conceptual framework. Agents in long-running networked ecosystems are allowed random action and limited visibility of the network structure in making decisions to cooperate or defect. Agents tradeoff expected payoffs from defection with increasing effort to cooperate,

benefiting from the resulting public good, by anticipating the behaviour of other agents and, through backward induction, formulate optimal strategies in game iterations by planning ahead. Network structures are assigned to public-private actor contexts. Defection behaviour and network evolution as a result yield two significant outcomes. First, that as agents occupy every node in the structure due to the network's long-running behaviour, the agents potential for random action implies that no dominant steady state of power configuration is achieved. Second, that nodes closer to networks are more susceptible to policy interventions than more randomly dispersed nodes.

Chapter four is comprised of three essays. The first essay uses weaponised interdependence as a proof of concept in developing a dynamic theory of cyber power in static information networks. In particular, the examination of the supply-demand of commercial espionage capabilities, such as spyware, and the knowledge of software vulnerabilities, and how the US and China exploit their structural advantages to develop offensive cyber capabilities. The second essay uses the results in Chapter two and three to extend the proof of concept to dynamic structures. In particular, the application of the conceptual framework examines the operational styles of APT groups, such as their use of common tooling and infrastructure to mount espionage campaigns vis-a-vis their proximity to state sponsors. The third essay investigates the reverse direction of the conceptual framework to develop a more subtle outcome than fragmentation of trust relationships under strain from power competitions. In particular, the second novel concept of structural volatility is introduced, where the effects of great power competitions in cyberspace reduce trust for all actors, providing an explicit link between

strategic and cyberspace stability. Policy contexts, such as vulnerability equity disclosure, are assessed in the conclusion.

Over the thesis, the cross-domain competition between the US and China, and their strategic allies, is used as a running example. This necessitates a diversity of sources. In addition to English language publications in peer-reviewed journals, conferences, and workshops, Chinese language publications, especially in Chapter 4.2, are used to gain insight into Chinese scholarship on Western cyber postures. A UCL-provided proxy was used to access an archive of Chinese journal publications through the WanFeng gateway. Translation facilities and the contextual use of Chinese terminology were provided by Google Translate and ChatGPT. To ground the use of frameworks and models in real-world scenarios, technical reports from security researchers, threat intelligence analysts, government publications, and some news sources, publicly available until November 2024, are added to the analysis to provide context. As such, the limitations in the use of real-world examples are confined by the use of publicly available data; nonetheless, the framework and model provide some contextual rigour to hypothesise actor strategies, which may be validated in future as more data becomes public.

1.2 Definitions

Chapter-specific definitions are indicated in context. However, setting out preliminary definitions gives the reader a sense of the scope of this thesis, and to appreciate its corresponding limitations.

Digital espionage refers to the use of digital technologies and cyber-

assisted means to gain unauthorised access to a computer or computer network for the express purpose of surveillance or data exfiltration. The use of digital espionage markets refers to socio-technical ecosystems of actors in cyberspace and the supply-demand of offensive cyber capabilities developed by them in a market structure for the purpose of digital espionage. In particular, this definition extends espionage beyond the individual scope, as individual actors cannot produce espionage capabilities in isolation, to an operational tool to gain leverage in strategic power competitions.

Leverage is used in a normative sense in the context of this thesis, of using resources or exerting effort in a strategic manner to achieve advantage in a competitive situation. In particular, the thesis is concerned with the development and use of digital espionage capabilities as 'levers' by nation-states in service of their national objectives and achieving competitive advantage in political, economic, or military domains.

Public actors are actors belonging to one or more states, sometimes referred to as state actors when the atomicity of the public actor is indistinguishable. The use of 'public' is derived from their incentives to produce public welfare outcomes. Similarly, the use of 'private' actors refers to the property of information flows kept restricted to the actor to produce an economic good for profit-seeking. However, the public-private boundary is not always well-defined, such as in instances of espionage operations where transnational actors and other actors who covertly receive state sponsorship may be involved. The overlap between private and public, and relativity in these concepts, are discussed in Chapter 2, as conceptions diverge in the US and Chinese contexts, where the state takes different roles.

Information has various literature-specific definitions, but is referred

here in the sense of aggregated knowledge, as specified in Chapter 3. Interdependence refers to the connectivity of information flows within and across networks through one or multiple network nodes, where actors in one network rely on node to flow information to actors in other networks. Contextual definitions of interdependence are provided in Chapter 2, where a canonical description of interdependence is expressed in terms of the opportunity cost borne by actors in breaking interdependence. In Chapter 2, trust is formulated to describe a basis for information sharing, such that the result is the production of a public or commercial good. In this sense, interdependence defined as the shared welfare or profit from this good is compatible with canonical descriptions. Power and power projection refer to the capacity of an actor to develop capabilities as a product of interdependence, individual resources and partnerships of capabilities an actor can develop, and the mobilisation of this capacity in deploying these capabilities to achieve strategic outcomes, respectively.

The term 'advanced persistent threat' refers to actors that either belong to the state, work in partnership with the state, or are non-aligned, but possess significant offensive cyber capabilities, which they deploy systematically over long-running campaigns for strategic political or economic, or profit-seeking purposes. Security researchers encompasses a broad spectrum of cybersecurity analysts, from intelligence analysts to malware reverse-engineers, but they are used in the context of private actors that sell analyses to other private and public actors, or work in the open.

Active surveillance refers to the use of computer hacking for surveillance; passive surveillance refers to long-standing agreements between telecommunications and internet service providers, and public actors, where wiretap-

ping and backdoors provide monitoring without active compromise measures such as hacking. 0-days refers to unpatched vulnerabilities in software of which the manufacturer is unaware; an exploit refers to the conversion of the knowledge of vulnerabilities into software that provides unauthorised computer network access; malware refers to exploits which serve an attacker's malicious intent. The collective term for tools that compromise, surveil, and exfiltrate a computer network is referred to offensive capabilities. Where the underlying intent in a cyber-attack is unclear, it is referred to as offensive cyber activity.

Topologies, configurations, and 'horizontal-vertical relations' are variously used to reference the topology of a network within which nodes are connected to pass information that intuit some hierarchy or governance over information flow directions. Structures are used in the dual sense of international relations, to define relationships between actors, as well as in a more thin, technical sense, of the arrangement of networked information flows. Unless indicated otherwise, networks operate within or across information systems, such as cyberspace. Ecosystems are defined as an organised collection of systems, interdependent through networked information flows, as conceived by Adner.[20]

Finally, Chapter 4 introduces the concept of 'structural volatility' in cyberspace. While the concept is developed and defined within the chapter, volatility refers to the unstable nature of maintaining trusted information flows in networked structures due to several reasons, but particularly the complexity in discerning the reliability of an actor's signals.

20. R. Adner, "Ecosystem as Structure: An Actionable Construct for Strategy"' [in en], Available at: *Journal of Management* 43, no. 1 (2017): 39–58, https://doi.org/10.1177/0149206316678451., https://doi.org/10.1177/0149206316678451..

The complexity of actor interactions throughout this thesis necessitates a note on the scope of the thesis in omitting a thorough investigation of cybercriminals and well as the investigation of the impact of espionage on civil society actors. These have an extensive pedigree in literature, particularly in the aftermath of the impact of the Pegasus malware on journalists, politicians, and dissidents. However, they are excluded from explicit analysis, as they arguably do not play a direct role in states gaining strategic advantage in power competitions, but assist states in their influence-building initiatives. As such, the epistemological choice of the title in using the indefinite article “A", rather than “The" is a deliberate one. Furthermore, this thesis refrains from making value judgments on democratic or autocratic systems of government; instead, it is concerned with contrasts in the topologies of their respective domestic and foreign relationships, and possible limitations in manipulating information flows to their advantage as a result.

Chapter 2

Trust, interdependence, and power in cyber statecraft

This chapter was presented and discussed at the European Cyber Conflict Research Initiative Fall Workshop 2024.

2.1 Overview

This chapter establishes the key conceptual framework used in the thesis as an analytical basis. The central question this chapter addresses is the role of a dynamic political economy in cyber statecraft. How do nation-states leverage domestic political institutions and economic policies to establish credible cyber deterrents over their competitors to project power in cyberspace?

The argument proceeds in the following steps: first, based on a discussion of key geopolitical, economic, and technological events, contrasts between economic and cyber statecraft reveal that multilateral attempts to define normative cyberspace behaviours have had limited success. This

discussion contributes to the literature on national security and political economy.

A conceptual framework links the notion of power in information systems with the view of trust as a process established in information transactions. Trust is a contested and multivariate concept, and key security, political, and economic literatures are synthesised. A systemic and contextual definition of trust is proposed, based on which, possible structures of interdependent information flows are discussed. The relative position of actors in interdependent network structures determines their ability to project power.

Strategies of coercion and cooperation are developed as capabilities achieved through structural advantage. The use of coercive and cooperative strategies on private actors to achieve leverage in power competitions is discussed. Finally, espionage, as an intelligence-gathering practice where the flow of necessary technologies are subject to competition dynamics, is situated within the concepts of cyber statecraft introduced here. This chapter sets the foundation for discussing how topologies of cyberspace structures change over time as a result of trust dynamics, modelled in Chapter 3, and the implications on power relations, analysed in Chapter 4.

Abstract:

What is the role of political economy in cyber statecraft? Nation-states develop, exercise and restrict the use of offensive and defensive capabilities in cyberspace to meet their strategic objectives. To do so, they rely on a number of private actors; a state's ability to coerce them is governed by structural variables of trust, interdependence, and power in state-state and state-private relations. We analyse these relationships through a concep-

tual framework that theorises political, social, economic, and technological trust within cyberspace as an information system. Contrasting Chinese and Western cyber ecosystems, we find that leveraging domestic political economy is key in projecting national cyber power, at the cost of adverse structural outcomes, such as asymmetry, volatility, and potential fragmentation in cyberspace. Implications for coercive and cooperative strategies, and the future of cyber statecraft are discussed.

2.2 Introduction

There is no salient political theory of cyber statecraft. What makes a state more prone to conflict in cyberspace? What makes states such as North Korea decide that the use of highly destructive, yet lucrative, denial-of-service or extortion attacks, such as ransomware, are appropriate instruments of statecraft, while others such as Russia and China use their capabilities to target dominant tech platforms and global supply chains through sophisticated "living-off-the-land" techniques? Why do some prefer to have stronger defensive postures than offensive capabilities, such as Germany prior to its 2023 *Zeitenwende*? Why do seemingly liberal democracies engage in the facilitation of spyware on their civil societies? Understanding state intentions in cyberspace is increasingly necessary due to the "high risk of misperception" and potential for conflict escalation.[1]

States adopt varying heuristics in conducting relations with others over cyberspace: some may see it as a continuation of long-standing "information operations" to maintain or increase dominance, others as newer ground for

1. Erica D. Borghard and Shawn W. Lonergan, "The Logic of Coercion in Cyberspace," *Security Studies* 26, no. 3 (2017): 452–481, https://doi.org/10.1080/09636412.2017.1306396, https://doi.org/10.1080/09636412.2017.1306396.

espionage, coercion or subversion, and still others as a means for strategic advancement through intellectual property theft, extortion, or expanding foreign influence. The use of statecraft in cyberspace may signal political, military or economic intentions in other domains. We define cyber statecraft as any methodology deployed in, on, or using tools of cyberspace to secure a state's national interests domestically and overseas, by achievement of some political, economic, societal, or technological strategic goal [2]

Parallels with economic statecraft are natural. Both strategically deploy instruments to deter, engage, or debilitate another; the use of Stuxnet, attributed to the US and Israel, in neutralising Iran's nuclear centrifuges is a canonical example. Post-1945, theories of economic statecraft and national security were postulated and evolved in the shadow of the Cold War. Notably, the centrality of power to the political economy of international relations (Knorr, 1975), with contemporaneous formalisms between power and interdependence (Keohane and Nye Jr, 1977), and theories of economic sanctions (Baldwin, 1985) led the way for reconciling national security issues through instruments of statecraft between two ideologically opposed and economically independent superpowers.

In the aftermath of Perestroika, security studies literature took momentum within the liberal perspective of political economy (Gilpin, 1987), promoting and reinforcing economic inducements of free trade and glob-

2. Economic, political or technological conflict is mediated through interdependence in cyberspace: in strategic competition over control of semiconductor supply chains for greater compute, market domination over electric vehicle and associated consumer data, subsidies in tech sector investments, and trade reciprocity in the use of consumer tech apps such as TikTok or WhatsApp in US and Chinese digital marketplaces respectively, can all indirectly impact and influence strategic success. Legal instruments, such as China's new counter espionage laws targeting foreign businesses, also have second-order effects in gaining leverage.

alisation, and punishment such as sanctions[34] to uphold Western security interests for the first two decades of the 21st century. However, the perceived rise of China, strengthening alliances such as BRICS and SCO, and Russian military interventions in Ukraine and Georgia, amongst domestic factors in the West, particularly increasing economic inequality since the 2008 financial crisis, have led political scientists to pursue structural perspectives at the nexus of economic statecraft and national security, revisiting and revising the "weak effects" of interdependence under US hegemony during peacetime.[5]

Interdependence in cyberspace remains understudied explicitly. Recent literature on coercive strategies based on weaponised interdependence[67] has been applied to domains of surveillance,[8] governance of Internet platforms,[9] telecommunications rivalries,[10] semiconductor manufacturing and

3. Daniel W. Drezner, *The Sanctions Paradox* [in fr], Cambridge Books, Cambridge University Press, number 9780521644150. 1999.

4. Jean-Marc F. Blanchard, Edward D. Mansfield, and Norrin M. Ripsman, "The political economy of national security: Economic statecraft, interdependence, and international conflict," *Security Studies* 9, no. 1 (September 1999): 1–14, ISSN: 0963-6412, 1556-1852, accessed April 12, 2024, https://doi.org/10.1080/09636419908429393, http://www.tandfonline.com/doi/abs/10.1080/09636419908429393.

5. K.N. Waltz, "Structural Realism after the Cold War"' [in en], *International Security* 25, no. 1 (2000): 5–41.

6. Farrell and Newman, "Weaponized Interdependence."

7. T. Oatley, "Toward a political economy of complex interdependence"' [in en], Available at: *European Journal of International Relations* 25, no. 4 (2019): 957–978, https://doi.org/10.1177/1354066119846553., https://doi.org/10.1177/1354066119846553..

8. H. Farrell and A.L. Newman, "Of Privacy and Power: The Transatlantic Struggle over Freedom and Security"' [in en], in *Of Privacy and Power*, Available at: (Princeton University Press, 2019), https://doi.org/10.1515/9780691189956., https://doi.org/10.1515/9780691189956..

9. N. Tusikov, "Internet Platforms Weaponizing Chokepoints" [in en], in *The Uses and Abuses of Weaponized Interdependence*, ed. D. Drezner, H. Farrell, and A. Newman (Washington, DC: Brookings Institute Press, 2021), 133–148.

10. A. Segal, *Huawei, 5G, and Weaponized Interdependence'* [in en], ed. D.W. Drezner, H. Farrell, and A.L. Newman, Available at: 2021, 149–166, https://www.jstor.org/stable/10.7864/j.ctv11sn64z.10.

global supply chains,[11] and as policy responses to Chinese governance models.[12] "Weaponised interdependence" suggests that nation-states weaponise power asymmetries entrenched in globally networked ecosystems — such as the global financial system or the Internet — acting as 'panopticons' or 'chokepoints' to funnel or restrict information flows respectively.

The late 1990s emergence of early e-commerce platforms was revitalised by REST APIs in the mid 2000s, propelling social media websites into advertising powerhouses. Software businesses such as Apple and Microsoft diversified into tech ecosystems offering a series of interconnected products, despite anti-trust concerns. Similar digital marketplaces appeared in China and Russia, albeit with alternative domestic competition policies and state interventions. Despite the distributed architecture of the Internet, power concentrations have become centralised in such tech platforms. Any conception of "great power cyber competition" in the realist tradition,[13] is bounded by the constraints owing to Internet topology, its dominant private actors, and anarchical behaviour in cyberspace.

Unlike its economic analogue, cyber statecraft has no enduring collection of multilateral bodies that capture, define, or defend evolving normative behaviours in line with technological and geopolitical changes. Whilst the UN ITU and GGE bodies propose cyber norms and remain important forums for transnational debate on the Internet's balance of power, even

11. L.S. Chen and M.M. Evers, ""Wars without Gun Smoke": Global Supply Chains, Power Transitions, and Economic Statecraft"' [in en], Available at: *International Security* 48, no. 2 (2023): 164–204, https://doi.org/10.1162/isec_a_00473., https://doi.org/10.1162/isec_a_00473..

12. Victor D. Cha, "Collective Resilience: Deterring China's Weaponization of Economic Interdependence," *International Security* 48, no. 1 (July 1, 2023): 91–124, ISSN: 0162-2889, https://doi.org/10.1162/isec_a_00465, https://doi.org/10.1162/isec_a_00465.

13. Gioe and Smith, *Great Power Cyber Competition: Competing and Winning in the Information Environment*.

according to Tallinn 2.0, "cyber operations are not per se regulated by international law".[14] Espionage, in particular, a ubiquitous tool of statecraft, is notoriously resistant to norm emergence and governance[15].[16] The alignment of private sector incentives with contrasting views of states such as the US or the UK, that purport to prioritise a "whole of society" and "responsible power" approach in cyberspace, as opposed to those that take the view of "strategic autonomy" and "sovereignty" in cyberspace above all, remains elusive.

As a result, the relationships between state actors and private actors, such as tech platforms and third party groups that supply or exploit cyber capabilities, are largely self-determined and self-governing. As Chen and Evers point out, "business-state relations ... shape the effectiveness of economic statecraft" and "... as two [rising and dominant] states ... seek to maximise their relative power ... resulting disruption to profits leads high-value businesses to develop more conflictual relations with the dominant state in which they are based." States must contend with domestic economic challenges posed by businesses while balancing foreign policy objectives. Those especially susceptible to protectionism in trade policy face the increased cost of breaking out from interdependent structures, and use cyber statecraft as a potential means of reducing this cost.

In cyberspace, primarily a system of interdependent information flows, states' abilities to exercise coercion or cooperation strategies to achieve do-

14. Schmitt, "Cyber operations not per se regulated by international law."

15. R. Buchan and I. Navarrete, "Cyber espionage and international law"' [in en], in *Research Handbook on International Law and Cyberspace*, Available at: (Edward Elgar Publishing, 2021), 231–252, https://www.elgaronline.com/edcollchap/edcoll/9781789904246/9781789904246.00021.xml..

16. Harnisch and Zettl-Schabath, "Secrecy and Norm Emergence in Cyber-Space. The US, China and Russia Interaction and the Governance of Cyber-Espionage."

mestic or foreign security objectives depend on navigating trust and power relations with key private actors, as well as adversarial or allied states. In this chapter, we present a conceptual framework on the effect of trust relations on cyber power, public-private interdependence, and accordingly, evolving cyber statecraft. Trust, an independent variable, is presented as a systemic process that preserves the properties of information flowing between two agent(s) as remaining private or public. The process may be used by the agent to signal their trustworthiness, forming cooperative relations and fomenting interdependence, and the resulting structural implications on power (Figure 2.1).

Seeing trust as a systemic process rather than just a normative phenomenon allows us to reconcile its extant formulations: as a concept in computer network security; as a political or personal social phenomenon; and as an action of economic agency. This may help in explaining perceived inconsistencies in an agents behaviours towards other agents, for instance, states increasingly form relationships based on a wider set of choices rather than relying the influence of a single power axis, as well as structural implications on power of trust relations shifting from "what to trust" to "who to trust", as seen through network effects on social media. Yet, the scope of this conceptualisation of trust may raise objections from normative or sociological views of the 'degree' of trust: how to quantify trust with regards sharing information with an actor, and what the content of this information might be. Conceptualising trust as a process in this framework is a conceit used to explain how interdependence of information networks is formed. As such, the execution of this processes repeatedly over time is both critical to the fidelity of the information passed between trustor and trustee, but

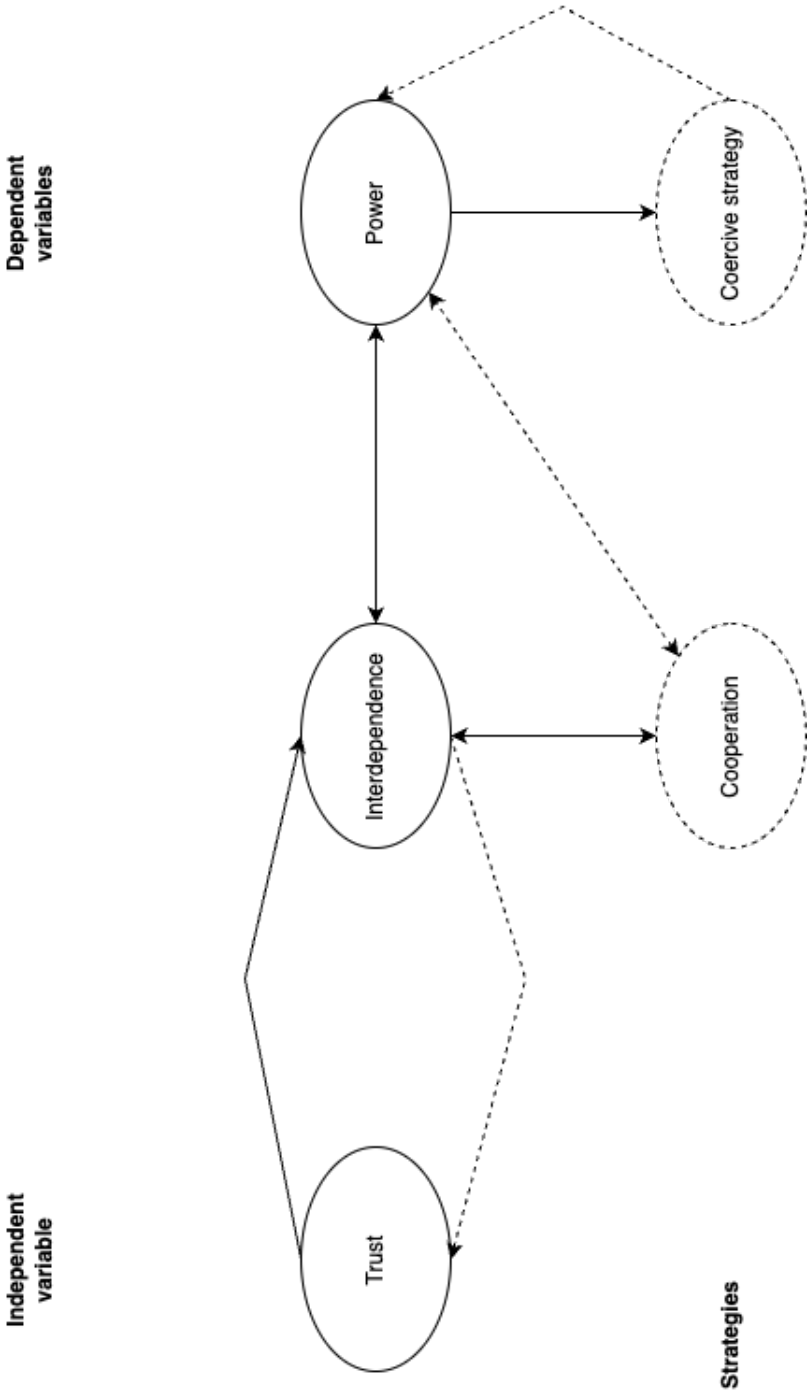


Figure 2.1: A conceptual framework in an information system highlighting the structural dependence of the systemic variable, power, on the process variable, trust, through new and established interdependences. An actor's ability to deploy and leverage strategies such as cooperation or coercion depend on its structural position vis-a-vis interdependence and relative power.

makes the content of the information itself as verifiable implicit, as it is dependent on the beliefs of the trustee to continue interacting with a trustor — or the recipient of information to continue interacting with a sender — based on the value gained from the information exchange for both actors.

The exploitation of these trust relationships, through "influence operations" that redirect information flows in favourable directions, or direct coercive strategies in the form of offensive cyber operations, form the basis of cyber statecraft. For example, a state like North Korea, which has no trust relationships, and therefore interdependences, with Western allies, has impunity to exercise coercive cyber power in the extreme by using ransomware to target its adversaries' civil society, as seen in the WannaCry case. It may impose the maximum possible cost on its adversaries, short of escalating into armed conflict or other severe war-fighting strategies.

On the other hand, among the Five Eyes, trust relationships formed as a result of the collective means that intelligence as a commodity is interdependent; it would be too expensive for each member to gather intelligence in isolation [17]. As such, members are more likely to use the least coercive means possible to achieve their objectives; usually through passive surveillance, as seen in the Snowden leaks regarding US surveillance on Germany. The manner of exploiting trust — and its structural power implications — are signalled by the adversary's strategic interests, ultimately derived from its political economy in concert with other diplomatic, military, or

17. David Baldwin characterises economic interdependence as the "opportunity cost" it would take to break out of the structure. Synergies in cyberspace include the cost incurred by an agent to leave a network due to a trust relationship that is no longer desirable, such as a security alliance, or some too-expensive redundancy, such as free-riding on a dominant agent(s) for a public good, such as security, when it is no longer in the dominant agent's interest to keep providing. The other type of cost is the maximum possible imposed on an adversary, to achieve some behavioural outcome, through a coercive strategy like offensive cyber operations.

economic tools.

This chapter makes three contributions: first, the conceptual framework introduces trust as a variable in deploying cooperative or coercive strategies, in particular, a definition of trust as a systemic process that changes the property of information flows, adding to scholarship on security and statecraft. Second, we construct a case study based on secondary Chinese sources on China's security ecosystems in combination with interpretations from the security researcher community on the Anxun leaks of February 2024 to find that although the behaviour of private actors in comparison to Western counterparts is not so different, China's political economy creates structural exceptions through increased domestic coercive power. Finally, we discuss the impact of the trust-based framework on security policy questions such as "de-risking" and "de-coupling" supply chains in cyberspace, and the effect of trust fragmentation on emerging powers.

Section 2.3 provides a systemic definition of trust, discuss applications to cyberspace, and implications on strategies of cooperation and coercion. Section 2.4 discusses the aims of cyber statecraft, the benefits of using these instruments on creating or ending trusted relationships, and the networked actor ecosystems under consideration. In Section 2.5, we outline public-private actor relations, discuss the conflict in the state's roles and impact to trust and power relations. We construct a picture of the Chinese cyber ecosystems and chart trust relationships in contrast with Western counterparts, and Section 2.6 concludes with a summary of policy and structural implications, potential future work on modelling trust dynamics, and a discussion of complexity and limitations of the framework.

2.3 On trust

2.3.1 Many faces, many actors

The conceptual treatment of trust in different literatures is inconsistent. Across the social sciences, it is presented as either a capacity in, or a commodity "given" by, one actor to another in exchange for meeting a social or economic expectation. Sociologists have formulated typologies of trust relationships between the government, through the roles its institutions play towards societies and citizenry, in describing contexts such as power hierarchies. Economists tend to commonly use trust as an implicit property of a transaction that provides a basis for cooperative strategies between actors, while some omit the need for presenting it as an explicit concept (Williamson, 1993), relying on norms assumed to be mutually known, shared, and understood.

Trust in organisational and management theory is presented in sociological frameworks to explain institutional structure and organisational constraints; although there is no consistent definition across management theory, it is used to describe incentives in institutional actors and as behavioural support for decision-making over, for example, resource allocation. International relations scholars use trust implicitly in describing relationships between states; in particular as a conduit in reducing uncertainty and 'Hobbesian' fear between dominant and challenger states, in firmly established concepts such as deterrence theory and security dilemmas. In computer science and related fields such as cybersecurity, trust is viewed as a by-product of an access control policy, controlling information flows

between two computer systems, and has led to popular computer network security architectures such as those based on 'zero trust' (Ward and Beyer, 2014).

In summary, trust has been defined, variously, as a property in, product of, or a feature of a transaction between actors. Where this property is present, trust is a descriptor of the relationship between "trustworthy" actors. As a property of a transaction, it is dependent on the participating actor's agency; their choice of strategies, based on beliefs, incentives, preference sets or some other relevant outcome calculus. (Sabel, 1992) for example, adopts the definition that trust is "the mutual confidence that the other party to an exchange will not exploit one's vulnerabilities". The inherent reciprocity assumed in this definition is a departure from its sociological counterparts that describe institutional power, for example. In reasoning about market power and behaviour,[18] develops a "political economy" of trust; a taxonomy organising different perspectives in literature on the bases of confidence factors between actors, such as structural considerations or mutual knowledge of norms. These bases are used to establish a notion of "high" and "low" trust economies, bridging sociological and economic literatures.

However, conceptual formulations of trust as a relationship descriptor present some limitations to analysing behaviour as it is revealed, rather than expected, possibly because underlying assumptions about factors such as norms, reciprocity, vulnerabilities, shared incentives, and information asymmetries remain implicit. How trust is interpreted becomes highly rel-

18. M. Korczynski, "The Political Economy of Trust"' [in en], Available at: *Journal of Management Studies* 37, no. 1 (2000), https://doi.org/10.1111/1467-6486.00170., https://doi.org/10.1111/1467-6486.00170..

ative; the observer outside an actor's frame of reference interprets a possible trust relationship through their own beliefs — for example, beliefs arising from their own political systems — but the actors conducting the relationship inside the frame of reference may have a different, selective, or more granular view towards those with whom they enter into trust relations and form networks. Trust relations may not be mutual; the direction of information flows from the truster to the trustee and may not be reciprocated. As networks become more complex, multiple trust relations are established through constituent information flows. Actors create a dependence on those they share information with — the recipient carries the dependant's expectation of not perverting the information flow.

Unreciprocated trust creates heterogeneity in the quantity and properties of information known to actors in a network, in turn, creating information asymmetries between actors. Recipients who exploit this asymmetrical interdependence have greater relative capabilities to exercise cooperative or coercive strategies in their neighbours; we define the ability to exert these strategies as an actor's relative power in a system. On the other hand, while conceptual formulations of trust at present explain the structural effects of power on trust relations, they do not identify the structural effect of trust on power relations. For example, Kydd[19] argues through rational-actor security dilemma games that, at the time of US hegemony as a 'solitary superpower', "the structural features of the post-Cold War era indicate that US foreign policy may... raise world suspicions of US motivations" and that, post-Iraq, the US "will need to implement a policy of reassurance,"

19. Andrew H. Kydd, *Trust and Mistrust in International Relations* (Princeton University Press, June 5, 2018), ISBN: 978-0-691-18851-5, https://doi.org/10.1515/9780691188515, https://www.degruyter.com/document/doi/10.1515/9780691188515/html.

especially towards defection-prone states with high-trust thresholds.

The structural effect of trust formation and strengthening on power relations, however, is the cause of gradual relational changes, such as power transitions or new interdependences. A structure may represent a collection of networks representing a market, institution, or organisational hierarchy. As (Gambetta, 1998) and[20] observe, in "high trust" market economies, relative power is balanced among actors; in "low-trust" economies, institutions are weakened. In cyberspace, the result of globally interdependent information flows has been to allow actors a greater choice in who they share information with. Strategic choice is a second, implied limitation of previous conceptualisations of trust. Conceptualised as an actor's capacity, trust corroborates the "spheres of influence" theory in international relations, but may be inadequate in explaining perceived inconsistencies in states' behaviours, given a greater choice of potential trust partners. Middle powers such as India and Saudi Arabia have seemingly contradicting stances on security and trade, in relation with the US position on Russia since the war on Ukraine. Middle and emerging powers increasingly operate in an "à la carte world".[21]

Both limitations, in their inability to explain how power relations are affected by trust, arise due to implicit social, political and economic assumptions, possibly as these analyses are restricted to trust observed in a dyadic relationship behaviour, as opposed to the relationship being conducted in a wider system with multiple frames of social, political, and economic ref-

20. Korczynski, "The Political Economy of Trust'."

21. T.G.A. Leonard, Ivan Krastev, and Mark, *Living in an à la carte world: What European policymakers should learn from global public opinion, ECFR* [in en], Available at: 2023, https://ecfr.eu/publication/living-in-an-a-la-carte-world-what-european-policymakers-should-learn-from-global-public-opinion/..

erences. As such, the so-called "trustworthiness" of actors is neither homogeneous across networks, nor consistent within actor relationships. Modelling methodologies such as rational-actor game theoretic treatments can omit the cause and network effects of multiple, many directional informational flows, arbitrated by pluralistic views of actors' trustworthiness. As recorded in social network literature and revealed on social media, these network effects account for much of the "who to trust" phenomenon, over information integrity, as discussed earlier. Over a long-running network, the focus on dyadic relations and implicit assumptions result in exacerbating information asymmetries; the worst effects of actor-based, rather than information-based, trust processes is seen in the rise of disinformation on social networks, in turn reinforcing the erosion of social trust.

Finally, while extant treatments in sociology and economics literatures use trust to form a basis for cooperative interaction between actors, they do not provide explicit or rigorous reasoning for seemingly inconsistent behaviour, such as an actor with some relative power using an established cooperative relationship in one strategic domain to coerce an ally into showing cooperative behaviour in another strategic domain. Given the cross-domain nature of statecraft spread over political, economic, military, diplomatic, and now, cyber information systems, structural advantages of interdependence and greater relative power in one domain may allow for greater bargaining in relationships in other domains. In this chapter, we use the conceptual framework to overcome some of these limitations by not assuming homogeneity in political and economic factors in analysing cyber statecraft, but by basing trust relationships in the context of state actors' domestic political economies.

A state's ability to choose between cooperative or coercive strategies in cyberspace, and the success of these strategies in achieving national objectives and intended leverage, relies on state-state relationships vis-a-vis foreign policies, the mobilisation of the state's domestic private sector — such as its tech industry, critical infrastructure providers, researchers, or third parties sponsored by the state — as well as to incentivise key foreign private sectors to cooperate, for example, by providing market access. The extent and nature of each strategy, 'vertical' or 'horizontal' in the power arrangement of public-private and private-private relations, respectively, is determined by political economic variables of trust, interdependence, and power. Cyberspace, as an information system, offers domain-specific features that enable states with opposing political economies to exercise cooperative and coercive strategies of statecraft, given their relative power and degree of interdependence.

2.3.2 In cyberspace as an information system

Cyberspace is the collection of all networked computer-based information systems[22]. There is more consensus in literature about the characteris-

22. An objection to this definition might be the counter-example of airgapped systems. However, networked computer-based information systems need not be publicly networked, as in the case of the Internet, but include private networks, as well as so-called isolated systems that can still share information voluntarily or involuntarily as seen in the Stuxnet attack (through physical hard drives) or indirectly interact with TEMPEST environments that prevent information leakage due to environmental factors, such as electromagnetic radiation. A second objection may the usefulness of seeing cyber-physical systems in the context of information systems. The key question in cyber-physical systems is the optimal placement of sensors and actuators, which reduces cost as well as signal to noise ratios in information picked up and transmitted. The interaction of sensors and actuators with physical systems connects the physical world with cyberspace, as information storage, processing, and synthesis occurs in the 'cyber' portion of these systems. However, given our trust context, we note that sensors and actuators may follow some optimisation methodology, but do not per se exhibit strategic behaviour or agency

tics of cyberspace than its definition[23]; operators and users, or in our vocabulary, "actors", digital technology, and information communication give cyberspace social, political, economic, technological and military dimensions.[24] Accordingly, trust in cyberspace has been variously conceptualised as a system-level property of "trustworthiness", where a system acts according to expectation;[25] maintained by 'transparency' of the provenance of data and 'objectivity'.[26] This technocratic, system-level view of trust has motivated many secure computer network architecture models, based on the principle that systems integrity is key to preventing distrust, especially in conflict domains.

The concept of trust in this chapter is similarly based in informational integrity; it does not presuppose the characteristic property of a system, rather, as a process variable within an information system, associated to an actor as part of their agency. Trustworthiness is a structural property in an actor; as the perception of an actor's ability to execute a trust process changes, so does the observer's beliefs of the actor's trustworthiness. As a

23. The original use of cyberspace as attributed to William Gibson in the 1984 novel *Neuromancer* describes a psychological medium or "consensual hallucination" where information itself has form in a grid-like structure. In the context of this thesis, we are specifically concerned with the information system where actors are capable of showing strategic behaviour, lending the context for the conceptualisation of trust.

24. David J. Pym, "The Origins of Cyberspace," in *The Oxford Handbook of Cyber Security*, ed. Paul Cornish (Oxford University Press, November 2021), 0, ISBN: 978-0-19-880068-2, https://doi.org/10.1093/oxfordhb/9780198800682.013.1, https://doi.org/10.1093/oxfordhb/9780198800682.013.1; Starr Kuehl and Nye; R. Ottis and P. Lorents, "Cyberspace: Definition and Implications"' [in en], in *in. International Conference on Information Warfare and Security* (2010); D.D. Clark, *Characterizing cyberspace: Past, present and future. Working Paper* [in en], Available at: 2010, https://dspace.mit.edu/handle/1721.1/141692..

25. Fred Schneider, ed., *Trust in Cyberspace* [in en], National Research Council, Google-Books-ID: mAslCrFPwAIC (National Academies Press, January 1999), ISBN: 978-0-309-06558-0.

26. G. Yeo, "Trust and context in cyberspace"' [in en], Available at: *Archives and Records* 34, no. 2 (2013): 214–234, https://doi.org/10.1080/23257962.2013.825207., https://doi.org/10.1080/23257962.2013.825207..

result of the conceptual framework, the relative power of actors is a system variable, dependent on trust. Specifically, it is the power, compared to other actors, of the ability to deploy coercive or cooperative strategies on to targets in service of some objective. The mutually beneficial, or public, good, that arises from a trust relation becomes the source of leverage. In cyberspace, the framework establishes a relationship between "structures", or networks in international relations, and "systems", as understood in computational and management literature.

By assigning a common taxonomy to actor behaviours, structural bounds on their beliefs and relative agency, a dynamic theory of power relations emerges: by adding to the literature on existing theories of structural power competitions, such as "weaponised interdependence", we discuss how state-state and state-private relations, in concert, underlie national power projections. Changes in these relations initiate entrenched power transfer or imbalances, albeit slowly, as opposed to a 'steady state' model of initial power configurations exacerbating over time. In particular, a more dynamic approach to trust and power relations can be adapted to both 'great power' as well as middle and emerging power behaviours, given that structures both facilitate and temper power simultaneously; the framework does not assume its bases in a liberal international political economy.

Cyberspace, imbued with social, political, economic and technological character, must accommodate overlaps with financial, political, and societal information systems through pervasive digital technologies which act as communication channels. Financial transactions and political discourse are increasingly conducted in cyberspace, for example, and weaponised. The overlap in these information systems provides a foundation for reconcil-

ing computational, personal or political, and economic definitions of trust. Any instrument of statecraft, such as overt or covert action, must balance the structural considerations of relative power vis-a-vis these overlapping information systems. In an information system, instruments of statecraft are the set of strategies available to an actor, where the cost of deploying a strategy depends on the initiator and target's relative structural position. In cyberspace, these strategies are deployed through legal, economic, political, or technological action in ecosystems.

We define ecosystems[27] as self-forming substructures around the economic character of a digital technology. This definition motivates states' leveraging their political economies with regards public-private relations and the relative economic value extracted by private actors. Typically, the economic character is some demand-supply based resource transaction, such as disclosing personal information to a tech company in exchange for personal or social utility derived from its products. Tech platforms are incentivised to create ecosystems with closed feedback loops to retain consumer trust. On the other hand, economic character based around the demand for commodities, such as spyware, engages a collection of ecosystems of public and private actors researching different technology stacks, with a commercial organisation such as an exploit vendor delivering the offensive capability to state or state-sponsored actors. Ecosystems are networked through such information transactions: public ecosystems are accessible to all agents in the wider system, private ecosystems require new trust relations to be formed or broken for agents to enter or leave.

An agent may establish or improve its "trustworthiness" if it can use

27. Adner, "Ecosystem as Structure: An Actionable Construct for Strategy'."

its agency and resources to signal to other agents that it is able to execute a trust process, and the receiving agents accept the signal. Trust is improved over multiple, possibly repeated transactions; a relationship is a mutually trusted one when process execution is bilateral between agents. The perception of a trusted relationship between two agents may initiate trustworthiness signals in a third agent, execute a new process, and the network expands. In cyber statecraft, as in the case of economic statecraft, interdependences formed as a consequence of expanding networks are exploited by agents in structurally favourable positions directly, or through proxies. While some ecosystems may be networked, other networks may not have overlapping ecosystems, such as ideological separate political information systems in the Cold War, despite economic interdependences.

Structurally favourable positions lead to power hierarchies, formed initially as a result of some trust process such as voting for a political party in a democratic election, but then reinforced through cooperative or coercive strategies by the resulting government on to the "citizen" agent. Political trust, and the trustworthiness of a government actor, signalled in its policies and institutions can affect interpersonal trust between agents.[28] In cyberspace, both personal and political trust as social phenomenon are reflected through information intermediaries, such as social media platforms, which are a natural target for coercive strategies such as so-called influence operations from state actors of varying relative power. By attempting to manipulate existing or new trust processes through offensive cyber capabilities, the coercer attempts to reroute information flows that form the basis

28. M. Levi and L. Stoker, "Political Trust and Trustworthiness"' [in en], Available at: *Annual Review of Political Science* 3 (2000): 475–507, https://doi.org/10.1146/annurev.polisci.3.1.475., https://doi.org/10.1146/annurev.polisci.3.1.475..

for social trust.

On the other hand, states in unfavourable structural positions, or lower relative power, find themselves compensating by imposing more defensive costs in their targets if there are no interdependences, or if the cost of an offensive incurred is lower than breaking indirect interdependences. In defensive capacities, as seen with strategic choice, they may instead appeal to structurally better positioned actors through offering one-sided economic or political inducements, or cooperating in another information system in exchange for free-riding benefits from the better positioned actor's security offering. As any first-mover advantage is limited in relatively lower power actors, they are more likely to be targets of coercion in strategic competition between states of approaching power parities.

In this chapter, we are concerned with cyber statecraft firstly in the context of state-state relations, such as through instruments like foreign policy or covert strategies, directly on to the target state or through a proxy. Secondly, in state-private relations, where a state either attempts to leverage domestic policies to extract a political outcome through engaging with a private actor operating within its jurisdiction, or it exploits an interdependence forged through an ecosystem such as a supply chain between a domestic private actor with a target foreign private actor.

The latter strategy, in turn, is implicitly aimed at some strategic competitor state, which houses the target foreign private actor. Direct strategies of statecraft include inducing cooperation in, or coercing, a competing state through security coalitions or covert cyber operations. Indirect strategies of statecraft target private sector supply chain interdependence, and success depends on the initiating state's structural position in trust net-

works. These structural positions determine relative power in both public and private actors; the surrounding cyberspace as networked information systems takes on the political and economic character of these actors.

2.3.3 Coercion and deterrence, cooperation and defection

Strategic leverage is gained as a result of coercive or cooperative dynamics; successful statecraft must calculate the appropriate balance[29]. Our conceptual framework supplies additional perspectives in the logic of coercion: where trust relations create structural conditions such as new or retrenched interdependences, agents bid to consolidate domain power, determining how effective any coercive strategy can be, whether domestic or foreign. The CCP's exploitation of social network trust dynamics through account mining and surveillance along with an estimated $7 billion spend annually on Internet censorship nationwide helps shape its influence operations domestically by suppressing dissent, and internationally by profiling sceptics and generating noise as distraction.[30]

Coercion is an offensive strategy deployed on a target agent to deter a behavioural outcome. Applied in an information system, coercion addresses an informational asymmetry by bypassing, manipulating, or denying the execution of a target's trust process, in order to deter the target's intended outcome. The strategic rationale behind the coercive method depends on

29. In 2013, the UK Defence Academy and Ministry of Defence published an inquiry report on 'The Global Cyber Game', which expresses cooperation and coercion (among others) as strategic levers in a gamified presentation of power competitionhttps://www.gov.uk/government/publications/the-global-cyber-game.

30. A. Thompson, "Buying Silence: The Price of Internet Censorship in China"' [in en], Available at: *Center for Security and Emerging Technology*, 2021, https://cset.georgetown.edu/article/buying-silence-the-price-of-internet-censorship-in-china/..

some cost calculus; successful coercion can achieve deterrence at a cost-benefit advantage to the coercer, mostly by increasing defence costs for the target, or by deploying cheaper instruments to punish the target than up to some threshold of conflict escalation.

Through cyberspace, as in other mediums of coercion, the desired change in the target's behavioural outcome is in "... align[ment] with the coercer's political, social and economic preferences... coercion serves as a mechanism of [the attacker's] preference revelation".[31] As an offensive strategy on the target's political economy, coercion in cyberspace is exposed to the same structural considerations vis-a-vis the effects of power and interdependence on coercive abilities. Operationally, the coercer either attempts cyberattacks that may cause a denial of service, exfiltrate data, or more generally, reroute information flows, or the use of a legal instrument that disproportionately increases the cost of target defence.

The coercer's structural position and relative power within an ecosystem determines both its access to such an offensive cyber capability, as well as the resulting cost of coercion, based on the target's relative power and the expected effect of the cyberattack. Similarly, the target's structural position and relative power determines the credibility of the coercer's perceived threat. Through our trust framework, we ascribe two character types to coercion: overtly coercive strategies such as cyberattacks on critical national and civilian infrastructure that (are intended to) threaten domestic, political trust-based structures. Covertly coercive strategies, such as espionage and most counterintelligence operations in cyberspace, targeting specific,

31. David Blagden, "Deterring Cyber Coercion: The Exaggerated Problem of Attribution," Publisher: Routledge _eprint: https://doi.org/10.1080/00396338.2020.1715072, *Survival* 62, no. 1 (January 2, 2020): 131–148, ISSN: 0039-6338, https://doi.org/10.1080/00396338.2020.1715072, https://doi.org/10.1080/00396338.2020.1715072.

powerful actors in heterogenous networks, may be more expensive for the coercer, but carry lesser weight on the need for public attribution, instead, acting as "accommodative signals".[32]

Both types of coercion are intended to fill a "leverage deficit", albeit in different ways. There is broad consensus among cyber coercion scholars that the cyber domain alone is insufficient in producing a concessionary outcome than when used in conjunction with other domains[33] in part due to the so-called "stability-instability" paradox[34] where damage incurred due to cyberattacks is minimal despite cyberspace being an unstable system. However, why some coercive strategies in the cyber domain remain more or less successful at producing strategic outcomes remains to be explained; for example, the seemingly limited success of Chinese cyber espionage in evoking concessions, or the alleged success of the US model of combining espionage, cyber degradations and economic threats.[35]

In responding to overtly coercive outcomes, the target state has to defend its resilience domestically to its society and industry to maintain trust. Since China's 2014 compromise of the US Office of Personnel Management through the People's Liberation Army and one of several Advanced Persistent Threat (APT) groups associated with it, the position of the US and

32. S.W. Lonergan, "Cyber Operations, Accommodative Signaling, and the De-Escalation of International Crises"' [in en], ed. E.D. Lonergan, Available at: *Security Studies* 31, no. 1 (2022): 32–64, https://doi.org/10.1080/09636412.2022.2040584., https://doi.org/10.1080/09636412.2022.2040584..

33. Borghard and Lonergan, "The Logic of Coercion in Cyberspace."

34. Jon Lindsay and Erik Gartzke, "Coercion through Cyberspace: The Stability-Instability Paradox Revisited," in *The Power to Hurt: Coercion in Theory and in Practice* ((Oxford University Press, Forthcoming), August 25, 2016).

35. Brandon Valeriano, "Cyber Coercion as a Combined Strategy," in *Cyber Strategy: The Evolving Character of Power and Coercion*, ed. Brandon Valeriano, Benjamin Jensen, and Ryan C. Maness (Oxford University Press, May 15, 2018), 0, ISBN: 978-0-19-061809-4, https://doi.org/10.1093/oso/9780190618094.003.0004, https://doi.org/10.1093/oso/9780190618094.003.0004.

its allies towards such coercive strategies has increasingly become public attribution. In recent years, the Five Eyes have been vocal about the Volt Typhoon intrusion into Microsoft, another APT using lateral movement techniques, attributed to the Chinese state, and its additional, alleged role in compromising defence personnel records in the UK.

Through transparent national strategies, keeping their populaces informed and partnering with their private sectors on defence, Western allies seek to maintain trust relations with their societies and one another, and this transparency is claimed by the body politic to be consistent with their liberal democratic political systems. On the other hand, the lack of public attribution of Western cyberattacks by target states like China and Russia is explained by Western analysts as owing to their illiberal systems of government, to prevent admitting weakness, in accordance with their attitude towards trust, and containing dissent. There are no records of attributing offensive cyber activity or passive surveillance attempts between China and Russia either, despite deepening trade, security, and political relations. Repeated instances of public attributions by the West have not deterred China from pursuing coercive strategies in cyberspace.

China's political economy helps in analysing its attitudes towards public attribution, choice of coercive strategies, and how it views its own structural position and relative power in a cyberspace it has long sought to free from interdependences that create information asymmetries to its disadvantage. In the domestic sphere, China views personal economic freedoms as separate from political liberties, "contrary to Western media portrayals... [the population] does not want democracy" despite access to Western technol-

ogy and the democratisation of ICTs[36].[37] Additionally, in what it perceives to be its domestic sphere, China's coercive strategies in Hong Kong and the Taiwan Strait are a further indication of its attitude towards trust.

China's attitude to maintaining trust appears to be based on increasing information asymmetries. According to Manantan,[38] China views deterrence and coercion as interchangeable through its philosophy of "weishe". The implications of this approach may provide useful strategic responses to China's bargaining efforts in multilateral forums towards its desired cyberspace sovereignty: in virtual or physical territories that it views as domestic — legitimately or otherwise — China's approach in leveraging its structural position and power appears to use coercive strategies by default. In summary, in both its foreign and domestic relations within cyberspace, China's coercive approach to promoting its national interests results from, and reinforces growing relative and absolute power, respectively.

Given this structural advantage, responses to cyberattacks in the form of economic sanctions applied by Western states on individuals actors such as Chinese military personnel or civilian hackers has very limited to no deterrent effects, leading to supply chain sanctions on high-value businesses such as Huawei 5G. As such, offensive cyber activity is normalised in China's information operations to the point of being a "strategic substitute" in compensating for military shortcomings, and as a gauge for reprisals to

36. J. Damm, "The Internet and the Fragmentation of Chinese Society"' [in en], Available at: *Critical Asian Studies* 39, no. 2 (2007): 273–294, https://doi.org/10.1080/14672710701339485., https://doi.org/10.1080/14672710701339485..

37. Y. Jiang, *Cyber-Nationalism in China. Challenging Western media portrayals of internet censorship in China* [in en], Available at: 2012, https://doi.org/10.1017/9780987171894., https://doi.org/10.1017/9780987171894..

38. M.B. Manantan, "The People's Republic of China's Cyber Coercion: Taiwan, Hong Kong, and the South China Sea"' [in en], Available at: *Issues & Studies* 56, no. 03 (2020): 2040013, https://doi.org/10.1142/S1013251120400135., https://doi.org/10.1142/S1013251120400135..

show of power through coercive strategies like 'brinkmanship'.[39] China has no structural incentive to deter from using coercive strategies; its relative power in an interdependent cyberspace assures that any significant deterrence would be structural, and its cost also borne by the coercer. Despite its desire for Internet sovereignty, much of China's impunity is owed to interdependence.

New scholarship since the Ukraine war on evolving Russian attitudes towards deterrence in cyberspace describes the lack of a coherent, current doctrine in anticipation of the Kremlin's objective of information sovereignty, but theorises the concept of "cumulative coercion", derived from historical and cultural factors, that — similar to China — conflates with "strategic deterrence" as "... constant low-intensity engagement of the adversary... unlimited use of limited force".[40] Conflict and coercion are described as interchangeable parts of an overarching influence and shaping strategy with little difference between offensive and defensive operations. As such, while a common attitude of persistent coercion appears in both Chinese and Russian cyber statecraft as a means of deterrence, China's "wangluo quangguo" strategy of a competitive tech industry is incentivised to invest in long-term cyberspace stability, in contrast to Russia.[41]

China's cooperative strategies in cyberspace are an extension of its foreign policy objectives. Accrued power from established interdependence allow China to cooperate with a state in one domain that it could coerce

39. F.S. Cunningham, "Strategic Substitution: China's Search for Coercive Leverage in the Information Age"' [in en], *International Security* 47, no. 1 (2022): 46–92.

40. D. Adamsky, *The Russian Way of Deterrence: Strategic Culture, Coercion, and War', in The Russian Way of Deterrence* [in en], Available at: 2023, https://doi.org/10.1515/9781503637832., https://doi.org/10.1515/9781503637832..

41. D. Broeders, L. Adamson, and R. Creemers, *Coalition of the Unwilling? Chinese and Russian Perspectives on Cyberspace'* [in en], Available at: Rochester, NY, 2019, https://papers.ssrn.com/abstract=3493600.

in another. The digital and non-digital dimensions of the Belt and Road initiative intersect in West African states where China invests in building infrastructure as a loan as part of its Belt and Road initiative, use the resulting soft power from so-called nation building, and apply it to cooperative alliances on security, such as through the 2023 Global Security Initiative [42]. Any aggregated debt from Chinese investments in infrastructure-building provides future coercive instruments in cyberspace and otherwise.

As the dominant power within its networked ecosystem of allies, China's signals of trustworthiness are necessary for engendering cooperation between other states in its alliance,[43] thereby expanding Chinese influence in multiple domains. Indeed, the effect of previously established interdependences and resulting cooperative strategies has consequences for substructure alliances. The exclusion of France from the 2021 AUKUS alliance for nuclear powered submarines in the Indo-Pacific created diplomatic tensions ultimately resolved in December 2023 through a bilateral security agreement between France and Australia;[44] trust relations between an agent and other nodes in the network may be expected to be preserved in newly formed substructures. Policymakers may assess where allied or adversarial agents are positioned structurally in a network topology to assess the impact of policies that undermine new and established trust relations, and resulting limitations on cooperative strategies.

42. https://www.fmprc.gov.cn/mfa_eng/wjbxw/202302/t20230221_11028348.html Ministry of Foreign Affairs of the People's Republic of China, 2023

43. Kydd, *Trust and Mistrust in International Relations*.

44. J. Holland and E. Staunton, ""BrOthers in Arms": France, the Anglosphere and AUKUS"" [in en], Available at: *International Affairs* 100, no. 2 (2024): 712–729, https://doi.org/10.1093/ia/iiae016., https://doi.org/10.1093/ia/iiae016..

2.4 The aims of cyber statecraft

How states decide to adopt overtly, covertly coercive, or cooperative strategies to secure national objectives, and in what proportion, is as much a function of a state and its target's relative structural position in cyberspace, as much as a feature and limitation of cyberspace itself. Conceptions of cyberspace vary significantly: regulatory approaches conceive of cyberspace as anarchical,[45] fated to self-regulation,[46] or destined for international order;[47] as a social, networked space,[48] as an 'equaliser' affording all actors the power of scale, markets and anonymity;[49] as a "control space" consisting of socio-technical regulatory and contract mechanisms that operates as "an institution" instead of anarchy;[50] as a previously anarchical space that may be governed through evolving norms and standards which liberal democracies can hold themselves up to.[51]

These varying viewpoints are correctly contemporaneous interpretations. Without much anachronism, our framework can reconcile these

45. D.G. Post, "Anarchy State and the Internet" [in en], *Journal of Online Law, Article* 3 (1995).

46. L. Lessig, "The Zones of Cyberspace"' [in en], Available at: *Stanford Law Review* 48, no. 5 (1996): 1403–1411, https://doi.org/10.2307/1229391., https://doi.org/10.2307/1229391..

47. J.W. Forsyth and B.E. Pope, "Structural Causes and Cyber Effects: Why International Order is Inevitable in Cyberspace"' [in en], *Strategic Studies Quarterly* 8, no. 4 (2014): 112–128.

48. J.E. Cohen, "Cyberspace as/and Space"' [in en], *Columbia Law Review* 107 (2007): 210.

49. J. Rowland, M. Rice, and S. Shenoi, "The anatomy of a cyber power"' [in en], Available at: *International Journal of Critical Infrastructure Protection* 7, no. 1 (2014): 3–11, https://doi.org/10.1016/j.ijcip.2014.01.001., https://doi.org/10.1016/j.ijcip.2014.01.001..

50. J.R. Lindsay, "Restrained by design: the political economy of cybersecurity"' [in en], Available at: *Digital Policy, Regulation and Governance* 19, no. 6 (2017): 493–514, https://doi.org/10.1108/DPRG-05-2017-0023., https://doi.org/10.1108/DPRG-05-2017-0023..

51. J. Nye, "The End of Cyber-Anarchy? How to Build a New Digital Order."' [in en], *Foreign Affairs* 101, no. 1 (2022): 32–42.

views to an extent. Cyberspace is neither uniformly anarchical, nor uniformly governable. Despite systemic factors such as mixed success in norm-building due to role conflicts, opposing national objectives, hegemonic challenges, and examples of 'responsible cyber power' behaviour, cyberspace is a heterogenous network where agents' relative power governs the nature of information flows around the information system. States with sympathetic political economies attract interdependence, fluctuating in a fluid, "territorial ontology" with networks.[52] States that can influence new trust processes will do so through power consolidated by entrenched interdependences. Through cross-domain coercion, diplomatic instruments through multilateral institutions, or offensive cyber capabilities, success in the governance of a relevant part of cyberspace is structural.

As discussed before, cyber statecraft may lend itself to natural comparisons with economic statecraft as a means of securing national objectives, even though cyberspace and the global financial system aren't isomorphically governable. Both types of statecraft leverage domestic business relationships to achieve national security objectives, but may not be seen mutually exhaustively. Legal and regulatory measures also exist at the nexus of the two information spaces, for example, export controls on spyware. Lucas Kello[53] observes that sanctions display "negative" power, causing denial of gain, but in recent years denial of service attacks on protocols and platforms such as the DNS provider Dyn and Amazon Web Services, show similar effects through downtime in digital economies. The effects of puni-

52. Daniel Lambach, "The Territorialization of Cyberspace*," *International Studies Review* 22, no. 3 (September 1, 2020): 482–506, ISSN: 1521-9488, 1468-2486, https://doi.org/10.1093/isr/viz022, https://academic.oup.com/isr/article/22/3/482/5488469.

53. L. Kello, "The Meaning of the Cyber Revolution: Perils to Theory and Statecraft"' [in en], Available at: *International Security* 38, no. 2 (2013): 7–40, https://doi.org/10.1162/ISEC_a_00138., https://doi.org/10.1162/ISEC_a_00138..

tive economic measures may be felt quickly and publicly; the same is not true for covertly coercive cyber strategies. But contradictions in operationalising cyber statecraft further limit its success as an effective coercive strategy.

States must develop long-term trust relations with actors who perform offensive cyber operations by permission or in partnership. These semi-private actors, mercenaries, or APT groups must balance high degradation of cyber capabilities with persistent offensive engagement. This "transitory nature" of offensive cyber capability[54] incentivises states to limit access to new capabilities through legislative means or by disclosure, causing immediate degradation, and in turn also limiting accessibility and development of exploits for private actors who share such tools.[55] The cost of cyber coercion is not always an advantage over other domains, as impact of covert action is easily miscalculated; "the cost of Stuxnet... could have launched three cruise missile offensive strikes"[56] and the supposed "ease of attack" may not lead to deterrence through ease in deception.[57]

Despite mixed success in signalling intentions due to a high risk of misinterpretation, scope creep by affecting unintended targets through interdependence, or miscalculation in imposed costs on both sides, overtly

54. M. Smeets, "A matter of time: On the transitory nature of cyberweapons"' [in en], Available at: *Journal of Strategic Studies* 41, no. 1–2 (2018): 6–32, https://doi.org/10.1080/01402390.2017.1288107., https://doi.org/10.1080/01402390.2017.1288107..

55. A. Lemay, "Survey of publicly available reports on advanced persistent threat actors"' [in en], Available at: *Computers & Security* 72 (2018): 26–59, https://doi.org/10.1016/j.cose.2017.08.005., https://doi.org/10.1016/j.cose.2017.08.005..

56. B. Jensen, "The Cyber Character of Political Warfare"' [in en], *The Brown Journal of World Affairs* 24, no. 1 (2017): 159–172.

57. E. Gartzke and J.R. Lindsay, "Weaving Tangled Webs: Offense, Defense, and Deception in Cyberspace"' [in en], Available at: *Security Studies* 24, no. 2 (2015): 316–348, https://doi.org/10.1080/09636412.2015.1038188., https://doi.org/10.1080/09636412.2015.1038188..

coercive strategies do not always produce concessions[58] — possibly because the target's structural position renders concessions more expensive than imposed by coercion, or the object of concession has been misunderstood between coercer and target. As a strategic substitute, persistent coercive engagement is seen as 'fair game' by China and Russia as "low-intensity conflict behaviour". Other covertly coercive strategies as a result of civil society surveillance have either levelled the structural disadvantages of smaller states, for instance through commercial spyware getting cheaper over time before Western moratoria, or consolidated power in pre-existing information "panopticons" through weaponised interdependence.

So why cyber statecraft? Coercive strategies such as cyberattacks in the past decade have verified that cyberspace is no equaliser, but rewards existing structural asymmetries of power that determine coercive success. Smaller states without coherent national cyber strategies or digital resources are disproportionately affected by cyberattacks of varying technical sophistication. Cooperative strategies such as coalition-building in the form of establishing norms, standards, or responsible behaviour agreements either favour coalitions of sympathetic political economies, or elicit little recourse for misdemeanours. Losing the offender's trust may be too expensive vis-a-vis upholding cooperative relations in other domains, with few levers to deter undesirable actions without risking volatility in a coalition, and punishment is simply too expensive. The utility of cyber statecraft, particularly in its overtly coercive forms, must not be exaggerated.

However, coercion in cyberspace can disproportionately favour middle powers as well as challengers to hegemons in asymmetric networks as they

58. Valeriano, "Cyber Coercion as a Combined Strategy."

lack the economic power to impose loss through sanctions. Established powers find themselves in a defensive position by default — due to unpredictability and obfuscation of the challenger's objectives, as Kello observes — and are better equipped to initiative cooperative strategies that passively exploit a priori interdependences. As opposed to the financial system as an information space, cyberspace suffers from a lesser burden of authentication, verification and audit in transactions, and can act as a gateway to other domains that leverage ICTs with controlled risk. Networks in cyberspace, like the Internet, were initially designed without security protocols in TCP/IP, and security features such as sender-recipient validation were added in layers; routing information flows requires a lower technical and resource cost than in networks such as, for example, SWIFT.

While the creation of new trust relationships and structural change in existing power asymmetries favouring agents with lower relative power in an ecosystem may be limited, it is much easier for these agents to undermine trust relations between other agents with higher relative power. This is a product of the heterogenous nature of anarchy in cyberspace, that states not bound to cooperative coalitions need not adhere to 'responsible' behaviour, and is a comparative advantage of cyber statecraft. Additionally, while economic punishments in response to cyber coercion may come at a disadvantage to the target, as sanctions affect businesses with high levels of interdependence in global supply chains, responses in cyberspace to economic coercion impose cost on the defender. For structurally less significant nation-states, the benefits of cyber statecraft aren't absolute, but incremental and comparative than from other domains; it may not yield concessions, but increase bargaining power.

The hegemon is incentivised to preserve the balance of power and need only engage asymmetrically in specific, tactical conditions, as it can wield far more influence through cross-domain engagement; the challenger seeks to break this status quo and must, strategically, engage asymmetrically. Over time, covertly coercive strategies such as influence operations based on disinformation, or more sophisticated persistent engagement, can alter trust relations in the target's domestic structures, extending to existing cooperative strategies with foreign partners. In this case, the style of statecraft adopted by a nation-state in domains such as trade and finance are indicative of the overall posture and political economy, which may serve as predictors of cyberspace behaviour. For example, Chinese economic statecraft targets domestic political economic actors directly, through the state taking a "king-making role" that favours commercial entities who espouse state objectives.[59]

So far, the conceptual framework describes the dynamics between adversarial or allied nation-states, where interdependence arises from trust processes between agents in networked ecosystems. Nation-states must also leverage their private-public sector relations efficiently to achieve political, economic and social objectives in cyberspace. Some analysts attribute the difference between the expected damage and sabotage to critical national infrastructure caused by Russian offensive cyber operations, as opposed to the more passive reality of greater espionage attempts and influence operations since the Ukraine war at least in part due to the inability of the Russian state to mobilise its private partnerships, despite Western intelli-

59. W.J. Norris, *Chinese Economic Statecraft: Commercial Actors, Grand Strategy, and State Control* [in en], Available at: 2016, https://www.jstor.org/stable/10.7591/j.ctt18kr4kx..

gence agencies' high estimation of Russia's cyber capabilities.[60] Complex interdependence extends to the private sector through global supply chains; we offer a graduated view of the actors involved, their relationships with the state, and implications for structures and statecraft.

2.5 Public-private actor structural relations

Many analyses of public-private relations in national cyber strategies tend to focus on relationships between the state and business, where the "privateness" of the business actor extends, in particular, to technology industry ecosystems such as consumer platforms or infrastructure providers, which operate with a degree of independence from the state, consistent with market economy-based governance systems. However, unclear separation of duties in operational matters of technology security and undesirable market effects in the private sector can create national security vulnerabilities from asymmetric public-private power relations.[61] Additionally, given the aims and instruments of cyber statecraft, we must consider a number of private actors that states seek to leverage through coercive abilities arising from their domestic political economies. In particular, roles played by third party actors such as cyber mercenaries, hacker-for-hire and/or APT groups, and providers of offensive cyber capabilities, are subject to varying degrees of state control, which is a key determinant of strategic success in cyberspace.

60. G.B. Mueller, *Cyber Operations during the Russo-Ukrainian War'* [in en], Available at: 2023, https://www.csis.org/analysis/cyber-operations-during-russo-ukrainian-war.

61. M. Carr, "Public–private partnerships in national cyber-security strategies"' [in en], *International Affairs (Royal Institute of International Affairs 1944* 92, no. 1 (2016): 43–62.

2.5.1 The "privateness" of actors

The tech industry actor offers services that are consumed by societies within competing states. Whether through direct interaction on consumer platforms such as social media, or indirect interaction in providing the state and other industries with underlying infrastructure needed to operate digital economies or coordinate physical infrastructure, the tech industry plays a pivotal role in mediating societal attitudes towards their governments. States are incentivised to cooperate with, or coerce, tech industrial actors domestically to maintain or entrench a political status quo. However, tech businesses create online ecosystems that are designed to "gatekeep" user information, satisfying their engagement-based business models.

The ability of the actor to keep information flows private results in an economic good, motivating the property of "privateness". To compete with other businesses in digital marketplaces, they form informational interdependences as part of global supply chains. From these supply chains, businesses extract "high" and "low" economic values, that govern their negotiating strategies with their respective states; dominant states are, furthermore, more likely to play home state to high-value businesses, setting up inter-state competition.[62]

Private-sector interdependences vary; the provision of low-level materials such as semiconductor chips to increase computing power and compete on the new strategic frontier of language learning models; critical national infrastructure such as telecommunications, for example, the soon-to-be-reversed reliance of British Telecom on Huawei equipment for lower fi-

62. Chen and Evers, ""Wars without Gun Smoke": Global Supply Chains, Power Transitions, and Economic Statecraft'."

delity cellular services such as 2G and 3G, or the removal of Android from Huawei OS due to US export control; marketplace mediations, such as Apple's removal of WhatsApp from the Chinese App Store; low-level software supply chain interdependence such as the use of another provider's software libraries in, for example, cryptographic protocols. The resulting economic value or public good is a target for overt or covert action through cyberspace; states are also incentivised to target tech companies internationally to undermine a competitor state's objectives, as seen in Operation Aurora, the Chinese state espionage campaign on Google in 2009.[63]

The tension between the state's coercive abilities as an offensive actor and a company's defensive posture as potential attack surface varies based on economic advantages from the company's structural position as a defensive strategy, as well as its ability to respond to state coercion. Such power dynamics are less volatile for other, (less) private actors, such as state-sponsored mercenaries or exploit vendors, as their incentives are derived from regular state patronage. In general, states form long-term trust relations with cyber mercenaries to compensate for lack of in-house capability or achieve national objectives through arms-length covertly coercive operations.[64] However, leaks on the code repository GitHub in February 2024 containing a dump of documents belonging to a Chinese government contractor, Anxun (i-Soon), long associated with APT-41, provides meta-analyses into the Chinese offensive cyber ecosystem.

First, Anxun is understood to have had contracts with the Chinese government at state and provincial levels, undertaking hacking activities tar-

63. B. Buchanan, *The Hacker and the State: Cyber Attacks and the New Normal of Geopolitics* [in en], Available at: 2020, https://doi.org/10.2307/j.ctv3405w2m., https://doi.org/10.2307/j.ctv3405w2m..

64. T. Maurer, *Cyber Mercenaries* [in nl] (Cambridge University Press, 2018).

geting both international economic actors, such as Canadian firm Com100, as well as fulfilling its regional statecraft ambitions in central and east Asia, as well as smaller African nations. Second, Anxun developed training materials for burgeoning offensive cyber practitioners. Third, it developed and provided not just low-level surveillance tools, but also information exfiltration tooling targeting large email platforms as well as spyware, hardware interceptors, and surveillance evasion tooling.[656667].[68]

While previously identified APT and state-sponsored groups operated as now-defunct front companies for the PRC, Anxun appeared to be an independent security contractor as any private actor, headed by a former hacktivist. It also appears to have had a much larger scope of work vis-a-vis list of domestic and International targets, technological capabilities and tooling, simultaneous remit as a hacker-for-hire, exploit vendor, and educational capabilities, while harbouring internal employee discontent over low pay, which may indicate that the PRC did not see Anxun as a market player in regards to compensation.

Finally, leaked supporting documents reveal a complex ecosystem, not too dissimilar from Western counterparts, of smaller exploit vendors acquired by larger groups in bidding for government contracts, as well as

65. M. Brazil, *Foreign Intelligence Hackers and Their Place in the PRC Intelligence Community, Jamestown* [in en], Available at: March 2024, https://jamestown.org/program/foreign-intelligence-hackers-and-their-place-in-the-prc-intelligence-community/..

66. N. Team, "i-SOON: Another Company in the APT41 Network"' [in en], Available at: *Natto Thoughts*, 2023, https://nattothoughts.substack.com/p/i-soon-another-company-in-the-apt41.

67. Anxun and Chinese APT Activity - ReliaQuest [in en], Available at: 2024, https://www.reliaquest.com/blog/anxun-and-chinese-apt-activity/..

68. "Data From Chinese Security Services Company i-Soon Linked to Previous Chinese APT Campaigns"' [in en], 24 February. Available at: *Unit* 42 (2024), https://unit42.paloaltonetworks.com/i-soon-data-leaks/..

subcontractors handling different aspects of offensive tooling on offer.[69] In summary, the distinctions drawn from the Anxun leaks raise two significant observations: first, not all mercenaries and exploit vendors may be seen as separate private actors; "privateness" is relative to state coercive abilities and a company's product offering, and second, that the Chinese military-industrial complex as regards its offensive cyber ecosystem appears to be broader and with more blurred public-private lines than Western counterparts, with foreign, military, provincial, and civil objectives supplicated in partnership with a single private actor.

The coercive ability of a state actor like China can deploy regulatory, legislative, and more covert resources into leveraging its private sector, whether in the 'whole-of-nation' offensive cyber ecosystem of mercenaries and exploit vendors, academia, and military-state organisations, but also in its tech industry; its "Anti-Monopoly Law" is a dual use instrument of domestic suppression — to regulate tech platforms that are perceived to pose a domestic political threat, as with Alibaba, while simultaneously a lever in suppressing foreign businesses and other strategic fronts of competition with the US. American and European approaches to regulating tech platforms' economically or societally undesirable consequences respectively vary widely, depending on political will, while China's use of antitrust regulation as a foreign policy instrument of retaliation has significant, if economically limited, consequences as political signals to global regulatory regimes due to regulatory interdependence.[70]

69. W. Bernsen, *Same Same, but Different, Margin Research* [in en], Available at: 2024, https://margin.re/2024/02/same-same-but-different/.

70. A.H. Zhang, "Weaponizing Antitrust During the Sino-US Tech War"' [in en], in *Chinese Antitrust Exceptionalism: How The Rise of China Challenges Global Regulation*, ed. A.H. Zhang (Oxford University Press, 2021).

2.5.2 Coercive and cooperative strategies as capabilities

Private actors are subject to hierarchies of power depending on their economic status in global supply chains as high or low value. They interact 'horizontally' with other private actors of relative higher or lower values, 'vertically' with the state in its legislative and regulatory roles, as well as irregularly with foreign states by forming economic partnerships or becoming security targets. The topology of these relationships describe a private actor's vulnerability to state coercion, and are structural indicators of private power.

The state must be capable of weaponising a more favourable structural position to wield the appropriate strategy over a target private actor located in a competing state, and use it to implicitly target its strategic competitor. Effectiveness weaponisation depends on the political and economic levers available to the state; these levers are originate from, and affect, economic and political information systems through, and in addition, to cyberspace. Uses of cross-domain levers on domestic or foreign private actors, distinct from the more direct strategy of cross-domain coercion in state-state relations, are nevertheless structural strategies and may be analysed as state capabilities.

In particular, the state must command to its advantage three interdependent features in domestic political economy to leverage private actors in achieving its national objectives. First, political coupling. The more closely a private actor is coupled with the political objectives of the state in which it locates primary operations, the more it will be aligned to changes in the

state's domestic and foreign policy. As the private actor develops a self-reinforcing trust relationship with the state (which may not be reciprocal) the actor may enjoy the state's protection and favour as it loses political independence. In authoritarian governments, such as with the Chinese state's role as "king-maker", tight political coupling plays to the economic incentive of the private actor; it is especially in the interest of the mercenary to maintain trust with the state, despite staff-level discontent in the Anxun case.

Second, economic independence. When the private actor extracts a high or low economic value in a global supply chain based on market forces, the state's coercive capabilities on the actor are reduced up to a threshold, where high value businesses can counter with coercive strategies of their own, such as threats to leave a jurisdiction or domestic market. For example, consumer apps such as WhatsApp and Signal threatened to leave UK markets in response to drafts of the Online Safety Bill that propose state access message metadata, bypassing end-to-end encryption, and OpenAI and other tech startups' resistance to safety provisions in the European AI act.

High-value businesses have increased bargaining abilities which can overcome the state's coercive strategies and impact national security. In democratic capitalist systems in particular, the state may interpret higher economic value in a private actor, such as a tech platform, as a proxy for societal trust, which it can instrument to foster political trust to achieve domestic objectives. In general, the state is better positioned to exercise cooperative strategies the more "private" the actor becomes in such political economies, at the potential short-term trade off in public goods such

as national security, to use the reputational or economic leverage gained in cyberspace. Low-value businesses look to forming economic interdependences with higher value actors through interaction in the supply chain, in part to benefit from the free rider benefits that come with the high value actor's bargaining power with the state.

Third, legal and regulatory incentives. High-value businesses in market economies can coerce the state's regulatory apparatus towards extreme situations such as regulatory capture; the resulting entrenched power allows the private actor to exercise "state-like" strategies, as any attempt for the state to remove its own interdependences may be too expensive. Political compliance thresholds imposed in authoritarian systems, on the other hand, allow the state to coerce even high-value businesses and their lower-value dependencies. China's dynamic regulatory model can tighten or loosen regulatory controls quickly in the absence of dissent to its top-down hierarchies and severe domestic information asymmetries, but pivoting comes at the cost of high volatility and disengagement of the private sector.[71]

Depending on the type of market failure correction, Western counterparts can instrument regulation that imposes a greater proportional cost on lower-value businesses to comply, but can generate the same public good in other jurisdictions because of interdependent information flows, such as data protection through the EU GDPR. Although the effect of the regulation, such as antitrust, reroutes the direction of information flows to limit the economic benefit to private actors from gatekeeping, the formulation of regulation is based on cooperative strategies in liberal democratic systems that trade-off slow reversal for greater stability between industry and

71. A.H. Zhang, *High Wire: How China Regulates Big Tech and Governs Its Economy* [in en] (Oxford University Press, 2024).

state allies. In contrast, Zhang's model uses Chinese tech regulation as an implicit trust process between state and industry, which industry uses to calibrate self-regulation in practice where state coercion is too expensive.

In summary, private actors, especially industry actors, must balance their structural vulnerabilities to state coercion with market competition; the imposed cost on the actor to remain competitive will also be passed to low and high value businesses in the supply chain. In May 2024, Huawei smartphones replaced Google's Android operating system with a proprietary OS to evade US export controls, at significant cost to WeChat and other smaller app developers, who must rewrite apps to remain OS compatible.[72] If the state's coercive capabilities are too aggressive, it may still achieve its national security goals, but change trusted information flows within the private actor ecosystem that encourage competition by reducing the cost of innovation or integration. As private actors seek power parity with competitors, their reciprocal strategies towards foreign and home state capabilities are guided by the same structural incentives as middle power states in state-state dynamics; strategic choice may allow rising private actors to use cooperative regulatory and economic state strategies while evading too-close political coupling.

On the other hand, the state actor, in its several roles vis-a-vis private actors, such as a regulator of private information flows in tech ecosystems, a buyer of offensive cyber capabilities, a partner on public-private defensive strategies, has limited coercive abilities on cyberspace directly as offensive cyber capabilities are not without technological interdependences. Instead,

72. I. Fujino, *Huawei breaks free from Google ecosystem with homegrown OS, Nikkei Asia* [in en], Available at: 2024, https://asia.nikkei.com/Business/China-tech/Huawei-breaks-free-from-Google-ecosystem-with-homegrown-OS..

the state uses political coupling, economic and legal incentives or punishments to shape political and economic information systems, for which cyberspace serves as the underlying communication channel by facilitating information flows. Policymakers must balance existing trust relations and interdependences in all three information systems to select optimal strategies that reshape networks in cyberspace and meet their national objectives. In describing China's statecraft towards regional powers, Huang[73] characterises China's engagement as asymmetric by default. The state adopts a mix of "uniform" and "selective" strategies towards its neighbours, based on structural factors such as relative power, existing "alignment", or competitor status. In cyberspace, to continue asymmetric engagement with competing states, it must overcome a low-trust domestic environment of fluctuating coercion, high volatility and fragility to maintain or expand its whole-of-nation coercive leverage, otherwise risking fragmentation in business-state trust relations to create new national security vulnerabilities.

2.6 Conclusion: The impact of trust relationships on structures and statecraft

A political theory of cyber statecraft may be instructive for national security strategists and scholars in analysing, predicting, or responding to adversarial behaviour in cyberspace. An adversary's structural position in domestic and foreign ecosystems, using the tool of political economy, can form the basis for these dynamics. The use of political economy as

73. Yuxing Huang, *China's Asymmetric Statecraft: Alignments, Competitors, and Regional Diplomacy* (UBC Press, February 15, 2023), ISBN: 978-0-7748-6814-3, Google Books: xCSpEAAAQBAJ.

an analytic tool for cyberspace behaviour and governance is not new; using the theory of 'structuration', Powers and Jablonski[74] argue that "the real cyber war... is a competition between different political economies of the information society". In this chapter we have constructed a conceptual framework that unites the political economy variables of power and interdependence through an explicit approach to trust within information systems such as cyberspace.

Our discussion omits specific military aspects of cyber statecraft, in particular, the mobilisation of state and private actor capabilities in the military domain and the application of trust relations. This is, in part, due to the complexity generated by multiple roles assumed by the state. Previously opaque structures within authoritarian governments are changing towards a separation of roles in cyber statecraft; even the Chinese state, which has traditionally seen information warfare as a homogenous offensive front through the Strategic Support Force, has now separated its military activities within the PLA through a new Information Support Force, in addition to state and provincial bodies.[75] Its British and American counterparts, namely the National Cyber Force and US Cyber Command, have published responsible behavioural standards they claim to abide by, as well as making the case for efficient use of taxpayer funds. Capturing the specific, complex role contexts played by a state across conflict domains may be useful for future work on theorising the development and mobilisation of a state's cyber power.

74. S.M. Powers and M. Jablonski, *The Real Cyber War: The Political Economy of Internet Freedom* [in en] (University of Illinois Press, 2015).

75. M. Nouwens, *China's new Information Support Force, IISS* [in en], Available at: 2024, https://www.iiss.org/online-analysis/online-analysis/2024/05/chinas-new-information-support-force/.

We conclude with three implications of our theory for cyber statecraft. Firstly, the role of entrenched trust relationships over time. One possible outcome of structural shifts in cyberspace is fragmentation — similar to what some analysts suggest is happening in the global financial system — where accessibility of the open Web is restricted by geopolitical boundaries and protectionist infrastructure. The literature on fragmentation is vast, with varying and often contradictory conceptions of cyberspace itself,[76] but in the language of our conceptual framework, it points to a hardening of trust relations over time at the cost of forming new ones, leading to the formation of "information enclaves". The Western intelligence community has long raised fears of a so-called 'balkanisation', most recently in the aftermath of China's proposals to the UN ITU for new Internet architectures that reflected its objectives of cyberspace sovereignty.

However, policy responses such as increased emphasis on norm-contesting[77] in what has been characterised as an anarchical space, may have deepened the emerging cyberspace phenomenon that prioritises trust based on identity, rather than information integrity. While national security strategies may incentivise states to contain information flows within their jurisdictions, in liberal democracies, fragmentation leads to a security paradox where increased information asymmetries lead to poorer defences and security, as seen in military cyber incident response initiatives.[78]

The paradox presents two corollaries regarding the impact of these

76. M. Mueller, *Will the Internet Fragment?: Sovereignty, Globalization and Cyberspace* [in en] (John Wiley & Sons, 2017).

77. "Office of the Director of National Intelligence, 'US-Backed International Norms Increasingly Contested'" [in en], Available at: *Report October*, 2022, https://www.dni.gov/files/images/globalTrends/GT2040/NIC-2021-02491_GT_Future_of_Int_Norms_22Mar22_UNSOURCED.pdf.

78. E. Cardon, "Fighting Alone is called Losing: The Unlearned Lessons of Fragmented Systems'" [in en], *The Cyber Defense Review* 7, no. 1 (2022): 75–82.

structural changes to future trust relationships. Firstly, the strategic implications of "who to trust" rather than "what to trust" on decision-making in middle powers and how they will choose to align themselves in future, as well as the future of trust in multilateral institutions, such as the UN itself. Secondly, that in a bid to reduce information asymmetries caused by fragmentation, covert activity in cyberspace, such as espionage, will further rise to compensate for the resulting leverage deficit — the US Cyber Command strategy of "persistent engagement" is a recent example.

Recent scholarship on national strategies for a fragmented cyberspace acknowledges the renewed need for building trust, using tried-and-tested liberal democratic instruments of trade agreements, aid, coalitions and partnerships with aligned public and private players, and norm-building,[79] but admits that the suggestion of former Japanese premier, Shinzo Abe, that "trusted data flows" should be prioritised over spreading Western-style democracy was an effective guiding principle.

Secondly, the ability for effective response to structural changes, desirable or otherwise. In particular, the adaptiveness of nation-states to leverage their domestic public-private relationships to achieve foreign policy objectives. Chinese analysts appear to have noted growing divergences in the American and European political economies, the resulting security implications since the 2008 financial crisis,[80] and abandoned a liberal economic approach.[81] Top-down, centralised leadership in China has enabled

79. N. Fick, "Confronting Reality in Cyberspace: Foreign Policy for a Fragmented Internet" [in en], Available at: *Council on Foreign Relations*, 2022, https://www.jstor.org/stable/resrep42123..

80. Yao Xiaohong, *Zhongguo meng: weilai guojia zhanlue yu Zhongguo jueqi [The China dream: future national strategy and China's rise* [in zh-Latn] (Beijing: Dangdai Zhongguo, 2013), 15.

81. Norris, *Chinese Economic Statecraft: Commercial Actors, Grand Strategy, and State Control*.

rapid coercion strategies to control tech platforms domestically, for example, bypassing bureaucratic norms, citizen dissent, and civil society to reverse a regulatory regime that was reliant on Western capital, but at the severe cost of high domestic volatility.[82] Some security researchers have linked China's 2021 law on vulnerability disclosures with increased offensive cyber activity.[83]

On the other hand, coercive strategies in Western nation-states vary in their effectiveness based on political economic attitudes: the European Union's approach to regulating the tech sector for anti-trust and anti-competitive behaviour through the Digital Markets Act, for example, indicates the underlying basis of such policies as rooted more in social welfare rather than in the American perspective of a market-based approach.[84] One potential trade-off of slower mobilisation of domestic private-partner relationships is the increased independence of industry to innovate, diversify its supply chains, and contribute to structural changes in a more stable manner.

Thirdly, the stability of coalitions based on a vaguely defined common interest versus trust-based relations which may be long-term and strategic, or short-term and tactical in nature. The degree of interdependence within coalitions of competitors in different sectors that show adversarial behaviour to so-called Western interests in cyberspace, such as China, Russia, Iran, and North Korea is a salient example. Offensive cyber operations

82. A.H. Zhang, "Agility Over Stability: China's Great Reversal in Regulating the Platform Economy"' [in en], *Harvard International Law Journal* 63 (2022): 457.

83. Group, *Charting China's Climb as a Leading Global Cyber Power'*.

84. Nicholas Zúñiga et al., "The geopolitics of technology standards: historical context for US, EU and Chinese approaches," *International Affairs* 100, no. 4 (July 10, 2024): 1635–1652, ISSN: 0020-5850, https://doi.org/10.1093/ia/iiae124, https://doi.org/10.1093/ia/iiae124.

originating from 'CRINK' can spark two opposing types of policy recommendations: to either retaliate against the "common interest" rather than the specific adversary,[85] or to analyse adversaries' interests for similarities rather than comparing them, as seen in recent literature on great power cyber competition,[86] missing the opportunity to compare their tradecraft and exploiting its differences. This may, in part, be due to a growing consensus that "the attribution problem" of who to blame for cyberattacks and how to punish them is outliving its usefulness as a deterrent instrument in cyberspace.

However, simply challenging hegemonic power does not mean that self-interest need also be aligned with common interests. While defence commentators in the West perceive of this coalition of non-liberal democratic or authoritarian governments as a new "axis", it has coercive dynamics of its own. Each player has associated structural strengths and weaknesses, and relative power. China's "all-of-nation" approach to offensive cyber activity and domestic structures are in stark contrast with Iran's cyberspace posture, or North Korea's extortion-based attacks to support its political economy. The national objectives these adversaries seek to fulfil, manifested through destabilising actions in cyberspace, seemingly intend to produce sectorial outcomes. Simple belligerence towards various aspects of Western polities and economies may not form the basis for stable foreign relations.

Dyadic relations, in addition to group relations, may be another useful indicator. Russia's alleged military alliance with North Korea two years

85. Blagden, "Deterring Cyber Coercion."

86. M. Grzegorzewski and C. Marsh, "A Strategic Cyberspace Overview: Russia and China"' [in en], in *Great Power Cyber Competition* (Routledge, 2024).

into the Ukraine war may compel the Chinese to further undermine North Korea by assuming the role of primary supplier, or move limit the relationship's outcome by coercing Russia. Finally, domestic structures are key; the future of China's domestic political economy may well indicate its changing statecraft.[87] Any emerging threat must be appraised through the short- and long-term viability of these networks in relation with their domestic contexts; Western media, Chinese whistleblowers and dissidents portray Xi Jinping as an unpopular leader. Chinese economy has been volatile since Covid-19, and further asymmetric engagement with the West may exacerbate this, but China has disproportionately high coercive power in its own fragile coalitions. The sustainability of this power, and for the West to "... yield to pragmatism" will mean that the "geometry of the future is variable".[88]

2.7 Situating espionage in statecraft

The trust-interdependence-power framework in the context of espionage raises questions on strategic intent, and operational questions on the deployment of dual-use technologies. As a covert competition strategy, espionage proves a risky proposition vis-a-vis misinterpretation leading to escalation, albeit less costly than other coercive cross-domain measures. The strategic intent behind espionage-like activities may be misread by the target. If the target misinterprets espionage as operational preparation for

87. Norris, *Chinese Economic Statecraft: Commercial Actors, Grand Strategy, and State Control*.

88. N. Inkster, "Power Versus Pragmatism: Unlearned Lessons in Dealing with China"' [in en], *The Cyber Defense Review* 7, no. 1 (2022): 41–50.

a serious attack, it may be drawn into warfighting responses.[89] If the target misinterprets espionage as cybercrime, it may deploy tactical defences that fall short of securing against the true cost of long-term data loss. Given the unreliability of signalling, despite making technically accurate attributions, the target can overestimate imposed costs, leading to conflict escalation, or underestimate, encouraging the coercer to expand the scale of its campaign. Furthermore, intent, actual or perceived, can signal trustworthiness, leading to the formation of new information networks, or the defection of actors in established networks. Dual-use technologies subvert trusted information flows by exploiting cooperation between network nodes to coerce, especially after the costs of defection in interdependent networks are too high for the target.

The intent of the coercer may be ambiguous as the coercer simultaneously fills leverage deficits in other domains. To capitalise on its economic espionage in cyberspace, China has invested significantly in domestic industries and situational awareness to materialise intellectual property theft into competitive advantage, yet falls short in military technology and innovation, in part due to a top-down governance model historically[90].[91] Yet

89. Ben Buchanan and Fiona S. Cunningham, "Preparing the Cyber Battlefield: Assessing a Novel Escalation Risk in a Sino-American Crisis" [in English], in *Cyberspace and Instability*, ed. James Shires, Robert Chesney, and Max Smeets, Accepted: 2023-04-12T05:30:58Z (Edinburgh University Press, 2023), https://library.oapen.org/handle/20.500.12657/62312.

90. Jon R. Lindsay and Tai Ming Cheung, "From Exploitation to Innovation: Acquisition, Absorption, and Application," in *China and Cybersecurity: Espionage, Strategy, and Politics in the Digital Domain*, ed. Jon R. Lindsay, Tai Ming Cheung, and Derek S. Reveron (Oxford University Press, May 2015), 0, ISBN: 978-0-19-020126-5, https://doi.org/10.1093/acprof:oso/9780190201265.003.0003, https://doi.org/10.1093/acprof:oso/9780190201265.003.0003.

91. Andrea Gilli and Mauro Gilli, "Why China Has Not Caught Up Yet: Military-Technological Superiority and the Limits of Imitation, Reverse Engineering, and Cyber Espionage," *International Security* 43, no. 3 (February 2019): 141–189, ISSN: 0162-2889, https://doi.org/10.1162/isec_a_00337, https://doi.org/10.1162/isec_a_00337.

Chinese cyber espionage efforts have intensified, especially in the military domain, as the PLA has reorganized its Strategic Support Force into Space, Cyberspace and Information Support Forces. Beyond the pervasive espionage aimed at advantage in economic competition, in recent years targets comprise corporate intellectual property as well as personnel data in US military, defence, and wider government organisations, healthcare insurers, and credit brokers.[92] While some analysts allude the intent to blackmail, China's extensive domestic monitoring may be a better framework to understand its coercive aims in what it perceives as self-defence in countering outsized US influence.

Intent is crucial in forming deterrent logic. Neither cyber deterrents, through the amassing of exploits and commercial spyware, nor investment in cyber defenses have discouraged Chinese espionage, despite imposing the resulting greater costs of offensive capability, which China seemingly meets through growing influence in other domains. A deterrent strategy of persistent or active engagement, or applying the principles of nuclear detente, such as mutually assured destruction, will not contain digital espionage.[93] As such, the possible strategic advantages confer, albeit limited and uncertain, potentially cover national security, counterintelligence, political advantage in diplomatic negotiations, economic advantage in accessing intellectual property, containing conflict escalation, and expanding

92. Ben Buchanan, "Strategic Espionage," in *The Hacker and the State*, Cyber Attacks and the New Normal of Geopolitics (Harvard University Press, 2020), 86–107, ISBN: 978-0-674-98755-5, https://doi.org/10.2307/j.ctv3405w2m.7, https://www.jstor.org/stable/j.ctv3405w2m.7.

93. Joseph S. Nye Jr., "Deterrence and Dissuasion in Cyberspace," *International Security* 41, no. 3 (January 2017): 44–71, ISSN: 0162-2889, https://doi.org/10.1162/ISEC_a_00266, https://doi.org/10.1162/ISEC_a_00266.

influence. The high costs of espionage campaigns[94] supported by the state will continue to grow: in the event of increasing protectionism in Internet governance, complementing China's strategy of cyber sovereignty, cybersecurity will conversely increase redundancy in security research, and therefore, the cost of offensive and defensive tools. As discussed in Chapter 4, the upfront costs of developing 0-days into exploits is also higher, owing to a professionalisation of the vulnerability research community via exploit brokers. But despite rising operational costs, the possibility of multiple strategic advantages may be one reason for increasing coercive activity. Given economic interdependence with the West through both trade and labour markets, unlike the strategic intent in Soviet espionage during the Cold War, Chinese espionage may confer advantage in other competition domains than replicating technology capabilities.

Western counter-strategies on containing adversaries' development of espionage-facilitating tools must reflect deterrent logic. In government publications outlining their vulnerability equity process, member agencies of the Five Eyes stress on a policy of disclosure of vulnerable technologies as the preferred option. While vulnerability disclosure makes asymmetric information flows symmetric, as the knowledge of a vulnerability is made public, nation-states cannot leverage symmetric information flows to project power. However, symmetric information flows, such as on social media, can be leveraged for influence campaigns. Additionally, disclosure of espionage capabilities, as seen in the Snowden leaks, the NSA-Shadow Brokers dump, the Russia-Vulcan leaks, and the China-Anxun leaks, can

94. William C. Banks, "Cyber Espionage and Electronic Surveillance: Beyond the Media Coverage The 2016 Randolph W. Thrower Symposium Redefined National Security Threats: Tensions and Legal Implications" [in eng], *Emory Law Journal* 66, no. 3 (2016): 513–526, https://heinonline.org/HOL/P?h=hein.journals/emlj66&i=531.

create new asymmetries benefiting both adversaries and third-party actors in politically-motivated espionage aimed at influence-building. Reversing asymmetries impose security costs on adversaries, but can have knock-on effects on defence; China's mandatory reporting of industry actors discovering vulnerabilities, creating potential exploit stockpiles, is a double-edged strategy where patches in Chinese tech products are unavailable even if the state is aware of the vulnerability. Calls for multilateral cooperation on standardising the vulnerability equity process are well-founded, but due to likelihood of misinterpreting intent, insufficient in applying strategic deterrence.

Underlying intent may simply be one of scale, especially befitting cross-domain covert action. Key private actors that command high economic value in global supply chains, providing mass-market technologies or critical components for civil infrastructure, serve as leverage points for nation-states in coercing downstream actors in the supply chain, as well as consumers in digital economies. The development and deployment of exploits on so-called dual-use technologies achieves objectives at scale. To exfiltrate data from these computer networks in any meaningful, long-term operational setting may expand the state's reliance on equities to consuming proprietary tooling, such as spyware or other custom malware. The term dual-use is intended for both software that serves information flows that may be exploited for gaining network access, as well as the dual-use of malware itself in multiple settings such as ransomware or espionage, depending on the coercer's intent. In particular, non-aligned, rising, and middle powers that are outliers to great power competitions may find these particularly useful, as they lack the pervasive surveillance capabilities of

the US, the economic, legal and regulatory chokepoints of China, and do not have enough economic power to bargain sufficiently with high value global private actors.

The transformation of credible threat into coercion, and coercion into concessions, requires these state actors to bolster alliances with private actors who are aligned to a sympathetic great power's interests. Israeli spyware companies, for example, have served multiple EU member states in inter-state operations, and historically shared infrastructure and capabilities with the US. As such, political trust is reflected in trusted information flows that share the knowledge of exploits and vulnerabilities. However, both dual-use offensive capability, as well as consumer software, such as apps, that may be weaponised, are controlled by levers such as export control, which may undermine intent. Dual-use, in practice, is meaningless from the target's perspective,[95] which neuters the practical effects of export control. Furthermore, economic protectionism of commercial offensive capabilities, rendered through export control, restricts the flow of trusted information across jurisdictions, which creates a leverage deficit in non-aligned states' deterrents, in reducing access to offensive capabilities. It further undermines the security of technologies for all actors, even as the knowledge of vulnerabilities in the technology may become public and yet conflict with private actors' own bug bounty programmes. As in the Apple-Pegasus case, the private actor's incentive drive vulnerability remediation as information flows become symmetric.

Symmetric information flows indicate bilateral trust and even power

95. Lena Riecke, "Unmasking the Term 'Dual Use' in EU Spyware Export Control," *European Journal of International Law* 34, no. 3 (August 2023): 697–720, ISSN: 0938-5428, https://doi.org/10.1093/ejil/chad039, https://doi.org/10.1093/ejil/chad039.

dispersion; asymmetry hedges trusted information flows in the direction of the more powerful actor. More broadly, as asymmetries favour power balances towards the state actor over non-state and private actors,[96] trust dynamics in information networks, such as defections over long-running networks, must be mediated by a stewardship mechanism to enable private actors in ensuring secure and reliable information flows, which stabilise network topologies despite the impact of espionage campaigns. The next chapter models these trust dynamics.

96. David Tucker, "The End of Intelligence: Espionage and State Power in the Information Age" [in en], in *The End of Intelligence* (Stanford University Press, August 2014), ISBN: 978-0-8047-9269-1, https://doi.org/10.1515/9780804792691, https://www.degruyter.com/document/doi/10.1515/9780804792691/html.

Chapter 3

Modelling trust dynamics in networked ecosystems

The body of this chapter was co-authored with Professors Julian Williams and David Pym.

3.1 Overview

This chapter constructs a model based on the concepts of trust, interdependence, and power outlined in Chapter 2 to validate answers to RQ2: how do trusted information network affect power structures? Cooperation and defection of actors in information networks require effort to generate public or commercial goods, or trade-off individual profit and penalise other actors in the network, respectively. Actor strategies are based on actor preferences and network structure in the model. Allowing for random behaviour in strategic action and long-running networks captures dynamics of public-private actor relationships. In particular, concepts such as 'privateness' are made explicit through proximity of nodes in the network. Network

volatility arising from randomness in actor interactions sets up arguments for RQ4, answered in Chapter 4, Section 3. The model finds that for hub-and-spoke and bipolar structures, optimal strategies for individual actors result in no dominant steady state network configuration.

The conception of trust as a process in information systems, such as cyberspace, has implications for both stability in cyberspace, as well as strategic stability in actor power relations. In capturing the individual agency of public and private actors, and constraining agent-based strategic behaviour to limited visibility of network structures, public and private actors must balance cooperative and competitive capabilities in line with their contextual preferences. In particular, the simulation of real-world constraints in doing so validates a key substantive feature of the conceptual framework, the argument on opposing domestic political economies.

This model of network games has two innovative features: first, ergodicity, or the ability of actors to occupy every possible node in a long-running game; second, stochastic behaviour, where nodes are capable of random action. Individual actors in the network balance agency with limited knowledge of the network structure to choose between a higher individual payoff from defection or continue cooperation, accruing production of a public good. Each actor, represented by nodes in the network structure, possesses information kept private to the network through aggregated effort. The model allows for third-party policy interventions, adding fluctuations to the network structure. Based on trade-offs between individual effort and payoff upon defection, the model discusses optimal strategies for agents' forward-planning, and how network structures evolve over a long time with resulting collaboration-defection dynamics.

Questions of trust vis-a-vis security arise in the context of networked systems. Where actors in networked ecosystems each possess valuable information, kept private as a property of network structure and actor cooperation , we present a new treatment of network games that models the dynamics of trust in such cases. Our treatment is applicable to a wide range of security and privacy problems, for example, trust in online ecosystems, the security of critical infrastructure, the market for 0-day vulnerabilities, and the adoption of privacy-enhancing technologies. In each of these cases, specific models have been proposed. We show that our treatment captures a variety of these specific models. Our framework models cooperation and defection in an exogenously evolving, but long-run ergodic, actor network. Actors motivated to disclose information private to the network, defecting on other actors, accrue a payoff greater than that received from cooperation. The remaining actors in the network suffer a significant loss. In most cases, the production of the public good from some intensity of effort by the cooperating actors suffers significant harm. This chapter seeks to benchmarks behaviours of collaboration and defection under conditions of uncertainty and strategic choice, in designing a framework for modelling such phenomena that allow choices on the long-run equilibrium structure of the network, choices on the preference set of individual actors, and allow for interventions by third parties through supervisory regulatory mechanisms.

3.2 Introduction

Security and privacy in information flows are a key concern in the context of networked systems. we present a new treatment of network games that is

applicable to a wide range of security and privacy problems, and apply the treatment to public-private actor dynamics in the context of international security and intelligence assessment. Related topics of interest include, for example, trust in online ecosystems,[1] critical infrastructure management,[2] and the adoption of privacy enhancing technologies.[3] In each of these cases, and more, specific models have been proposed. we show that our new treatment captures a wide of these specific models.

Conceptually, we are in general concerned with ecosystems of systems that interact in both space and time, through both collaboration and defection. Systems themselves have network structure, have agents that behave strategically with limited rationality, have resources consisting not only of system assets but also of current and (expected) future investment, and process information, conceived of as the agents' knowledge of the system's resources and network dynamics.

We address the problem of how to build models of such ecosystems and their behaviours that capture the real phenomena well enough to provide appropriate intuitions, but which are still sufficiently tractable to provide clean predictions of the impact of specific stimuli or constraints. Our framework is designed to give flexibility on the structure of the network and the degree of randomness in the node structure using ergodic Markov chains. The individual agents are strategic, forward-looking players that have several actions to undertake. Initially, they make costly investments

1. Christos Ioannidis et al., "Resilience in information stewardship," *European journal of operational research* 274, no. 2 (2019): see for instance.

2. Fabio Massacci et al., "Economic impacts of rules-versus risk-based cybersecurity regulations for critical infrastructure providers," *IEEE Security & Privacy* 14, no. 3 (2016): 52–60.

3. Karen Elliott, Fabio Massacci, and Julian Williams, "Action, inaction, trust, and cybersecurity's common property problem," *IEEE Security & Privacy* 14, no. 1 (2016): see for instance.

in the network and we define this as their 'intensity' of effort in interaction. Then, in each round, the agents can choose to defect, and receive some fixed proportion of the public good formed by the aggregation of connected intensities, or cooperate, and adjust their intensity level. Random fluctuations in the network structure then simulate idiosyncratic and aggregate shocks.

There is a growing extant literature on stochastic games and their use in guiding laboratory experiments, interpreting evidence from data driven analysis, and, of course, the subsequent design of regulations and legislation. Ho ever, there are significant challenges for the modeller in deciding on how to trade off information, complexity, and decision-making. For instance, how much forward planning should each agent be capable of undertaking? How should incomplete cognition be modelled at the individual and aggregate level?

Work by,[45],[6] and[7] has suggested that even simple cooperation-and-defection games can have significant complexity once uncertainty on the future is included and more than two players are considered. In these games, players have limited action and whilst the results are intuitive their ability to capture dynamism in structure are questionable. At the other extreme are models such as JUNE ([8]), which capture high levels of spatial

4. Lorens A Imhof, Drew Fudenberg, and Martin A Nowak, "Evolutionary cycles of cooperation and defection," *Proceedings of the National Academy of Sciences* 102, no. 31 (2005): 10797–10800.

5. Martin A Nowak and Karl Sigmund, "Evolution of indirect reciprocity," *Nature* 437, no. 7063 (2005): 1291–1298.

6. Martin A Nowak, "Five rules for the evolution of cooperation," *science* 314, no. 5805 (2006): 1560–1563.

7. Christian Hilbe et al., "Evolution of cooperation in stochastic games," *Nature* 559, no. 7713 (2018): 246–249.

8. Joseph Aylett-Bullock et al., "JUNE: open-source individual-based epidemiology simulation," *Royal Society open science* 8, no. 7 (2021): 210506.

granularity, modelling, say, every agent in a country (the delivered examples are individual agent models for the UK and Germany). In these types of models, agents have zero intelligence, but have random actions driven by data from surveys, census data, and other data-tracking information (such as mobile phone tracking). For policy issues such as pandemic response, a model like JUNE can be useful — the weak assumptions about agents notwithstanding — as it permits simple policies (such as vaccine roll-outs) to be simulated carefully and to analyse the impact on death-rates and transmission. However, a model such as this is almost impossible to apply to systems, such as online communities, in which the decision-making is driven by preference and tradeoffs that rely on some strategic interaction and in which the degree of effort in the production of less easy to measure constructs such as privacy.

The issue of environmental complexity versus the degree of agency in decision-making goes back to[9] and.[10] More recent work, summarized in,[11] including models suggested in[12] and,[13] has utilized the mathematical properties of networks to create models with strategic agents. A good example

9. John F Nash et al., "Equilibrium Points in N-person Games," *Proceedings of the National Academy of Sciences* 36, no. 1 (1950): 48–49.

10. J Ben Rosen, "Existence and uniqueness of equilibrium points for concave n-person games," *Econometrica: Journal of the Econometric Society*, 1965, 520–534.

11. Matthew O Jackson and Yves Zenou, "Games on networks," in *Handbook of game theory with economic applications*, vol. 4 (Elsevier, 2015), 95–163.

12. Daron Acemoglu and Asuman Ozdaglar, "Opinion dynamics and learning in social networks," *Dynamic Games and Applications* 1 (2011): 3–49; Daron Acemoglu, Asuman Ozdaglar, and Alireza Tahbaz-Salehi, "Systemic Risk and Stability in Financial Networks," *American Economic Review* 105, no. 2 (2015): 564–608; Daron Acemoglu, Azarakhsh Malekian, and Asu Ozdaglar, "Network security and contagion," *Journal of Economic Theory* 166 (2016): 536–585; Gabriel Kuper et al., "Who should pay for interdependent risk? Policy implications for security interdependence among airports," *Risk Analysis* 40, no. 5 (2020): 1001–1019.

13. Xiangyu Wu, "Essays on the economics of networks" (PhD diss., Durham University, August 2022).

of these types of games can be found in[14] and,[15] which use a fixed network structure and deterministic payoffs. In,[16] for instance, it is shown that for network games with a positive return to interaction, and hence a public good production problem, the lowest eigenvalue of the network is crucial in determining both the density and degree of uniformity in responsibility for agents producing the public good. This observation is then used to determine the optimal mechanism to destabilize criminal networks. However, for the types of models reviewed here, (a) the choices we re on a fixed network and (b) all decisions we re continuous action variables based around an intensity of commitment to the network.

This choice is deliberate. Computational tractability becomes an issue as all combinations of defections and investments must be solved for within the architecture of the model. From the foundational results in[17] and,[18] the key point is that for any network model that is (a) strongly connected, (b) has actions that are continuous within a set, and (c) for which the payoffs are diagonal concave (hence an optimum exists), then the following result holds: for a random starting point, if each agent self-optimizes versus all other agents' current positions, after a finite number of iterations, the game will attain an equilibrium which will be the unique Nash equilibrium. This result is used extensively in the network games literature either directly or indirectly. The model here is not sufficiently rich enough to predict

14. Yann Bramoullé and Rachel Kranton, "Public goods in networks," *Journal of Economic Theory* 135, no. 1 (2007): 478–494; Yann Bramoullé and Rachel Kranton, "Risk-sharing networks," *Journal of Economic Behavior & Organization* 64, nos. 3-4 (2007): 275–294.

15. Yann Bramoullé, Rachel Kranton, and Martin D'amours, "Strategic interaction and networks," *The American Economic Review* 104, no. 3 (2014): 898–930.

16. Bramoullé, Kranton, and D'amours.

17. Nash et al., "Equilibrium Points in N-person Games."

18. Rosen, "Existence and uniqueness of equilibrium points for concave n-person games."

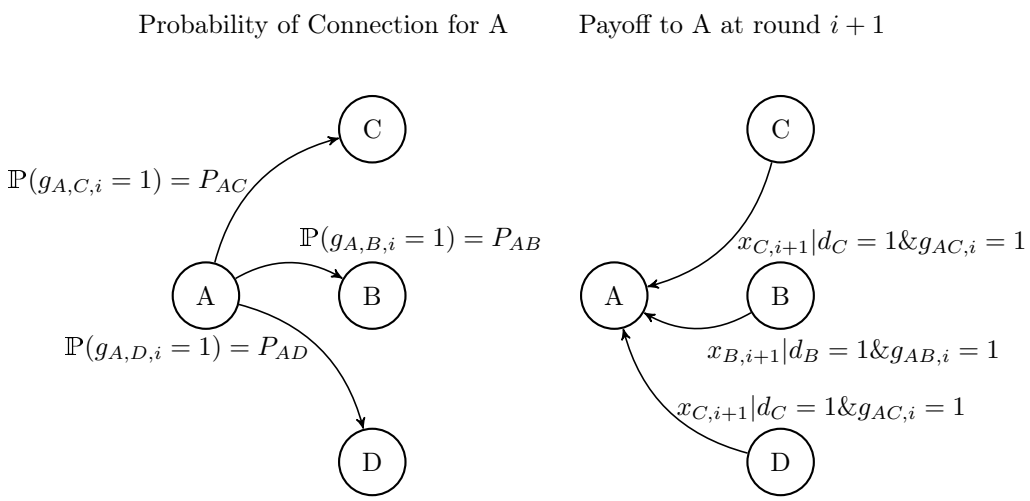


Figure 3.1: For four agents $\{A, B, C, D\}$, illustrates the change in the game state for agent A over rounds i to $i+1$. The left-side diagram presents the probability of a connection bet we en A and the other agents in the game, at $i+1$. This will be contingent on whether a connection exists in round i. A then chooses a level of costly intensity of effort $x_{A,i}$ and decides to cooperate or defect in round $i+1$ with probability $d = \{0, 1\}$. In round $i+1$, agent A receives a payoff proportional to the size of the aggregate intensities $x_{-A,i} = \{x_{B,i}, x_{C,i}, x_{D,i}\}$ if the connecting agents have not defected. If they defect, agent A loses the other agents' effort and suffers an additional proportional loss.

contextual dynamics without well-defined payoff functions and parameters, but nonetheless the simplification allows us to benchmark behaviours of collaboration and defection over long-running networks.

The innovations of our approach are (a) to relax the assumption on the fixed network structure and allow for stochastic connections whilst having an ergodicity in the network structure, (b) to allow for fixed and continuous choices in different iterations, and (c) to provide the modeller with choices on the degree of foresight and individual computational capacity. We accomplish this by a combination of diagonal sub-games iteratively solved in the normal fashion and statistically sampling across the fixed action space. In our example case, the agents iteratively select a continuous level of intensity of input into the game then decide to cooperate or defect given the fixed commitment from the prior round. Fig. 3.1 provides a high-level summary

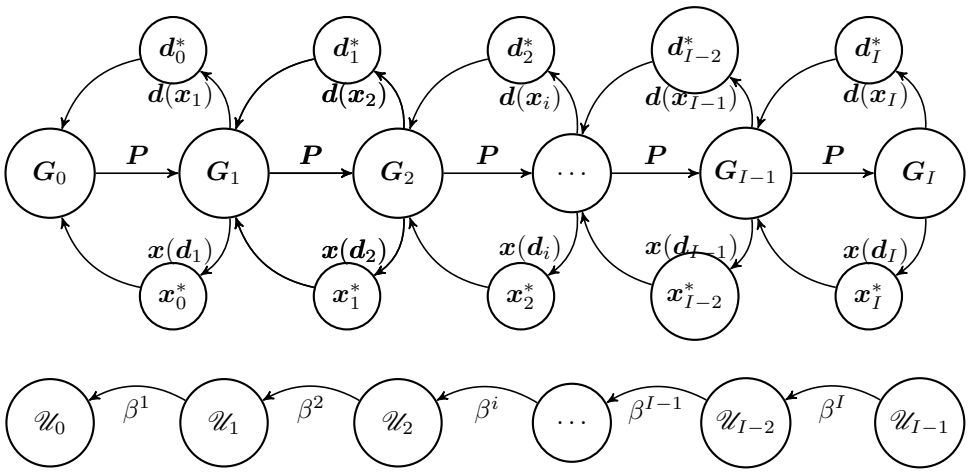


Figure 3.2: The backward recursion of the game state. The network described by the adjacency matrix $\boldsymbol{G}_i$ evolves from $\boldsymbol{G}_1$ onwards to $\boldsymbol{G}_I$ via an ergodic Markov chain with state transition matrix $\boldsymbol{P}$. For each forward iteration, there is a lattice of cooperation/defection decisions for each agent, $\boldsymbol{d}_i$, and an intensity of invested effort, $\boldsymbol{x}_i$, which pays off in proportion to the number of cooperating nodes and their investment.

of a single round of the game, for an illustration with four agents labelled A to D. The sequential choices are that at a prior round, the agents choose a level of costly intensity of effort, they also choose whether to cooperate or defect in the subsequent round. The connections to other agents evolve via a stochastically generated graph with a random adjacency dictated via a Markov Chain. For each non-defecting agent and for each connection, a payoff proportional to the other agents degree of intensity of effort is received. If other agents defect, then there is a penalty instead of a gain. In Fig. 3.2, we show how agents solve, recursively, their optimal strategy assuming some discount factor β.

As an example application, we apply the modelling approach to simulate the cooperation and defection actions within a privacy game. We will then provide some insight from the model to a series of cases connected to the rest of the thesis. First, whilst the network structure matters when assessing the impact of a change in parameters — for instance, when im-

posing a privacy regulation — the timing is arguably just as important; networks near the steady state can have radically different reactions to policy interventions than those further away. Second, but related to the first point, the degree of anticipated dispersion of the network is also important: counter-intuitively, networks with a more random structure are, in certain configurations, often more resilient to policy interventions than those with less dispersion.

3.3 The Model

Let $x_n \in \mathbb{R}_+$ be the intensity of interaction for player $n \in \{1, \ldots, N\}$ and let d_n be the decision to defect or cooperate for the n^{th} player. The higher the intensity, the more player n invests into the platform. This can be thought of as a stake or as a mechanism defining the level of we lfare $u_n = U_n(x_n, d_n | \boldsymbol{x_{-n}}, \boldsymbol{d_{-n}})$.The payoff for increasing x is we akly concave, such that:

$$\frac{\partial u_n}{\partial x_n} \geq 0 \quad \frac{\partial^2 u_n}{\partial x_n^2} \geq 0 \tag{3.1}$$

Let $\boldsymbol{A}_i$ be an association matrix of the graph $\mathcal{G}_i$, where $i \in \{1, \ldots, I\}$ represents a round of the game. we will look at cases in which I and N are potentially uncountable in some manner. Setting $\boldsymbol{a}_{n,j}$ to be a row from $\boldsymbol{A}_i$, where each element of $\boldsymbol{a}_{n,j}$ represents the weighted connection to another player. Each player in a prior round has chosen an intensity $x_{n,i-1}$. This is their commitment to the next round. The elements of $\boldsymbol{a}_{n,j}$ are therefore $x_{j,i}$ $\forall j \in \{1, \ldots, N\}$, if a connection determined by $\mathcal{G}_i$ links player i to player n.

Finally, let $\mathbf{D_i}$ be a decision matrix formed of repeatedly tiled row

vectors $\boldsymbol{d}_i$, formed of zeros and ones, where a 1 indicates that player $n \in \{1, \ldots, N\}$ has decided to cooperate and a 0 indicates that they have defected. The application of effort to generate the intensity $x_{n,i}$ is considered costly, so that there is a function $c_n(x_{n,i})$ that determines the cost of this effort to player n. We will assume that there is a universal discount factor, $0 < \gamma < 1$, that determines the relative valuation of effort and reward in the next round. The payoff for each player, within each round, is determined by the interior product $\pi_{n,i} = \boldsymbol{d}_i' \boldsymbol{a}_{n,j}$.

There is a block-wise Markov transition for which the connection matrix evolves over time. Let $\boldsymbol{g}_i = \text{vec}[\boldsymbol{G}_i]$, where vec[.] is the columnwise stacking operator. This matrix $\boldsymbol{P} = [p_{n,n'}]$ determines the probability that a connection transitions between two agents n and $n' \in \{1, \ldots, N\}$ in the network. Hence in period i, there is a vector $\boldsymbol{\xi}_i$ for which the state transition will evolve such that the probability of a state being connected is $\boldsymbol{\xi}_{i+1} = \boldsymbol{P}\boldsymbol{\xi}_i$. The steady-state probability of a connection is given by the solution of $\boldsymbol{\xi} = \boldsymbol{P}\boldsymbol{\xi}$. Setting $\bar{\boldsymbol{G}}$ to be the long-run adjacency matrix, now set $\boldsymbol{G}^* = \mathbb{E}[\mathcal{G}_{i+j} | j \to \infty]$ and, correspondingly, $\boldsymbol{\xi}^* = \text{vec}[\boldsymbol{G}^*]$. Finally, we will impose a graph operator $G = \mathscr{G}[A|\varphi]$, with threshold φ, such that the operator thresholds the elements of $g_{nm} = \mathbb{1}_{a_{nm} \geq \varphi}$, where $\mathbb{1}$ is the indicator function. Finally, set $\boldsymbol{g}_n$ to be the row of $\boldsymbol{g}$ corresponding to the n^{th} agent.

3.3.1 Nested Diagonal Concavity

Let $\mathscr{M}$ be a game that is played over a number of discrete rounds indexed by $i \in \{1, \ldots, I\}$, with $I \in \mathbb{N}_+$. There is no upper limit on I, so it can be countably infinite. Hence, the model is within a collection of games that

are considered diagonal concave, see.[19]

Within each round, players establish either a finite or infinite horizon pay-off and then solve for equilibrium outcomes in the normal fashion. For instance, let $\mathbf{x} \in \mathcal{X}$ be the set of all viable actions for each player. In the simplest form, $\mathbf{x}_i = [x_n]_i, \forall n \in \{1, \ldots, N\}$ with $x_i \in \mathbb{R}$ and $N \in \mathbb{N}_+$. Hence, actions are modelled by numbers of on the real line, for a possibly infinite set of players. Let $\boldsymbol{x}_{-\boldsymbol{n},i}$ represent the vector of actions for all other players except n at sub-game index i and $\boldsymbol{X}_{-\boldsymbol{n},i}^{(n*)}$ be the collection of all future actions of all players except for n, and $X_n^{(n*)}$ be the set of all actions for player n. Utility is then specified in the following form:

$$\mathscr{U}_{n,i} = U(X_n^{(n*)}, \boldsymbol{X}_{-\boldsymbol{n},i}^{(n*)} | \vartheta_n, \theta) \tag{3.2}$$

where ϑ_n is a set of time invariant environmental conditions subjective to player n, including some form of discount factor and θ is a set of global environmental parameters. In the simplest case, we have a linear discount global factor β and $F(.)$ is time separable; hence we can now construct

$$\mathscr{U}_{n,i} = U(X_n^{(n*)}, \boldsymbol{X}_{-\boldsymbol{n},i}^{(n*)} | \vartheta_n, \theta) = \sum_{j=n}^{n*} \beta^{j-n} f(x_{i,n}, \boldsymbol{x}_{-\boldsymbol{n},i}) \tag{3.3}$$

It is on this type of model that we are focusing our attention. There are already some well-known results in this area for versions Eq. (3.3) when the payoff model that player n has for all other opponents is non-stochastic and each agent is solving for a single round.

Consider the one period setting. Define the matrix $\mathscr{D}_i = \boldsymbol{\nabla} \boldsymbol{U}_i(\boldsymbol{x}_i | \boldsymbol{d}_i)$ as

19. Rosen, "Existence and uniqueness of equilibrium points for concave n-person games."

the Jacobian matrix of first-order derivatives for each player with respect to their own action x_i and all other players actions $\boldsymbol{x}_{-\boldsymbol{n},i}$), that is:

$$\mathscr{D}_i \equiv \boldsymbol{\nabla} \boldsymbol{U}_i(\boldsymbol{x}_i|\boldsymbol{d}_i) = \begin{pmatrix} \frac{\partial \mathscr{U}_{1,i}}{\partial x_1} & \frac{\partial \mathscr{U}_{1,i}}{\partial x_2} & \cdots & \frac{\partial \mathscr{U}_{1,i}}{\partial x_{N-1}} & \frac{\partial \mathscr{U}_{1,i}}{\partial x_{N-1}} \frac{\partial \mathscr{U}_{1,i}}{\partial x_N} \\ \frac{\partial \mathscr{U}_{2,i}}{\partial x_1} & \frac{\partial \mathscr{U}_{2,i}}{\partial x_2} & \cdots & \frac{\partial \mathscr{U}_{2,i}}{\partial x_{N-1}} & \frac{\partial \mathscr{U}_{2,i}}{\partial x_{N-1}} \frac{\partial \mathscr{U}_{2,i}}{\partial x_N} \\ \vdots & \vdots & \vdots & \vdots & \\ \frac{\partial \mathscr{U}_{N-1,i}}{\partial x_1} & \frac{\partial \mathscr{U}_{N-1,i}}{\partial x_2} & \cdots & \frac{\partial \mathscr{U}_{N-1,i}}{\partial x_{N-1}} & \frac{\partial \mathscr{U}_{N-1,i}}{\partial x_{N-1}} \frac{\partial \mathscr{U}_{N-1,i}}{\partial x_N} \\ \frac{\partial \mathscr{U}_{N,i}}{\partial x_1} & \frac{\partial \mathscr{U}_{N,i}}{\partial x_2} & \cdots & \frac{\partial \mathscr{U}_{N,i}}{\partial x_{N-1}} & \frac{\partial \mathscr{U}_{N,i}}{\partial x_{N-1}} \frac{\partial \mathscr{U}_{N,i}}{\partial x_N} \end{pmatrix} \tag{3.4}$$

A well-known result by[20] demonstrates that if $\mathscr{D} + \mathscr{D}'$ is negative definite, then, for some non-zero random starting point $\mathbf{x}_0$, the sequential optimization of players in a one-period game results in a stable equilibrium point describing a unique Nash equilibrium. Indeed, this set of results is the basis for most discrete or continuous sets of games exploiting the properties of the Kakutani fixed point theorem. See[21] for a full explanation and derivation.

3.3.2 Adding Defection

The general results above have been utilized to determine properties of games on graphs and to understand larger-scale versions of classic games such as the prisoner's dilemma as $N \to \infty$. Ho we ver, many of the perceived issues with these classic games are not resolved within this deterministic framework. For instance, in the public good and n-player prisoner's dilemma cooperation only occurs under certain conditions; $I \to \infty$ and specific discount factors. However, empirical results suggest that observed

20. Rosen.
21. Rosen.

cooperation and defection are mode volatile. A further issue is that the cases for cooperation require infinite games and these are only tractable in a limited number of cases.

The suggestion in[22] is that by adding random effects to actions effects suppressed by the strict adherence to the equilibrium path will be forthcoming. Furthermore, in a public good game (PGG hereafter), cooperation can be generated by anticipation of random action and that this can create more balanced game structures, better mapping to empirical observation of phenomena where repeated actions occur, but which are not expected to be infinite (which is claimed to be the majority of cases). In this sense, we are almost always dealing with symmetrical games with N substantially greater than 2 with inheritance of state from round to round. In this case, the global variable θ is now round-dependent, as θ_i, and has a differential impact on each player through f. Then

$$\mathscr{U}_{n,i} = F(X_n^{(n*)}, \boldsymbol{X}_{-\boldsymbol{n},i}^{(n*)} | \vartheta_n, \theta_i) = \sum_{j=i+1}^{n*} \beta^{j-n} f(x_{i,n}, \boldsymbol{x}_{-\boldsymbol{n},i}) \tag{3.5}$$

Each sub-game nests itself in terms of an optimal set of choices from the prior game. Depending on the defect or cooperate choices and the degree of assumed intensity on the pathway.

3.3.3 The value of interactions

Each agent has utility function $u(-)$ that determines their optimal payoff given its statistical model of the other agents to which it might be connected.

22. Hilbe et al., "Evolution of cooperation in stochastic games."

Consider an agent n, connected to C_n agents, each with x_c interactions. When all agents cooperate, the value of the interaction is $x_n \sum x_c$. For each agent that defects in the local interaction space, there is a cost $-x_n x_c$. As such the utility for a given vector of connected decisions is

$$U_n|(d_n = 1) = u(x_n \sum_{c=1}^{C_n} \mathbb{1}_{d_c=1} x_c - \gamma x_n \sum_{c=1}^{C_n} \mathbb{1}_{d_c=0} x_c) \tag{3.6}$$

where γ is a constant. When $\gamma \to 0$, the agents do not care about defecting connections. When $\gamma = 1$, then the value of defections is exactly the same as the value of an equivalent cooperating connection. When $\gamma > 1$, the cost is higher. If agent n defects $d_n = 0$, then agent gains a payoff

$$U_n|(d_n = 0) = u(\delta \sum_{c=1}^{C_n} x_c) \tag{3.7}$$

where δ is a multiplier that determines the value of information to which agent n is connected.

3.3.4 Agents' statistical models of connections

Each agent constructs a statistical model based on the likely agents to which they are connected. The expected connection in round i is

$$\boldsymbol{\xi}_i = \boldsymbol{P}\text{vec}[\boldsymbol{G}_i] \tag{3.8}$$

In a full information system, each agent will look at all agents and assess their likelihood of defection based on the anticipated number of connections their have. Each agent then constructs a statistical model of the anticipated level of intensity invested by the other agents connected to them. Hence

each agent constructs an optimal pay-off using the following expected utility maximization:

$$x^{\dagger}_{n,i}(\boldsymbol{x}^{\dagger}_{-\boldsymbol{n}}, \boldsymbol{d}_n|\boldsymbol{G}_i, \boldsymbol{P}) := \arg\max_{x} \mathbb{E}\left[\sum_{j=0}^{I} \beta^{-j} U_i(x_n, \mathbb{E}[\boldsymbol{x}^{\dagger}_{-\boldsymbol{n}}|x^{\dagger}_{n,i}], \boldsymbol{d}_n)|\boldsymbol{G}_i, \boldsymbol{P}\right] \tag{3.9}$$

where $\mathbb{E}[\boldsymbol{x}^{\dagger}_{-\boldsymbol{n}}|x^{\dagger}_{n,i}]$ is the vector expectations computed for each agent given the optimal responses for each agent across the grid of potential connections. The LHS and RHS of Eq. (3.9) are recursive, as agents form expectations of other potential connections, as follows:

$$\mathbb{E}\left[\sum_{j=1}^{I} \beta^{-j} U_i(x_n, \mathbb{E}[\boldsymbol{x}^{\dagger}_{-\boldsymbol{n}}|x^{\dagger}_{n,i}], \boldsymbol{d}_n)|\boldsymbol{G}_i, \boldsymbol{P}\right]$$

as a function of their own actions. A necessary, but not sufficient, condition is that for an optimal unique fixed point to exist the conditions in Eq. (3.2) to Eq. (3.4) being satisfied and $0 < \beta < 1$ — see[23] for examples of the same technique in other areas and[24] for single period games.

In these types of models, the choice of solution set is determined by numerical search recursively from some future index I, such that the unit utility from the $I + 1$ iteration represents less than the threshold of $1 - \lambda$ fraction of the $j = 0$ time index, for some number λ that is arbitrarily close to unity.

This approach represents a trade-off between models such as,[25] where

23. Angelia Nedic and Asuman Ozdaglar, "Distributed subgradient methods for multi-agent optimization," *IEEE Transactions on Automatic Control* 54, no. 1 (2009): 48–61; Acemoglu and Ozdaglar, "Opinion dynamics and learning in social networks"; Acemoglu, Malekian, and Ozdaglar, "Network security and contagion."

24. Wu, "Essays on the economics of networks."

25. Nowak and Sigmund, "Evolution of indirect reciprocity"; Nowak, "Five rules for the evolution of cooperation"; Imhof, Fudenberg, and Nowak, "Evolutionary cycles of cooperation and defection."

the production of goods in a multiplayer framework is driven by population expectations of payoffs in two parallel games (one with positive returns to collaboration and one without). However, the agents in these models still act with foresight in a manner that can be tractably simulated across a range of simple parameters and network settings, unlike a fully geospatial-agent-based model, such as,[26] where agents have high levels of structure, but do not make strategic choices[27].

3.3.5 Stochastic Networks

Innovative feature of this game is the careful degree of control that can be placed on the random structure of $\boldsymbol{G}_i$. The stochastic structure of the network determined by the Markov chain $\boldsymbol{P}$. For our purposes we will restrict the Markov model based on the following assumptions:

A1. The equilibrium network structure: let $\boldsymbol{\zeta}^*$ be the long run network structure such that $\boldsymbol{P}\boldsymbol{\zeta}^* = \boldsymbol{\zeta}^*$.

A2. From A.1, $\boldsymbol{P} \in \mathscr{Z}$ belongs to the set of all real, non-negative matrices $\mathscr{Z}$ for which the largest eigenvalue is unity and the corresponding eigenvector is $\boldsymbol{\zeta}^*$

A3. Diagonality: Let $\boldsymbol{\Sigma}$ be an arbitrary diagonally symmetric non-negative, right singly stochastic matrix with eigen-decomposition $\boldsymbol{\Sigma} = \boldsymbol{\Xi}^{\ddagger}\boldsymbol{\Delta}\boldsymbol{\Xi}^{\ddagger,\prime}$, where $\boldsymbol{\Delta} = \text{diag}[\boldsymbol{\delta}]$, such that all elements of the vector $\boldsymbol{d}$, $0 < d_n < 1$

26. Aylett-Bullock et al., "JUNE: open-source individual-based epidemiology simulation."

27. Our model also addresses cases where agents demonstrate strategic behaviour with assumptions based on rationality. In particular, games in national security contexts, where agents deploy a range of strategic behaviours, such as coercion, concealment, disclosure, and so on, are able to forward plan for best strategies based on visibility of other, networked agents' behaviours.

are real and non-zero. Finally, let $s_{nm} = \nu_n \sigma^{|m-n|}$, for a decay parameter $0 < \sigma < 1$ and scaling ν that ensures the matrix $\boldsymbol{\Sigma}$ is right singularly stochastic.

A4. From A.2 and A.3, we replace the first column of the matrix $\boldsymbol{\Xi}$, denoted $\boldsymbol{\xi}_1 = \boldsymbol{\zeta}^*$, then set $\boldsymbol{P} = \boldsymbol{\Xi}\boldsymbol{\Delta}\boldsymbol{\Xi}^{-1}$. Hence, there is a right singly stochastic matrix $\boldsymbol{P}$ with an equilibrium eigenvector of $\boldsymbol{\zeta}^*$ and the Markov chains stochasticity is proportional to σ.

Assumptions A.1–A.4 allow for a broad range of equilibrium network structures and careful control over the degree of randomness of the network structure. When $\sigma \to 1$, the network arrangement is highly volatile and connections approach maximum entropy. When $\sigma \to 0$, the network tends to converge on $\boldsymbol{\zeta}^*$.

3.4 Solving the Forward Network Problem

Consider the case in which $N = 20$ and the equilibrium network is cyclical with one hub. In the equilibrium state, each player is connected to the hub and two players either side of them; see Fig. 3.3 for an illustration using a digraph map.

Fig. 3.4 illustrates the equilibrium adjacency matrix diag$[\zeta^*]$. In this case, there is one central node and then a series of bilateral connections. This pattern will, to an extent be imparted into the transition matrix. For instance, when dispersion is added, the likelihood of connections shifting from the central node should be low, but the number of connections randomly occurring outside the central node could be relatively dispersed (depending on the degree of dispersion imparted by the decay parameter

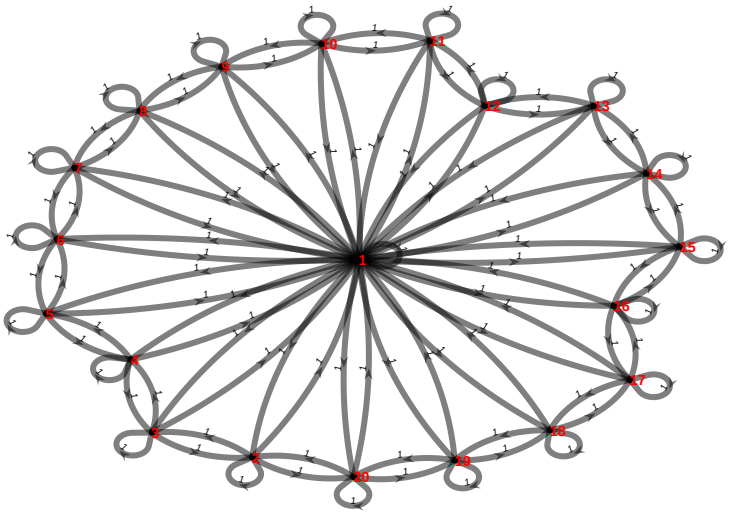


Figure 3.3: The long-run network structure diag[ζ^*] for a single hub and two nearest neighbours network using a digraph network plot.

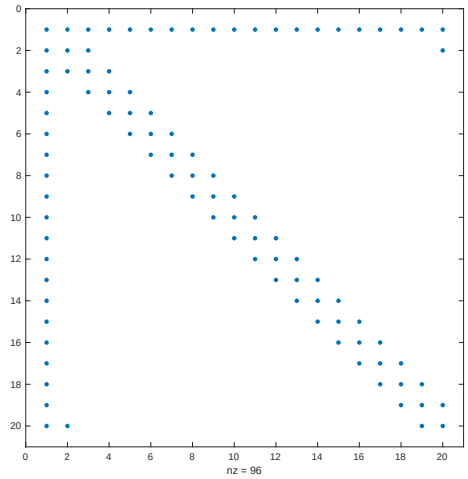
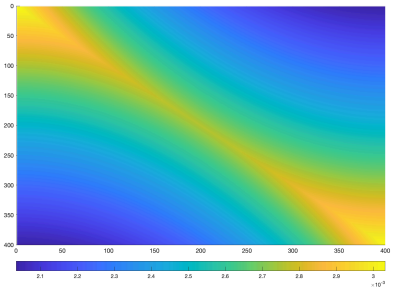
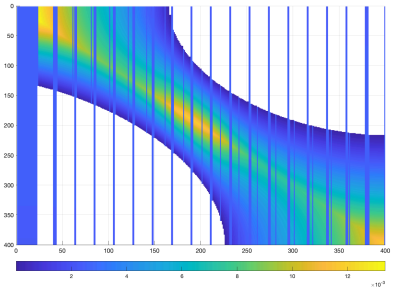


Figure 3.4: Non-zero elements of the adjacency matrix diag[ζ^*] for a single hub and two nearest neighbours network.

σ). Setting $\sigma = 0.99$ — so a very high dispersion — the 400 by 400 singly stochastic dispersion matrix $\mathbf{\Sigma}$ that determines the degree of variability of

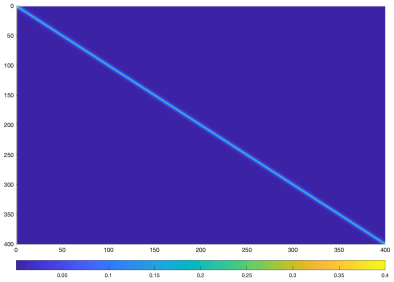


(a) The dispersion matrix $\boldsymbol{\Sigma}$.

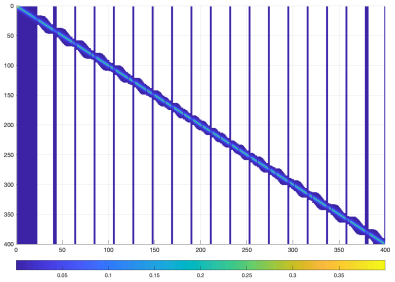


(b) Markov transition matrix $\boldsymbol{P}$.

Figure 3.5: Markov Transitions Stochastic Network, $\sigma = 0.999$



(a) The dispersion matrix $\boldsymbol{\Sigma}$.



(b) Markov transition matrix $\boldsymbol{P}$.

Figure 3.6: Markov Transitions Stochastic Network, $\sigma = 0.6$

the network is illustrated in Fig. 3.5a. This matrix will be the same for all $N = 20$ games, with $\sigma = 0.99$ and is shown in Fig. 3.5a.

It is first important to recall that the matrix $\boldsymbol{P}$ corresponds to the vector vec$[\boldsymbol{G}]$, so vectorizing the adjacency matrix. This mapping is hard to visualize, but the first block of 20 columns represents transitions from the first node. Hence, this is deemed unlikely to ensure that the long-run matrix converges on the desired cycle; that is, the ergodic solution.

Finally, using the algorithm in A.3 and A.4, the unique right singularly stochastic matrix with equilibrium network $\boldsymbol{P} = \text{diag}[\zeta^*]$ has elements with contours as illustrated in Fig. 3.6b. In this figure, threshold probabilities below φ are set to exactly zero and not plotted. we can see that the

block structure ensures that the central node is stable, but that transitions bet we en the outer nodes are possible. Furthermore, if a transition from the central node occurs, then there is clustering around the probability of returning to this node.

3.4.1 Solving for the optimal strategy

We will determine the optimal strategy by sequentially solving for each player, indexed by n, the optimal strategy given the anticipated actions of all other players based on the n^{th} player's statistical model of each other player's optimal decisions in the network. To accomplish this, the modeller has to make a series of choices on the sequence of decisions and then work through backward induction to the optimal choice. This is via backward induction from some arbitrary future point I.

We start with the pure public good version of the game, where all players cooperate $d_{n,i} = 1$, $\forall we \in \{1, \ldots, I\}$ & $n \in \{1, \ldots, N\}$. In this case, the only requirement is an optimal choice pathway for the intensity of interaction $x_{n,i}$. Given a suitable choice of concave utility function, $U(.)$ — for instance logarithmic utility — and discount factor β, then the sub-game for the i^{th} round is diagonal strict concave.

Recall that $\boldsymbol{x}_{i,-\boldsymbol{n}}$ are the strategies of the $N-1$ players not equal to n, setting $\boldsymbol{x}^{\ddagger}_{i,-\boldsymbol{n},a}$ to be the vector that the n^{th} iterates over to compute the optimal reaction function $\boldsymbol{x}^{\ddagger}_{i,-\boldsymbol{n},a}(\boldsymbol{x}_{i,-\boldsymbol{n}})$ and setting $\boldsymbol{U}^{\dagger}_{-\boldsymbol{n}}(\boldsymbol{x}_{i,-\boldsymbol{n}})$ to be the vector of expected utilities for all other players given $\boldsymbol{x}^{\dagger}_{i,-\boldsymbol{n}}$, we will be seeking the sub-solution for a given future iteration starting from $I-b$, $\forall b \in \{1, \ldots I\}$,

Algorithm 1 relies on each sub-game being diagonal strict concave,

Algorithm 1 Solve For Reaction Function at step $I - b$

procedure SOLVE FOR $\boldsymbol{x}^{\ddagger}_{i,-\boldsymbol{n}}(\boldsymbol{x}_{i,-\boldsymbol{n}})$
    set $\boldsymbol{x}^{\ddagger}_{i,-\boldsymbol{n},0}(\boldsymbol{x}_{i,-\boldsymbol{n}}) = \mathbf{0}$
    set $\varepsilon \to 0$
    set $\boldsymbol{x}^{\ddagger}_{i,-\boldsymbol{n},a+1}(\boldsymbol{x}_{i,-\boldsymbol{n}}) - \boldsymbol{x}^{\ddagger}_{i,-\boldsymbol{n},a}(\boldsymbol{x}_{i,-\boldsymbol{n}}) = \boldsymbol{\epsilon}_a$
    set $\boldsymbol{U}^{\dagger}_{-\boldsymbol{n}}(\boldsymbol{x}_{i,-\boldsymbol{n},a+1}) - \boldsymbol{U}^{\dagger}_{-\boldsymbol{n}}(\boldsymbol{x}_{i,-\boldsymbol{n},a}) = \Delta\boldsymbol{U}^{\dagger}_{a}$
Stopping Condition
    if $\Delta\boldsymbol{U}^{\dagger}_{a} < \epsilon_a$ **then return** false
    Set $I >> i$
    Set $\boldsymbol{x}^{\ddagger}_{i,-\boldsymbol{n},0}(\boldsymbol{x}_{i,-\boldsymbol{n}})$
loop:
    if $\Delta\boldsymbol{U}^{\dagger}_{a} < \epsilon_a$ **then return** true
Compute
        $\boldsymbol{x}^{\ddagger}_{i,-\boldsymbol{n},a+1}(\boldsymbol{x}_{i,-\boldsymbol{n}}) + \boldsymbol{\epsilon}_0$
        Find $x^{\dagger}_{m} = \arg\max_{x_m} U_m(x_m|\boldsymbol{x}^{\dagger}_{-\boldsymbol{m}})$
        Repeat $\forall m \in \{1, \ldots, m\}$
        goto *loop*.
    if Stopping Condition **then return** $\boldsymbol{x}^{\dagger}_{a}$
    Set $b = b + 1$
    Move to $I = we - b$
    close;
    goto *top*.
Complete Recursion

hence a random guess of the initial solution will iterate relatively quickly to a sub-game solution. Working backwards from I and discounting, we can then compute the $\boldsymbol{d} = \mathbf{1}$. The computationally intractable component is cycling through the grid of sequential the defection cases.

Let $\mathscr{D}$ be the lattice of all combinations of defection strategies. That is $\mathscr{D}$ consists of the N^N combinations of defections for all players.

$$\begin{aligned}\mathscr{D} := \{ \quad & \{1,1,1,\ldots,1,1,0\},\{1,1,1,\ldots,1,0,1\},\ldots,\{1,1,1,\ldots,0,1,1\} \\ & \{1,1,1,\ldots,1,0,0\},\{1,1,1,\ldots,0,0,1\},\ldots,\{1,1,0,\ldots,0,1,1\} \\ & \quad \vdots \\ & \{1,1,0,\ldots,0,0,0\},\{1,0,0,\ldots,0,0,0\},\ldots,\{0,0,0,\ldots,0,0,0\}\}\end{aligned} \tag{3.10}$$

To search and repeat all defection combinations is impossible, for 20 players, this is 1.0486×10^{26} combinations per forward iteration i hence we will have to make three computability assumptions for the search:

C1. Statistical Symmetry: agents with network ergodically identical network positions will make similar defection/cooperation choices.

C2. Importance sampling: agents rank connections based on the anticipated number of connections.

C3. Statistical determinacy, agents determine the ergodic connectivity by thresholding probabilities $\boldsymbol{\zeta}^*$ with respect to φ.

As such we statistically evaluate the approximated best response curve for the tuple $\boldsymbol{r}_{-\boldsymbol{n},j}(x_{n,j}) = (\boldsymbol{x}_{-\boldsymbol{n}}(x_n), \boldsymbol{d}_{-\boldsymbol{n}}(x_n))_j$ and then construct a lattice $\mathscr{R}_0(x_1,\ldots,x_i,\ldots,x_I) = \mathscr{U}(x_1^*,\ldots,x_i^*,\ldots,x_I^*|(\boldsymbol{x}^\dagger_{-\boldsymbol{n}}(x_n^*), \boldsymbol{d}^\dagger_{-\boldsymbol{n}}(x_n^*))_j)$. Where

the mapping of $d^{\dagger}_{-\boldsymbol{n}}(x^*_n))_j$) is computed via the approach outlined in Algorithm 2.

Algorithm 2 Generating the $\boldsymbol{d}$ Lattices

procedure GENERATE CONNECTION PATHWAYS
  Set number of paths replications B
  Set derive $\boldsymbol{P}$ from $\boldsymbol{G}^*$
loop:
  for $b \in \{1, \dots B\}$
  sub loop:
    for $i \in \{1, \dots I\}$
      Generate $\boldsymbol{G}_i | \boldsymbol{G}_{i-1}, \boldsymbol{P}$
      Save $\boldsymbol{G}_{b,i} \in \mathcal{G}$
      Draw H random vectors $\boldsymbol{d}^{\bullet}$, where $\mathbb{P}(d_i := 1) = \rho$, $\mathbb{P}(d_i := 0) = 1 - \rho$.
      Find $\boldsymbol{x}^* := \arg\max_{\boldsymbol{x}} U_i(\boldsymbol{x}|\boldsymbol{d})$, store in $\mathcal{U}$, using Algorithm 1, $\forall n \in \{1, \dots, N\}$
    close
Cumulative Distribution of Responses: Compute $\tilde{\mathscr{R}}_0(x_1, \dots, x_i, \dots, x_I) = \mathscr{U}(x^*_1, \dots, x^*_i, \dots, x^*_I | (\boldsymbol{x}^{\dagger}_{-\boldsymbol{n}}(x^*_n), \boldsymbol{d}^{\dagger}_{-\boldsymbol{n}}(x^*_n))_j)$ from lattices and sort to find the statistically optimal strategies for $\forall n \in \{1, \dots, N\}$
  close

Solving for the optimal state and summarising that information requires additional assumptions. For example, looking at the analysis from static and dynamic networks,[28] we can see that the way networks are illustrated, normally through some aggregation operator, determines the interpretational setting and the subsequent conclusions drawn.

Consider the collection of (potentially adjoint) operators $\mathscr{A}[\mathscr{D}, \mathscr{U}, \mathscr{X}]$. Here we have three measurements from the game state $\mathscr{D}$, the complete

28. See for instance Naoki Masuda and Renaud Lambiotte, *A guide to temporal networks* (World Scientific, 2016), as a collection of example cases; Xiao Zhang, Cristopher Moore, and Mark EJ Newman, "Random graph models for dynamic networks," *The European Physical Journal B* 90 (2017): 1–14; Tiago P Peixoto and Martin Rosvall, "Modelling sequences and temporal networks with dynamic community structures," *Nature communications* 8, no. 1 (2017): 582; Hadiseh Safdari, Martina Contisciani, and Caterina De Bacco, "Reciprocity, community detection, and link prediction in dynamic networks," *Journal of Physics: Complexity* 3, no. 1 (2022): 015010.

history of defection operations; $\mathscr{U}$, the complete history of welfare outcomes; and $\mathscr{X}$ the complete history of all continuous actions. $\mathscr{D}$ and $\mathscr{X}$ have internally consistent units. $\mathscr{U}$ is a unit-less metric (sometimes simply referred to as *utils*) that is presumed by assumption to be consistently measured by each individual agent only. For both $\mathscr{X}$ and $\mathscr{U}$ measurement is scale independent across agents, however, for $\mathscr{X}$ there is a real world equivalent measure.

3.5 Network Structures and Trust Contexts

Games of nation-state cooperation either neglect network dynamics[29] or assume full visibility of network structures.[30] State interaction with non-state and private actors model opinion formation through social networks[31] and containment of private power under political ideology,[32] but are limited in explaining the network effects of influence-building, in particular, norm propagation or policy diffusion through node dispersion, or intermediary, transnational actors.[33]

29. Kydd, *Trust and Mistrust in International Relations*.

30. Nowak, "Five rules for the evolution of cooperation."

31. Acemoglu and Ozdaglar, "Opinion dynamics and learning in social networks."

32. Daron Acemoglu and James A. Robinson, "Economic Backwardness in Political Perspective" [in en], *American Political Science Review* 100, no. 1 (February 2006): 115–131, ISSN: 1537-5943, 0003-0554, accessed August 28, 2024, https://doi.org/10.1017/S0003055406062046, https://www.cambridge.org/core/journals/american-political-science-review/article/economic-backwardness-in-political-perspective/7DE0FEDD01FA04387AB1F4689CF7944B.

33. Beth A. Simmons and Zachary Elkins, "The Globalization of Liberalization: Policy Diffusion in the International Political Economy" [in en], *American Political Science Review* 98, no. 1 (February 2004): 171–189, ISSN: 1537-5943, 0003-0554, accessed October 22, 2024, https://doi.org/10.1017/S0003055404001078, https://www.cambridge.org/core/journals/american-political-science-review/article/abs/globalization-of-liberalization-policy-diffusion-in-the-international-political-economy/B5221E84026490BEAD28085A42D636C0; Robert O'Brien and Marc Williams, *Global Political Economy: Evolution and Dynamics* [in en], Google-Books-ID: 37soEQAAQBAJ (Bloomsbury Publishing, October 2024), ISBN: 978-1-350-34787-8.

The assumptions of rationality based on visibility of how other agents behave, arising from network connectivity, are compatible with the agents' need to behave strategically. Decisions that involve asymmetric action may be explained by degrees of connectivity and effort expended; perceived irrationality, arising from lack of connectivity or the cost of forward planning and computation; covert action from lack of visibility; and more case-specific behaviours regarding strategic ambiguity, disclosure, ambiguity, can be made with adjustments to the model presented here.

Defection under state coercion captures information flows in static networks, where agent preferences are fixed; these steady-state models explain how network interdependence is entrenched, but not how network structures evolve with changing trust dynamics in the long term.[34] Cooperation models of strategic deterrence, such as 'balance of power', attribute strategic stability to actor agency, rather than to network structures in addition. The model aims to reconcile these concerns in international security by considering cooperation between nation-states, and between state and private actors in specific network structures.

3.5.1 Public-private actor networks

In cyberspace, private actors face a range of strategic choices bet we en defection as profit-seeking agents, and long-term cooperation with states, which requires forward planning and appropriate investment. Effort intensity determines how nodes become proximal and how closely coupled the private actor becomes with the state, and probability of defection under intervention. Networks of these private actors are more susceptible to policy

34. Farrell and Newman, "Weaponized Interdependence."

interventions when closely coupled with state actors. The state is primarily motivated by ensuring welfare outcomes through public goods such as national security, and is incentivised to cooperate with private actors for domestic security, as well as for developing capabilities to strategically compete with other states.

In public-private actor relationships, network ergodicity arises from the demand for goods produced by the private actor. State actors are incentivised to form long-term relationships with private actors, such as commercial security companies, exploit vendors and APTs, to access goods and services for deterrence, surveillance, and national security, such as offensive cyber capabilities. Long-term cooperation with the state in return for sponsorship outweighs defection for these types of private actors. Other private actors that produce technology and communications platforms, form strategies based on demand from non-state consumers in global supply chains. These actors must balance cooperation with states, which allows market access, with costs from regulatory and legal interventions. The state selects strategies based on its roles as regulator, consumer, and coercer of these technologies; the latter for national security objectives.

Polities that mediate information flows across networks provide ex ante topologies. In states with top-down governance models, or strategic governance that meets the state's incentives to mediate information flows, hierarchical relationships bet we en state and private actors are represented with a hub-and-spoke configuration. In states with distributed or devolved forms of governance with multiple stakeholders, some private actors, like technology platforms, can leverage investment from cooperation between non-state consumers in their platforms, to match the state's effort inten-

sity. The resulting advantage of greater visibility of network structures as well as their high value positions in global supply chains determine payoff strategies. These configurations will be explored in a bipolar network topology later in the chapter.

Global supply chains are networked ecosystems[35] operating within and across polities. Any payoff from defection that capitalises on the goods created by the cooperation bet we en actors in supply chains are based on cooperation strategies between each private actor and corresponding public actors. Constraints imposed by the structure of these supply chains influence actor visibility, and based on forward planning, optimal strategies and effort in iterations of the game. Specifically, policy effects on networks in closer proximity to state actors, in contrast to more randomly dispersed nodes or networks further away, leave key private actors, such as those providing critical infrastructure components, susceptible to state intervention. In response, susceptible private actors may decrease effort or defect on coercive states, and seek proximity to other hubs, whereas network in closest proximity increase effort to meet costs of intervention.

Public actors cooperate within and bet we en states. In particular, national security public goods are created through intelligence-sharing, in cooperation between intelligences agencies of the state. These public goods secure critical and public infrastructure. Public goods such as norms, standards, and international law are created through state-state cooperation in multilateral systems. Multilateral cooperation reduces conflict escalation risk by containing the effects of network volatility, as all actors must expend cooperative effort in the long-term. Finally, regional cooperation between

35. Adner, "Ecosystem as Structure: An Actionable Construct for Strategy'."

states can result in resource-sharing and security guarantees, improving strategic competition capabilities against adversaries. Regional state cooperation and inter-agency public actor cooperation are represented in a hub-and-spoke configuration; multilateral cooperation between great powers is represented in a bipolar configuration.

3.5.2 Example parametrisation

Stochasticity in actor interaction, and ergodicity in node interaction are innovative features of the model. Variability in connectivity from high dispersion shows no dominant steady state, unlike in static games, whilst low node dispersion reverts to the original structure. In long-running networks, nodes with stochastic behaviour visit all possible points in the action space. The resulting volatility raises questions on policy interventions that can preserve connectivity through stewardship. Updating preferences, effort, and visibility lends agents their strategic nature. As such, the model is appropriate in parametrising utility and optimal payoff in specific contexts.

Networks of intelligence agencies cooperate to share intelligence and act on states' strategic intent. Agents in the network assign value to the public good derived from cooperation, in this case, an intelligence 'product'. 'Actioning' leads to offence-defence measures to achieve national security and discloses the product, making a logarithmic utility function suitable to represent rapid depreciation in value after disclosure. Defecting on the network results in an agency discarding the intelligence product. The agent with the highest connectivity in the network has incentive to act, but bases its strategy on expending relative effort by anticipating defection of enough agents with lower connectivity. A hub-and-spoke structure is assigned to

the network.

Discounting benefits β applies to future costs from degradation in product value from inaction over time. Utility under agent defection $U_n|(d_n = 0) = u(\delta \sum_{c=1}^{C_n} x_c)$ represents an intelligence agency in the network recouping potential operational costs from actioning as opportunity cost. Random effects in low connectivity agents arise from exogenous factors, such as intelligence sources outside the network contesting the product; high degrees of dispersion through the decay parameter represent distant allies. Assigning an agent n connectivity to C_n agents, each with x_c interactions, structure $\boldsymbol{G}_i$ and Markov chain $\boldsymbol{P}$ such that optimal payoff under expected utility for each agent is as in Equation 3.9.

3.5.3 Example of a more complex network topology

Consider a more complex arrangement of the network, see Fig. 3.7. Similarly, to our previous example Fig. 3.5a there are 20 nodes, but here there are two primary nodes that intermediate the communications of two groups of ten. This is designed to mimic the gatekeeper approach outlined previously in this Chapter.

Here the largest two eigenvalues for the binary graph matrix are large and positive with the last two being large and negative and all others being close or equal to zero. Similarly the two eigenvectors corresponding to those eigenvalues have two large elements (around 3 in magnitude) and most equal to near zero, which is to be expected in a set up such as this where two nodes (1) and (2) act as bi-directional channels for their sets of sub-nodes.

Optimal strategy for agents other than the hub, in when to defect over

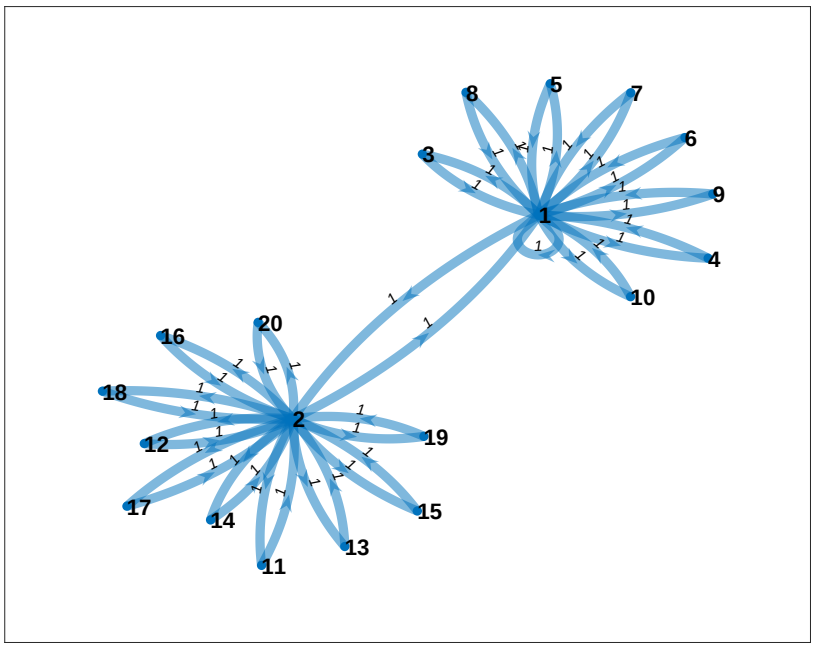


Figure 3.7: A Two Pole Network with 20 player nodes

iterations over I in a game state is generated by 2. The interesting question is whether there are optimal strategies that exhibit some cyclical (albeit stochastic) adjustments whereby the number of defecting agents (as in those agents with at least one defection within the matrix $\mathscr{D}$.

In Fig. 3.8 we can see the recursion for 20 agents exhibiting risk preferences governed an iso-elastic utility function (with constant relative risk aversion) with on a random assignment of risk aversion from a beta distribution with minimum value 0.5 and maxima of three and modal value of one, creating a bounding upper limit on risk aversion that is typical in these types of cases.

We can see the defection intensity in the network evolves quite dramatically, with period where all 20 agents have at least some defections. This least to persistent periods of high and low defections by agents. As would be anticipated by the network structure there are cascades of non-

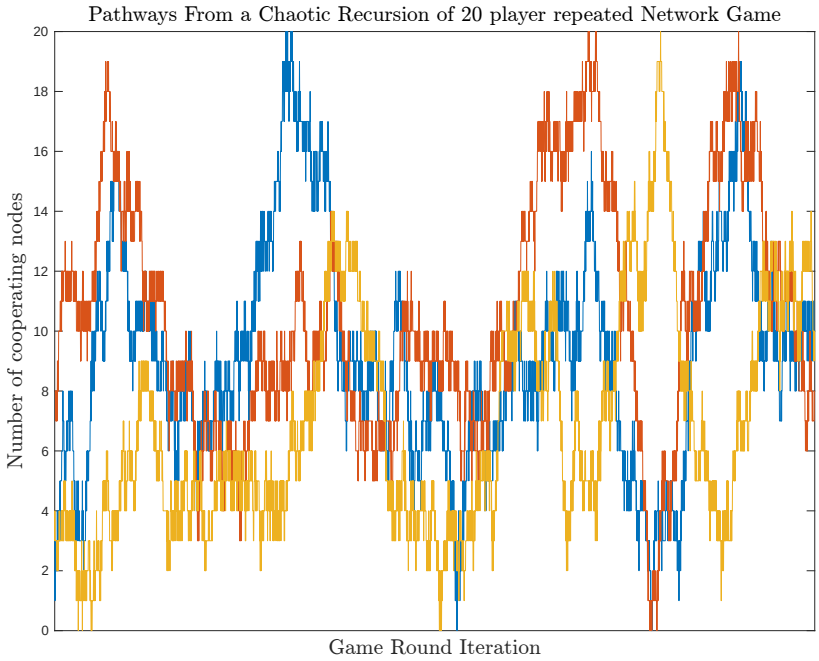


Figure 3.8: Three runs of the recursion model showing the degree of defection by agents on the node.

cooperation, but more interestingly, it is relatively easy to see that the process spends more time moving between the extremes of 0 and 20 than actually at 0 or 20 agents having at least one defecting strategy.

This result suggests that with a relatively simple network structure relatively complex time dynamics can be achieved in this type of framework.

Returning to the example that motivated this structure, we can think of intelligence agencies interpreting intelligence product and seeking validation of it. we can see that without some sort of global enforcement mechanism even trusted central nodes such as (1) and (2) will have points of defection within their strategies and it is simply a matter of time before such conditions will occur that will result in at least one defection by nodes (1) and (2). Their preferences can be skewed by imposing some reduced risk aversion and other endowments on (1) and (2), but as the game evolves there would, in this game space, normally be periods where those central

nodes will defect. Unfortunately, it is beyond the scope of this thesis to prove that in general this defection is always non-zero asymptotically. However, this approach can be viewed from an "Ellsberg paradox" perspective, where deviations from standard utility optimizing frameworks can be used to intuit strategies where trust is only driven aligned cost-benefit maximisation and is only forward looking, as in this case.

For instance Ellsberg[36] provides a framework for choice within an ambiguity game. The interpretation of this in an intelligence and conflict-management framework is then incorporated in[37] having been previously deployed in.[38] Here the general results of a model, where any ambiguity on the part of decision-maker is unintentional, can be used to develop a qualitative framework for understanding decision under uncertainty within a national security context.

Here we can see that strategic choice in a fully consistent dynamic framework, without imposing some arbitrary myopia, still results in ergodic behaviour. That is the model's discrete choice component will be conjectured to explore all routes within with space of choices, most notably within the $\mathscr{D}$ matrix. Clearly when inter-temporal defection is bounded and expected then why not adapt a more belligerent strategy? Again, the model provides a useful story telling framework. Whilst epochs of considerable defection are plausible, rational agents will be expected to spend a great deal of time within the intermediate states, during this period the welfare of agents is subjectively maximised. A full belligerent strategy, say by the

36. Daniel Ellsberg, "Risk, ambiguity, and the Savage axioms," *The quarterly journal of economics* 75, no. 4 (1961): 643–669.

37. Daniel Ellsberg, *The doomsday machine: Confessions of a nuclear war planner* (Bloomsbury Publishing USA, 2017).

38. Daniel Ellsberg, "The theory and practice of blackmail," *Lecture at the Lowell Institute, Boston, MA, March* 10 (1959).

core nodes (1) and (2) cannot achieve a better outcome and a *grim* strategy of permanent defection is not plausible as there will always be a network surplus that would be mutually beneficial at some stage — the recursion in algorithm Algorithm 1 is globally optimizing for each agent covering all possible future outcomes.

The novelty in these results is in the handling of redundancy: a key point is that the configurations of $\mathscr{D}$ expand with the factorial $N!$ of the number of agents rather than as a bounded polynomial (e.g. with N^2 or N^3). As such, fully exploring $\mathscr{D}$ is computationally difficult. A fast algorithm pre-computes samples from $\mathscr{D}$ for use in Algorithm 1 can sort self-similar outcomes as coefficients rather than compute each option individually. For instance, in the bipolar network, many defections by nodes not directly connected to each other are technically irrelevant.

3.6 Conclusion

This chapter has presented a network model that provides a counterpoint to existing approaches that are either highly abstract to ensure computational tractability, fix actor preferences, or neglect network structure. Network games of allowing for stochasticity in actor interaction and ergodicity in the sense of long-running interactions account for variability in actor interactions, forward planning from limited network visibility, and long-term structural outcomes. Aggregated effort through each actor's relative effort based on these strategies results in the production of a public good. These network games are understood in different trust contexts and network structures in public-private, private-private, and public-public actor

cooperation to address concerns in international security.

We find that as policy diffusion is less effective in networks with high node dispersion. In contrast, recent examples of offensive cyber activity show that node proximity to insecure policies can be weaponised; literal conceptions of proximity, such as computer network proximity between the intended target, and an initial target used to gain initial access to the shared network was reportedly exploited by a Russian hacker group, adapting espionage tactics to targeting insecure common infrastructure.[39] As such, this model can be adapted to real-world contexts. Furthermore, we find that in the event of multiple actors defecting, network stability is dependent on the actor's network position and optimal time in enacting the strategy. Defections may not always lead to network collapse, and multiple defections may collapse networks, without compromising the underlying system. Due to ergodicity, where actors can occupy all possible nodes in the game space, no dominant steady state is reached under long-term, variable interactions.

Our approach opens up future analytical and empirical work in contextual questions of international security, cybersecurity, and privacy. The model also allows for behavioural reasoning on issues of attribution (although not the salient theme), possible false-flag cyber operations, and deception in Chapter 4.2, where actors such as Advanced Persistent Threat groups must balance their cooperative dynamics between state sponsors as well as other groups that enable them to use espionage-supporting technologies.

39. Steven Adair, Sean Koessel, and Tom Lancaster, *The Nearest Neighbor Attack: How A Russian APT Weaponized Nearby Wi-Fi Networks for Covert Access* [in en-US], November 2024, https://www.volexity.com/blog/2024/11/22/the-nearest-neighbor-attack-how-a-russian-apt-weaponized-nearby-wi-fi-networks-for-covert-access/.

Stoachastic behaviour of actors, generating connectivity, and the ergodic nature of network structures result in no dominant steady states in network structures under actor defection. This result may be used to gauge power propagation and volatility effects. Model parametrisation can be adapted to specific networks where agents decide to trade off between individual payoffs or to continue investing in cooperation. However, our model also raises questions about the thresholds of network and system collapse under specific defection contexts, and the impact that network volatility in cyberspace as an information system may have on strategic stability.

In particular, the next chapter seeks to answer the following questions. How does cyber power propagate as a consequence of states' ability to control information flows across interdependent networks? What is the impact of cyber power dynamics on developing and gaining offensive cyber capabilities necessary for espionage? Having discussed the impact of trust dynamics on power relations, how does power projection, in turn, affect trust in networked structures? How does the development and deployment of espionage capabilities, necessary to compete, impact trust in cyberspace?

Chapter 4

Leveraging espionage networks to project cyber power

4.1 Overview

So far, trust has been introduced as a process which facilitates new information networks or 'structures', and evolves the topologies of existing structures based on individual actors' incentives to defect. How structures evolve has been a key limitation in previous treatments of international political economy, such as 'weaponised interdependence', which take a static view of power relations. This chapter develops a dynamic theory of cyber power, based on changing trust relations between state actors, and state and private actors.

The first essay uses 'weaponised interdependence' as an analytical framework for assessing how great powers use interdependent information networks to maximise their own offensive capabilities through state coercion over private actors. Limitations of this analysis, as a proof-of-concept mo-

tivating a dynamic approach, shows that static theories of cyber power are limited by omitting the context of a competing state's domestic political institutions and economic policies, and cannot address the emergence of new cyber powers and the decline of existing ones as a result of changing topologies.

The second essay applies the conceptual framework established in Chapter 2 to emphasise the role of trust in a state's relationships vis-a-vis its competitors and key private actors in the global supply chain. A state leverages relationships with private actors such as tech platforms, proxy hackers, and exploit vendors, to mount espionage campaigns on strategic competitors. As trust relationships evolve, topologies of structures change, enabling some states to better develop espionage capabilities over others. This essay addresses a limitation of weaponised interdependence, where the static treatment of structures neglects how individual actors' agency changing network topologies over time.

The third essay argues that power competitions undermine trust between information flows in cyberspace, invoking the bidirectional nature of the trust-power relation introduced in the conceptual framework. It contributes to literature on cyberspace instability by introducing a link between strategic instability and an unstable cyberspace as a result of great power cyber competition, arguing that coercion and cooperation strategies that great powers deploy to compete in cyberspace make cyberspace more unstable for all actors. In conclusion, the strategic implications of 'structural volatility' present a paradox, where volatility in security, reliability, and governability of information flows arising from great power competition undermines the competitor's ability to conduct espionage.

4.2 Towards a framework for analysing complex interdependence in digital espionage markets

The body of this text is based on the conference proceeding:

Datta, Ahana. 2024. 'Towards a Framework for Analysing Complex Interdependence in Digital Espionage Markets'. European Conference on Cyber Warfare and Security 23 (1): 675–82. https://doi.org/10.34190/eccws.23.1.2231.

4.2.1 Overview

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 section, 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.

4.2.2 Introduction

Cyberspace serves as a communication channel for multiple information systems. As such, national cyber power applies to cyberspace as a single domain of competition in itself, but also projects across the domains it supports. Cooperative or coercive strategies across economic domains such as global markets, payments systems and other financial systems, as well as political domains such as military and diplomatic organisations, are at least partly reliant on mobilising offensive and defensive cyber capabilities

to meet national objectives. To summarise from the conceptual framework, the extent to which a state actor is able to acquire or access, develop, deploy and maintain coercive capabilities is a structural indicator of its power. This accrued power may be applied directly back to cyberspace through overt and covert coercion, and entrenched power may be used in cyberspace or in other domains to foment cooperative relations with new public and private actors.

The public disclosure of Stuxnet and its use as a geopolitical instrument of de-escalation between the US, Israel and Iran may be credited for nascent, early theories of cyber power and state power competition in the cyber domain. While Stuxnet was far from being the first digital instrument of sabotage or espionage, as seen by the viruses and worms commonly used to deny service at scale in the 1990s and early 2000s, it served multiple purposes for security scholars as a basis for analysing digital weapons serving cross-domain purposes, their newfound promise in targeted, effective operations absent the costs of kinetic warfare, and the development of offensive capabilities as a cooperative exercise between allied states. Previous normative theories of power, such as those dependent on diverging definitions of cyberspace discussed in Chapter 2,[1] were recast simultaneously into literature on coercive elements such as cyber warfare and conflict theory

1. Daniel T. Kuehl, "From Cyberspace to Cyberpower: Defining the Problem" [in en], in *Cyberpower and National Security*, ed. Franklin D. Kramer, Stuart H. Starr, and Larry K. Wentz (University of Nebraska Press, March 2011), ISBN: 978-1-59797-933-7 978-1-59797-423-3, https://doi.org/10.2307/j.ctt1djmhj1, http://www.jstor.org/stable/10.2307/j.ctt1djmhj1; Stuart H. Starr, "Towards an Evolving Theory of Cyberpower," in *The Virtual Battlefield: Perspectives on Cyber Warfare* (IOS Press, 2009), 18–52, https://doi.org/10.3233/978-1-60750-060-5-18, https://ebooks.iospress.nl/doi/10.3233/978-1-60750-060-5-18.

on the one hand[2][3],[4] and cooperative elements, such as the governance of cyber power, on the other.

Natural comparisons arising from these cooperative and coercive elements, in addition to more public disclosures of state-backed offensive cyber campaigns on civil and military domains, as well as numerous methodologies in measuring power in other domains may have motivated the rise of cyber power indices in recent years to compare relative national cyber power. That there is no single, accepted methodology for measuring cyber power, or a universal cyber power index, may be in part due to need for greater comprehensiveness in the factors that presently make up these indices. Cyber power takes on both offensive and defensive characteristics, and indices must demonstrate that they consider all the subdomains that constitute offensive and defensive cyber capabilities at tactical, operational, and strategic levels. Attempts to measure comprehensiveness,[5] as well as revised underlying qualitative methodologies after new and significant cyber attacks, motivate new indices.

One benefit is that the relative position of a state within an index may provide an external view into the gaps in its capabilities. This may lead to greater investment in defensive technologies that benefits its societies, or into developing deterrents within or outside the cyber domain that support

2. Joseph S. Nye, *Cyber Power* (Harvard Kennedy School, Belfer Center for Science and International Affairs ..., 2010), http://pakistanhouse.net/wp-content/uploads/2016/11/Cyber-security.pdf.

3. T. Rid, *Cyber War Will Not Take Place* [in en] (Oxford, UNITED STATES: Oxford University Press, Incorporated.(Accessed, 2013).

4. D. Betz, "Cyberpower in Strategic Affairs: Neither Unthinkable nor Blessed"' [in en], Available at: *Journal of Strategic Studies* 35, no. 5 (2012): 689–711, https://doi.org/10.1080/01402390.2012.706970., https://doi.org/10.1080/01402390.2012.706970..

5. H. Cifci, *Comparison of National-Level Cybersecurity and Cyber Power Indices: A Conceptual Framework* [in en], Available at: 2022, –, https://doi.org/10.21203/rs.3.rs-2159915/v1., https://doi.org/10.21203/rs.3.rs-2159915/v1..

its offensive posture. Its position in an index may lead the state to revisit its private sector partnerships, or build new cooperative structures with allied states to benefit from cumulative capabilities. In short, gap assessments can provide progress reports for iteration. By contrast, the use of indices in presenting an accurate, dynamic, or valuable assessment of relative national cyber power is limited.

Accuracy is interpreted in two ways. First, the consistency of a state's relative cyber power with its domestic political economy, or in other words, inferring that prioritising and building offensive or defensive cyber capabilities are in line with the state's political and economic objectives. States with authoritarian political systems have different threat models to liberal democracies; a comparison in domestic surveillance capabilities or coercive levers on the domestic private sector, for example, will be weighted differently by each state according to its threat models. Second, accuracy in measurement. Measuring political power, such as economic or military power, remains highly context specific and ambiguous due to the complexity of taking into account the resulting information asymmetries and variables such as influence.[6] Indicators of investment, such as percentage of GDP spend on defence, or gross versus net asset production[7] are amongst many proposed economic metrics of political power.

A dynamic assessment of cyber power must also represent the benefits and constraints from domestic and foreign public-private and public-public

6. Herbert A. Simon, "Notes on the Observation and Measurement of Political Power," *The Journal of Politics* 15, no. 4 (November 1953): 500–516, ISSN: 0022-3816, https://doi.org/10.2307/2126538, https://www.journals.uchicago.edu/doi/abs/10.2307/2126538.

7. Michael Beckley, "The Power of Nations: Measuring What Matters," *International Security* 43, no. 2 (November 1, 2018): 7–44, ISSN: 0162-2889, accessed May 1, 2024, https://doi.org/10.1162/isec_a_00328, https://doi.org/10.1162/isec_a_00328.

relationships. Some cyber power indices are updated yearly presumably to capture these dynamics, but are not indicative of which relationships are expected to evolve in the long-term or more quickly. Evolution may be more subtle or targeted than the metrics present. Interdependence, in particular, has never been named as an explicit limitation or factor in considering the relative nature of these relationships, and despite their frequent updates, while they may take responsive capability in-situ into account, they do not evaluate the development of cooperative and coercive levers, such as the quality or level of control over responses to overt and covert strategies and events.[8]

Finally, the value of these indices has little impact on mobilising cyber power.[9] For policymakers in particular, investment in cyber capability remains siloed in military and civilian domains. Metrics for effective cybersecurity also differ with context. Emerging and middle powers have vastly different reliance on ICTs in critical national infrastructure and, as such, defensive postures that have highly varied costs. Most indices cannot take such complexities into account. Similarly, political considerations such as involving civil society in national cyber strategies differ in substance, as does the level of state control in obtaining private sector capabilities at cost. Lack of consideration of the underlying economic ecosystem devalues such indices.

8. Jeffrey Hart, "Three Approaches to the Measurement of Power in International Relations," *International Organization* 30, no. 2 (April 1976): 289–305, ISSN: 1531-5088, 0020-8183, https://doi.org/10.1017/S0020818300018282, https://www.cambridge.org/core/journals/international-organization/article/abs/three-approaches-to-the-measurement-of-power-in-international-relations/F4D580931E934A85351E9406832D354C.

9. N. Inkster, "Measuring Military Cyber Power"' [in en], Available at: *Survival* 59, no. 4 (2017): 27–34, https://doi.org/10.1080/00396338.2017.1349770., https://doi.org/10.1080/00396338.2017.1349770..

Even reputable indices, such as the Belfer Centre index[10] or a more comprehensive framework by the International Institute for Strategic Studies [11] suffer from these limitations. Their methodologies rely on qualitative frameworks, with questions such as whether a nation adopts 'a whole of society' approach in its cyber governance, or when national documents first mention 'cyber' as an indicator of maturity. Scoring based on these questions omits specific considerations, such as the level of information asymmetries in the political economies of states like China and Russia, or North Korea's disproportionate offensive cyber power and its aim at foreign civilian systems as a compensating mechanism for its economic status. 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. Comprehensiveness against a standardised framework of cyber power trades off the limited observability of empirical data, attribution, and national perspective.

On the other hand, cyber power theorisation has evolved significantly since Stuxnet[12][13],[14] with the identification and classification of Advanced Persistent Threat actor groups evaluated for their TTPs and distinctive styles, as well as their association with nation-states, supplementing cyber

10. J. Voo, *National Cyber Power Index 2020: Methodology and Analytical Considerations'* [in en], technical report, China Cyber Policy Initiative Reports [Preprint]. Available at: (2020), https://dash.harvard.edu/handle/1/37372389.

11. https://www.iiss.org/research-paper/2023/09/cyber-capabilities-national-power-volume-2/

12. F.D. Kramer, S.H. Starr, and L.K. Wentz, eds., *Cyberpower and National Security* [in en], Available at: 2011, https://doi.org/10.2307/j.ctt1djmhj1., https://doi.org/10.2307/j.ctt1djmhj1..

13. E Lincoln Bonner Iii, "Cyber Power in 21st-Century Joint Warfare," 2014,

14. Ralph Langner, "Cyber Power: An Emerging Factor in National and International Security," *Horizons: Journal of International Relations and Sustainable Development*, no. 8 (2016): 206–218, ISSN: 2406-0402, accessed October 20, 2023, JSTOR: 48573698, https://www.jstor.org/stable/48573698.

power. Relevant to this chapter, the 'vertical' nature of public-private relations and state coercion in these vertical relations is an established idea in cyber power analysis.[15] In recent years, more dynamic theories of relative power are gaining traction, in part, taking the equivalent lessons from economic statecraft and interdependent systems. The Russian state's evolving capability, for example, seen through iterations of publicly attributed cyber operations, within a conception of the state as an actor within a dynamic environment with access to vulnerabilities, and capabilities to mature them, attempts to capture some complexity of domestic 'horizontal' relations.[16] Other structural analyses compare European Union structure of federalised cooperative power in the form of centralised policies, standards, and regulation, as opposed to decentralised offensive power of member states,[17] and would benefit further from analysing the tension between incrementally different domestic political economies on mobilising offensive cyber power, as seen with the use of the Pegasus spyware by member states on their domestic political opponents.

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

15. Alexander Klimburg, "Mobilising Cyber Power," *Survival* 53, no. 1 (February 1, 2011): 41–60, ISSN: 0039-6338, accessed October 20, 2023, https://doi.org/10.1080/00396338.2011.555595, https://doi.org/10.1080/00396338.2011.555595.

16. J.K. Mattila, "A Model for State Cyber Power: Case Study of Russian Behaviour"' [in en], Available at: *European Conference on Cyber Warfare and Security* 21, no. 1 (2022): 188–197, https://doi.org/10.34190/eccws.21.1.207., https://doi.org/10.34190/eccws.21.1.207..

17. M. Dunn Cavelty, "Europe's cyber-power"' [in en], Available at: *European Politics and Society* 19, no. 3 (2018): 304–320, https://doi.org/10.1080/23745118.2018.1430718., https://doi.org/10.1080/23745118.2018.1430718..

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, Newman, and Oatley[18].[19] 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[20] and Maurer[21] use actor-network models to appraise coercive power in mercenary hackers, Harvey and Moore[22] analyse Meta's statecraft-like private power.

18. Farrell and Newman, "Of Privacy and Power: The Transatlantic Struggle over Freedom and Security'."

19. Oatley, "Toward a political economy of complex interdependence'."

20. Betz, "Cyberpower in Strategic Affairs: Neither Unthinkable nor Blessed'."

21. Maurer, *Cyber Mercenaries*.

22. C.J. Harvey and C.L. Moore, "Cyber statecraft by net states: the case of Meta, 2016–2021'" [in en], Available at: *Journal of Cyber Policy* 0, no. 0 (2023): 1–21, https://doi.org/10.1080/23738871.2023.2249008., https://doi.org/10.1080/23738871.2023.2249008..

4.2.3 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".[23] Natural questions arise: who does it, why, and how? Some perspectives deal mainly with intelligence operations conducted by states for political objectives,[24] 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 espi-

23. Rid, *Cyber War Will Not Take Place*.

24. J.R. Lindsay, "Cyber Espionage"' [in en], in *The Oxford Handbook of Cyber Security*, ed. P. Cornish, Available at: (Oxford University Press, 2021), 0, https://doi.org/10.1093/oxfordhb/9780198800682.013.12., https://doi.org/10.1093/oxfordhb/9780198800682.013.12..

onage. 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";[25] 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

25. M. Ben-Gad and A. Finkelstein, "On Intelligence Equities"' [in en], *Draft* 0, no. 9.1 (2022).

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,[26] 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.[27] 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.

4.2.4 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 ini-

26. I. Levy, *Equities Process'* [in en], Available at, 2018, https://www.ncsc.gov.uk/blog-post/equities-process.

27. Kot and Brian, *Why Does the Global Spyware Industry Continue to Thrive? Trends, Explanations, and Responses, Carnegie Endowment for International Peace*.

tially 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[28] adapt weaponised complex interdependence to privacy, surveillance, and its governance. Segal[29] applies weaponised interdependence to the 5G rivalry between the US and China,

28. H. Farrell and A.L. Newman, "Weaponized Interdependence: How Global Economic Networks Shape State Coercion"' [in en], Available at: *International Security* 44, no. 1 (2019): 42–79, https://doi.org/10.1162/isec_a_00351., https://doi.org/10.1162/isec_a_00351..

29. Segal, *Huawei, 5G, and Weaponized Interdependence'*.

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[30] 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',[31] 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.[32] Each actor interacts with another within its

30. Tusikov, "Internet Platforms Weaponizing Chokepoints."

31. Adner, "Ecosystem as Structure: An Actionable Construct for Strategy'."

32. Crofton Black and Omer Benjakob, "How a Secretive Swiss Dealer Is Enabling Israeli Spy Firms" [in en], *Haaretz*, https://www.haaretz.com/israel-news/security-aviation/2023-05-14/ty-article-magazine/.highlight/global-surveillance-the-secretive-swiss-dealer-enabling-israeli-spy-firms/00000188-0005-dc7e-a3fe-22cdf2900000.

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 Shwartz provides a look into exploit vendor actors and the wider industry.[33] 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

33. Maor Shwartz, *The boom, the bust and the adjust* [in en], June 2023, https://medium.com/@maor_s/the-boom-the-bust-and-the-adjust-ea443a120c6.

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[34] 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 cor-

34. D. Cary and K. Del Rosso, *Sleight of hand: How China weaponizes software vulnerabilities'* [in en], Atlantic Council, 6 September. Available at: 2023, https://www.atlanticcouncil.org/in-depth-research-reports/report/sleight-of-hand-how-china-weaponizes-software-vulnerability/.

roborated 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.

4.2.5 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: ide-

ological 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[35] 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

35. Robert Sheldon and Joe McReynolds, "Civil-Military Integration and Cybersecurity: A Study of Chinese Information Warfare Militias," in *China and Cybersecurity: Espionage, Strategy, and Politics in the Digital Domain*, ed. Jon R. Lindsay, Tai Ming Cheung, and Derek S. Reveron (Oxford University Press, May 1, 2015), 0, ISBN: 978-0-19-020126-5, accessed July 17, 2023, https://doi.org/10.1093/acprof:oso/9780190201265.003.0008, https://doi.org/10.1093/acprof:oso/9780190201265.003.0008.

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. 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.[36]

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

36. Bernsen, *Same Same, but Different, Margin Research*.

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.

4.2.6 Conclusion: Dynamic theories of cyber power

Any strategic leverage derived from digital espionage is not homogenous.[37] 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

37. Devanny, Martin, and Stevens, "On the strategic consequences of digital espionage."

security objectives; a recent example highlights the difficulty in establishing espionage norms between Russia, China and the West due to conflicts in this juxtaposition.[38] 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. In this regard, future measures of predictive cyber power may be most useful when they are measured in specific instances, such as offensive or defensive capabilities of nation-states at scale given their public-private relationships, relative to a comparator state's posture, rather than producing a universal set of qualitative measures that may overlook a state's specific political and economic contexts.

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,

38. Harnisch and Zettl-Schabath, "Secrecy and Norm Emergence in Cyber-Space. The US, China and Russia Interaction and the Governance of Cyber-Espionage."

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. The network structure of the Internet is shifting towards the Pacific due to increased private power in tech platforms serving the BRICS nations.[39] A plausible shift in the international 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.

39. Tusikov, "Internet Platforms Weaponizing Chokepoints."

4.3 Trust networks and cyber power

4.3.1 Overview

The previous section argued for a theory of cyber power that considers network dynamics. Cyber power theory, in extant literature, has neglected structural effects, such as how states leverage their domestic political economy in shaping intent and deploying offensive capabilities. 'Weaponised interdependence' was applied as an analytic framework for showing how the US and China stockpile vulnerabilities to develop offensive cyber capability and conduct espionage. This proof of concept outlined a basis for constructing a theory of dynamic cyber power on static networks. First, extant index-based approaches to measuring cyber power are limited by analysts' beliefs in constructing methodological frameworks to assess cyber power competitions. Second, cyber power is accrued as a result of individual actors' agency, but is also a structural consequence of nation-states' ability to leverage power in political and economic information systems. Third, given the situation of espionage within statecraft, espionage forms a cogent basis to theorise national cyber power and reason about strategic intent in competition. Fourth, that private actors are subject to state coercion, and successful coercive power is required for developing offensive cyber capabilities. However, a key limitation of weaponised interdependence, that Chapters 2 and 3 address, is its basis in static networks.

In this section, the proof-of-concept is expanded by applying the conceptual framework to state-private relationships, using the results of collaboration-defection network games. In particular, cyber, political, and private infor-

mation networks are connected through the supply-demand for offensive cyber capabilities; cyber power is reliant on leveraging political and private power. We consider the national cyber power of nation-states in their accessibility to cyber capabilities vis-a-vis relationships with private actors. Open, closed, and non-markets facilitate the circulation of knowledge about vulnerabilities, commodified exploits, and commercial offensive capabilities. States develop relationships with Advanced Persistent Threat (APT) groups, with whom they must cooperate to secure strategic interests by mounting sophisticated intelligence-gathering campaigns. APT groups concurrently operate in ecosystems of their own, where they share knowledge and infrastructure and compete for technological advantage with rival groups. Addressing a key limitation of cyber power theories in states' mobilisation of cyber power, we consider the operational properties of espionage campaigns, and states' proximity to APT groups in accessing offensive cyber capabilities, to develop cyber power and reason about strategic intent. Espionage campaigns are considered on a case-by-case basis in literature, as the TTPs and intent of each campaign vary. The contributions in this section may help analysts develop heuristics for assessing the adversary's offensive cyber posture through their relationships with APTs. The structural consequences, however, indicate that given the lack of an enduring steady state based on the cooperation and defection between state actors and private actors, such as APTs, offensive cyber activity will intensify.

4.3.2 Introduction

Trust relationships between actors in cyberspace enable public and private actors to exploit information flows to meet their political or economic objectives. However, the reliance of state actors on private actors, such as commercial security companies, exploit vendors, APT groups, and other third-party hacker groups, has led to a diffusion of security governance, reducing the state's monopoly on the legitimate use of 'force'.[40] Strategic intent of the private actor, as seeking profit, or achieving political objectives backed by the state, becomes more complex to distinguish with dual-use offensive capabilities for cybercrime or espionage purposes.

Multi-theoretic perspectives of political power position agency-centric conceptions[41] against structural conceptions;[42] in particular the role of the state and its institutions in developing national power, and how domestic institutions control the state's interactions with private actors, and as a result, capability-building for power projection or national security. Taxonomies bridging the tension in these methodological differences identify

40. Elke Krahmann, "Private Military and Security Companies, Territoriality and the Transformation of Western Security Governance" [in en], in *The Diffusion of Power in Global Governance: International Political Economy Meets Foucault*, ed. Stefano Guzzini and Iver B. Neumann (London: Palgrave Macmillan UK, 2012), 38–70, ISBN: 978-1-137-28355-9, accessed October 29, 2024, https://doi.org/10.1057/9781137283559_2, https://doi.org/10.1057/9781137283559_2; Herbert S. Lin, "Offensive Cyber Operations and the Use of Force," *Journal of National Security Law & Policy* 4 (2010): 63, https://heinonline.org/HOL/Page?handle=hein.journals/jnatselp4&id=65&div=&collection=.

41. David A. Baldwin, "Interdependence and power: a conceptual analysis," *International Organization* 34 (October 1980): 471–506, ISSN: 1531-5088, 0020-8183, https://doi.org/10.1017/S0020818300018828.

42. Stefano Guzzini, "Structural power: the limits of neorealist power analysis," *International Organization* 47, no. 3 (1993): 443–478, https://doi.org/10.1017/S0020818300028022.

the potential for a pluralist conception of power[43] that reflects real-world scenarios[44] of using both cooperation and coercion as power competition strategies.

A combination of agent and structural views provisions a theory of cyber power that situates actor agency in the bounds of a network structure. In particular, measures of cyber power, such as national cyber power indices, can draw from this pluralist idea; to the extent that cyber capabilities and cross-domain competition strategies help states in accruing national cyber power, economic and political factors that constrain the development of offensive cyber capabilities in lieu of developing defensive capabilities,[45] can provide a more accurate account of strategic interests in cyberspace.

Explicit links must be made between regional cooperation, its impact on great power competition, and the mobilisation of cyber power as cause and effect, in bipolar political and economic power domains. China's rapid mobilisation of space and military capabilities in competition with the US has belied expectations that its economic espionage may not translate into strategic advantage by establishing itself as a great power, beyond creating its own political and economic spheres of influence to threatening US al-

43. Michael Barnett and Raymond Duvall, "Power in International Politics," Publisher: [MIT Press, University of Wisconsin Press, Cambridge University Press, International Organization Foundation], *International Organization* 59, no. 1 (2005): 39–75, ISSN: 0020-8183, https://www.jstor.org/stable/3877878.

44. David A. Baldwin, "Power Analysis and World Politics: New Trends versus Old Tendencies" [in en], *World Politics* 31, no. 2 (January 1979): 161–194, ISSN: 1086-3338, 0043-8871, accessed October 30, 2024, https://doi.org/10.2307/2009941, https://www.cambridge.org/core/journals/world-politics/article/power-analysis-and-world-politics-new-trends-versus-old-tendencies/7B639F6FA5AA7F763D183E1626D91CBB.

45. Beckley, "The Power of Nations."

liances.[46] The role of cyberspace in developing and breaking cross-domain interdependence between great and rising powers in the international system is crucial.

As such, the focus of this section is on China-attributed APT groups, and the illustration of a complex ecosystem of APT groups and relationships with their state sponsors. A key limitation of this analysis is in empirically validating the application of the framework due to the varied, inconsistent, and opaque nature of APT data in public and state intelligence information domains. Nevertheless, the reasoning presented here may assist intelligence analysts in combining methodologies such as alternative competing hypotheses with the trust framework to construct models of adversarial states and their sponsorship of APTs to develop defence policies.

The central question raised in this section is what can the operational characteristics of espionage campaigns reveal about the relationship between attributed APT groups and their state sponsors? Despite developing and deploying malware of relative sophistication to maintain persistent access to target networks, APT groups must still rely on common tooling and infrastructure to conduct operations. The costs of fully proprietary technology may both be too high as well as undermine accessing a target that uses common infrastructure to defend itself. The resulting interdependence at the technological level, as well as competition with other APT groups, may guide APT behaviour. In particular, states overlooking their

46. Jennifer Lind, "Back to Bipolarity: How China's Rise Transformed the Balance of Power," _eprint: https://direct.mit.edu/isec/article-pdf/49/2/7/2479270/isec_a_00494.pdf, *International Security* 49, no. 2 (October 2024): 7–55, ISSN: 0162-2889, https://doi.org/10.1162/isec_a_00494, https://doi.org/10.1162/isec%5C_a%5C_00494.

APT groups' usage of offensive capabilities for profit may indicate challenges and detail the state's strategic priority as well as power mobilisation challenges.

First, an overview of the transformation of supply-demand relationships between cyberspace actors for offensive capabilities and knowledge of vulnerabilities discusses how the offensive cyber industry has consolidated into competing commercial entities over time. Commercial entities, by virtue of operating in a market or market-like information system, are subject to state coercion through legal instruments such as export control. APT groups, who may not always operate in market-based systems, can evade export control and still use the underlying offensive capabilities. Operation Triangulation serves as a motivating example to illustrate the dynamics. We conclude with a discussion of the Chinese APT ecosystem, and how analysts may reason about state resources and corresponding cyber power thereon.

4.3.3 Supply-demand of offensive cyber capabilities

In commercial exploit markets, unregulated or non-commercial markets and non-markets for vulnerability sharing,[47] private contractor ecosystems offer products and services in the commercial domain[48], as well as circulating the knowledge of vulnerabilities and exploits in less systematised domains, such as the 'underground' of access-restricted Internet forums and the Dark-

47. Ali Ahmed, Amit Deokar, and Ho Cheung Brian Lee, "Vulnerability disclosure mechanisms: A synthesis and framework for market-based and non-market-based disclosures," *Decision Support Systems* 148 (September 2021): 113586, ISSN: 0167-9236, https://doi.org/10.1016/j.dss.2021.113586, https://www.sciencedirect.com/science/article/pii/S0167923621000968.

48. Vendor conferences such as ISS World, where commercial actors such as NSO Group serve as conference sponsors, allow commercial market access and vendor ecosystems more widely to security and defence contractors and personnel globally.

Web to develop so-called nation-state capabilities.[49] A key difference in the incentives of researchers who discover vulnerabilities, and commercial capability vendors, is in their conceptions of 'profit'; while independent security researchers seek reputational gains that attract sponsorship from commercial, political, and public actors,[50] commercial actors leverage the vulnerabilities discovered by security researchers to attract public actors, often with overlapping client bases between allied and competing states alike.

The network structure of public actor ecosystems enables and constrains access to capabilities through governance diffusion. In the EU's federated structure, institutions have sought to sanction the NSO group in its deployment of the Pegasus suite on civil society actors, but political actors of its member states, such as in Poland, Hungary, and Spain, have reportedly consumed Pegasus for political espionage. Export control laws and NSO group's corporate policies have disabled access to the so-called competition 'axis' of nation-states such as China, Russia, the US, and Iran, while rising, middle, and non-aligned powers in African, Gulf, European, and Asian countries have deployed Pegasus as a surveillance tool for domestic political interests.[51]

Network structures and incentives of private actors in offensive cyber ecosystems impact strategic competition between states. In particular,

49. Zhuge Jianwei et al., "Investigating the Chinese Online Underground Economy," in *China and Cybersecurity: Espionage, Strategy, and Politics in the Digital Domain*, ed. Jon R. Lindsay, Tai Ming Cheung, and Derek S. Reveron (Oxford University Press, May 2015), 0, ISBN: 978-0-19-020126-5, https://doi.org/10.1093/acprof:oso/9780190201265.003.0004, https://doi.org/10.1093/acprof:oso/9780190201265.003.0004.

50. Katie Moussouris and Michael Siegel, "The Wolves of Vuln Street:" [in en] (2015).

51. Ronald J. Deibert, "Subversion Inc: The Age of Private Espionage," Publisher: Johns Hopkins University Press, *Journal of Democracy* 33, no. 2 (2022): 28–44, ISSN: 1086-3214, accessed October 30, 2024, https://muse.jhu.edu/pub/1/article/852743.

APT groups vary between using their offensive capabilities for cybercrime and sabotage-type campaigns and espionage in interests of their state sponsors,[52] which undermines strategic intent analyses. A decade ago, highly-priced exploits on the closed market depreciating in value as they entered the open market, due to patches being issued rapidly once made public (See 4.1, original source[53]). Vendors have adjusted to increasing public actor demand, costs of finding 0days imposed from improved cybersecurity, and a consolidation of commercial actors, which has reduced competition to a few commercial actors with the economic value to dominate in their supply chains.[54] Disparate groups of offensive security researchers evolved into 'clearing houses', centralising the supply of vulnerability research to exploit vendors.[55] Additionally, while price listing on closed markets has increased significantly due to market information asymmetries,[56] the changing market share of mass-market software, such as mobile operating systems, have changed the pricing mechanisms of commercial spyware. The Pegasus suite underwent at least 3 iterations into its final zero-click zero-day payload delivery mechanism, as the underlying malware evolved to overcome patches

52. Vlad Stolyarov and Dan Black, *Virus Bulletin :: Cybercrime turned cyber espionage: the many faces of the RomCom group*, accessed October 30, 2024, https://www.virusbulletin.com/conference/vb2024/abstracts/cybercrime-turned-cyber-espionage-many-faces-romcom-group/.

53. Houghton, J. and Siegel, M., "Advancing Cybersecurity Using System Dynamics Simulation Modeling for Analysing and Disrupting Cybercrime Ecosystem and Vulnerability Markets" [in en], Interdisciplinary Consortium for Improving Critical Infrastructure Cybersecurity (MIT Sloan School of Management, 2014).

54. Lillian Ablon and Martin Libicki, "Hacker's Bazaar: The Markets for Cybercrime Tools and Stolen Data," *Defense Counsel Journal* 82 (2015): 143, https://heinonline.org/HOL/Page?handle=hein.journals/defcon82&id=143&div=&collection=; Allen D. Householder et al., "Historical Analysis of Exploit Availability Timelines" [in en] (2020), https://www.usenix.org/conference/cset20/presentation/householder.

55. Maor Shwartz, "The Boom, the Bust and the Adjust," Medium, June 20, 2023, https://medium.com/@maor_s/the-boom-the-bust-and-the-adjust-ea443a120c6.

56. Matthias Dellago, Daniel W Woods, and Andrew C Simpson, "Characterising 0-Day Exploit Brokers" [in en], in *21st Workshop on the Economics of Information Security* (June 2022).

in iOS, and pricing, which started at $500k, now varies based on the number of target devices and end-to-end services.

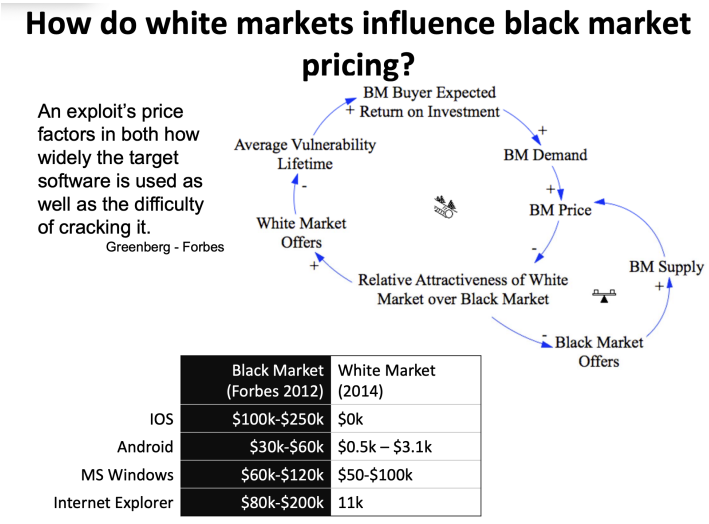


Figure 4.1: Exposure of undisclosed vulnerabilities to the open market reduce attractiveness and pricing, reproduced from (Houghton, Siegel, 2014)

Furthermore, private actors such as technology platforms, have developed internal security capabilities to rival intelligence agencies. Google Threat Analysis group, Meta and Apple Security teams partner with public actors, such as law enforcement, and private threat intelligence groups to neutralise and disclose espionage campaigns.[57] This has led some APT groups to target threat intelligence teams to prevent disclosure or to gain access to their forensic capabilities.[58] Additionally, denial of service campaigns run by private threat intelligence teams clash with law enforcement and state-controlled campaigns, where covert counterespionage and counterterrorism campaigns allegedly conflict with disclosure efforts as well as

57. *Buying Spying: How the commercial surveillance industry works and what can be done about it* [in en-us], February 2024, See for example, https://blog.google/threat-analysis-group/commercial-surveillance-vendors-google-tag-report/.

58. Clement Lecigne and Maddie Stone, *Active North Korean campaign targeting security researchers*, 2023, https://blog.google/threat-analysis-group/active-north-korean-campaign-targeting-security-researchers/.

detection campaigns mounted by private threat intelligence researchers, resulting in sinkholing legitimate traffic, for example.[59]

Technology platforms also run bug bounty programs, where researchers can disclose 0-day vulnerabilities to the platform, which are made public after a period of embargo when the platform can issue a patch. While researchers can make a greater profit keeping this knowledge underground, or selling it to a state actor, building trust relationships with platforms improve the researcher's reputation. However, the bounties paid out to the individual researchers are a small fraction of the value of the vulnerability; in 2022, over 30 0-days, each valued at approximately $1m, were reported to Apple[60]. Turnaround time of the remediation of vulnerabilities[61] creates an exposure window for the exploit development. Apple pledged $10m at mitigating the impact of spyware like Pegasus on civil society, however, operating profit from the number of licences sold by NSO group remains confidential. Disclosure changes pricing in the exploit market, as well as in developing a vulnerability equity, which may in turn lead the state actor to apply coercive levers on the platform to prevent patching.

The design and development of exploit tools can indicate the operational nature of the espionage campaign, as well as its success. Volumes of exfiltrated data depends on the persistence of malware in the target device, as well as the provisioning, uptime, and accessibility of storage in-

59. Michael Coppola, *Google: Stop Burning Counterterrorism Operations* [in en], June 2024, https://poppopret.org/2024/06/24/google-stop-burning-counterterrorism-operations/.

60. See 0-day sources compiled by Google's Project Zero: https://docs.google.com/spreadsheets/d/1lkNJ0uQwbeC1ZTRrxdtuPLCIl7mlUreoKfSIgajnSyY/edit?gid=694054923#gid=694054923

61. Yaman Roumani, "Patching zero-day vulnerabilities: an empirical analysis," *Journal of Cybersecurity* 7, no. 1 (January 2021): tyab023, ISSN: 2057-2085, https://doi.org/10.1093/cybsec/tyab023, https://doi.org/10.1093/cybsec/tyab023.

frastructure between multiple actors such as the APT and state sponsors. Espionage campaigns are generally characterised by a chain of events: initial access to a target, usually through compromising an end-user account by means of phishing or delivering exploit payload through a malware; establishing persistent access, such as through backdoors at various stages of the software supply chain; lateral movement across the network through privilege escalation and network surveillance; data exfiltration using off-the-shelf extraction tools; and cleanup, which may require root privileges to evade detection or modify logs.

Maintaining persistent access over long campaigns can impose operational costs from system administration and adapting malware to persist despite patching. The length of an espionage campaign varies from a one-time compromise to dump a database, to long-term access to endpoints, where political and economic developments motivate strategic intent.[62] Long-term access indicates the capabilities of the attacker, and the resources to adapt to platform defences. APT groups adapt early instances of malware into malware families that can provide target-specific capabilities at cost, and malware families are deployed by multiple APTs and over multiple campaigns once detection and disclosure provides the opportunity to modify the malware further.

4.3.4 Mobilising cyber power: exploiting the exploit markets

How can the operational characteristics of an espionage campaign indicate the relationship between a state actor and APT groups, and by extension,

62. Smeets, "A matter of time: On the transitory nature of cyberweapons'."

the strategic intent behind an espionage campaign? In considering the link between strategic intent and national cyber power, consider the following questions. What is the intent behind an espionage campaign, and what strategic objective is met through the campaign? In other words, does espionage work? On the other hand, how was the campaign mounted, and how was the data, exfiltrated from the target, assessed and actioned? Does the coercer possess capabilities to infiltrate the target and exfiltrate data, but also to store, assess, and convert the intelligence into strategic advantage? As such, mobilising cyber power is necessary to enact intent. To determine intent, analysts must ascertain the capacity of the state to mobilise cyber power. Espionage does not end at spying.

Supply-demand of offensive cyber capabilities highlight the challenges of identifying APT activity. APT groups must share infrastructure provided by technology platforms for staging exploits and setting up repositories for storing the target's exfiltrated data, as well as common tooling developed by offence-defence researchers, such as data exfiltrators and malware families to reduce operational expenditure. The distinction in exploiting 'dual-use' technologies can refer to both the defensive infrastructure of the target, such as access management[63] and monitoring tools, but also the use of offensive tooling for dual purposes, where malware is used for criminal as well as espionage activities. The profit-seeking preferences of the threat actor may reveal their relationship with the state sponsor; for example the nature of sponsorship that contracts the APT into delivering exfiltrated data, or the necessary offensive capability, indicates the sponsor's internal

63. UK National Cyber Security Centre, *SVR cyber actors adapt tactics for initial cloud access* [in en], https://www.ncsc.gov.uk/news/svr-cyber-actors-adapt-tactics-for-initial-cloud-access.

capabilities; the challenges of overlapping personnel and tooling between state actors and APTs are subject to internal compliance and personnel retention issues, leading to dual-use crimeware.

The tactics, techniques, and procedures (TTPs) of APT groups can reveal structural advantages and disadvantages in a state's mobilisation of cyber power. Information flows across APT groups and security researchers in the offensive cyber ecosystem are networked through the shared knowledge of exploits, shared staging infrastructure, used to deploy malware and store stolen data, and shared tooling, from market or non-market sources. On the other hand, to maintain technological advantage and secure sponsorship, APT groups must also influence cultural perspectives of rival groups, in selective and sparse usage of common tools, such as penetration testing tooling, to avoid being perceived as not technologically capable. Unlike commercial actors, who are subject to export control, APT groups share and develop malware through non-market networks, which might eventually be consumed by the commercial actor.

The network proximity, or 'privateness' of APT groups with their state sponsors can conflict with interdependence with other APT groups, with whom they share infrastructure or personnel, due to several factors. 'Tightness', close coupling, and 'privateness' are interchangeable phrases for how states allocate resources, personnel, financial, or technological, into APT sponsorship. The level of privateness varies between nation-states, such as the Chinese model, where alleged looseness enables plausible deniability, is in contrast with Iran, where close coupling between the executive state actor and intelligence actors enables strategic priorities to be communicated with less ambiguity.

First, the development of capabilities is based on vulnerabilities in the underlying software supply chains. Competition to develop these capabilities at cost conflicts with the advantage defenders have in fingerprinting and attributing the attacker. Where APTs are closely coupled with state sponsors, they may be less incentivised to deploy evasive methodologies in the design of malware, as reprisals from the target, such as economic sanctions, are less likely to harm personnel. On the other hand, persistent engagement such as long-term access becomes more expensive with detection and attribution. Second, the comprised personnel in APTs vary from wholly state-led groups, with intelligence or military leading campaigns, to hybrid models and non-state, private groups, whose criminal activities may be overlooked by state sponsors in exchange for sharing exfiltrated data.

Third, the alignment of the various actors within the state responsible for domestic and international security also vary; state actors between competing institutions, agencies, ministries, and military units consume offensive capabilities differently, ranging from procuring exploits to fully outsourcing the campaign and purchasing stolen data. While some state actors may have the resources to run espionage campaigns at a state-level, using procured exploits, others meet their objectives from moving deployment and exfiltration capabilities to third parties. The interplay between government and military leaders who have links with private contractor at governance and executive levels determine the nature of sponsorship. Fourth, less closely coupled APTs may suffer conflicts with strategic intent of the state sponsor when its complex ecosystem of APTs and private contractors misinterpret their sponsors' intent and actors in the state must expend resources to differentiate between contractor errors and false flags.

Examples of publicly attributed espionage campaigns illustrate the dependence of APT groups on state sponsors, and the resulting ability of the state to mobilise cyber power, given interdependence in deployment, detection, and evasive design of malware payloads.[64]

Operation Triangulation

Operation Triangulation serves as a motivating example in identifying the dynamics of technological interdependence between APTs and tech platforms with state sponsor relationships. In June 2023, the threat intelligence group at Kaspersky announced the discovery of the malware TriangleDB in certain versions of Apple iOS.[65] The malware chained four 0-day vulnerabilities into an exploit payload, delivered to iPhones through an iMessage invisible to the user. The intelligence-gathering campaign was reportedly conducted over four years, as ascertained from malware fingerprints. TriangleDB chained vulnerabilities from low-level kernel to high-level font parsers[66], exploiting Apple processor firmware through iMessage and the Safari browser to connect to a command-and-control malware server, gaining root privileges, and delivered the payload to specific targets, including Kaspersky researchers. The malware blocked some devices from upgrading the operating system and applying the patch issued the

64. Jonathan Haslam, *Near and Distant Neighbors: A New History of Soviet Intelligence* (Macmillan, 2015), Historian Jonathan Haslam describes a similar framework for identifying US HUMINT sources, devised by KGB counterintelligence officer Yuri Totrov in the Cold War to compensate for the Soviet technology deficit. Totrov conducted pattern analysis of potential representatives of different American intelligence agencies to define a common set of invariants in target behaviours to determine coupling, based on their lifestyles and how they were treated by American bureaucracy, to attribute personnel to their respective agencies.

65. Igor Kuznetsov, Valentin Pashkov, and Leonid Bezvershenko, *Operation Triangulation: iOS devices targeted with previously unknown malware*, technical report (Kaspersky, Inc), https://securelist.com/operation-triangulation/109842/.

66. The terminology of 'low' and 'high' level is derived from the Open Systems Interconnection model, which provides a framework for understanding information flows at different systems levels from hardware to software and application layers.

following month.

These operational steps led analysts to allude to TriangleDB as the most sophisticated technical campaign in recent years. The knowledge of the specific vulnerability in iOS kernel memory that executed the part of malware code providing root access, exfiltrating potentially all messaging data, was suspected only to be available to Apple, the intermediary processing chip provider, and, given the sophisticated chain of attack, nation-state intelligence communities. Kaspersky did not attribute the campaign, but the Russian Security Service accused Apple of partnering with the NSA to spy on government employees. The FSB sanctioned the use of Apple devices for official business; China and others followed.

Questions of technical attribution, such as whether Triangulation was an NSA campaign, an FSB false flag, or mounted by a non-state APT group that later aligned to a state sponsor, equip policymakers to construct reprisal frameworks, but can be extended into determining strategic intent behind the campaign by examining operational choices and reasoning about the attributed actor's cyber power. Would the use of proprietary tooling to store exfiltrated data, rather than the use of common platforms such as Amazon S3, have prevented detection of TriangleDB?[67] What can the choice of commercial infrastructure reveal about the APT's relationships?

Shared infrastructure provides software redundancy, where the responsibilities for infrastructure maintenance and uptime are owned by a third party. Redundancy lowers attack costs, saving APTs from expending resources to provision proprietary infrastructure for staging exploits and stor-

67. Bill Marczak, *Triangulation: Did "the NSA" fail to learn the lessons of NSO?* [In en], June 2023, https://medium.com/@billmarczak/triangulation-did-the-nsa-fail-to-learn-the-lessons-of-nso-5f36d251d02e.

ing exfiltrated data. However, the APT is exposed to vulnerabilities generated by other users of the shared infrastructure. If other actors in the network that shares infrastructure capabilities suffer leaks, tooling and vulnerability disclosures, or counterattacks, the cost imposed on the vulnerable actor is shared by the APT. In designing operations, APTs must account for these risks, and that using shared infrastructure enables detection. That despite the technological complexity of the malware itself, the APT deprioritised evasion, may point to indifference to detection after exfiltration has occurred.

Defenders may coerce the tech platform hosting APT activities, but additionally note that poor evasion may signal — intentionally or otherwise — the expectation of the APT to suffer minimal costs imposed from the defender's counterstrategies, possibly due to a close relationship with the state sponsor covering these costs. Alternative hypotheses of cost saving on infrastructure, rapid deployment and exfiltration, or being 'work-averse',[68] are weaker, given the resources invested in malware design. Two other hypotheses, first, that the use of common infrastructure provides another trusted actor access to exfiltrated data, and second, that the malware was developed by a different actor than the actor responsible for operations and providing stolen data, may be validated in future if further details are made public.

Future details, in particular, attributing TriangleDB to a class of malware families can inform policymakers in constructing models of APT-state

68. Luca Allodi, Fabio Massacci, and Julian Williams, "The Work-Averse Cyberattacker Model: Theory and Evidence from Two Million Attack Signatures" [in en], _eprint: https://onlinelibrary.wiley.com/doi/pdf/10.1111/risa.13732, *Risk Analysis* 42, no. 8 (2022): 1623–1642, ISSN: 1539-6924, https://doi.org/10.1111/risa.13732, https://onlinelibrary.wiley.com/doi/abs/10.1111/risa.13732.

relationships, as well as new APT-APT relationships. Consider the NSA-attributed Equation Group, which reportedly conducted espionage campaigns from at least 1996 until Kaspersky's public attribution in 2015.[69] With an arsenal of low-level firmware exploits, Equation Group's 'Fanny' malware, aimed at cyber-physical systems, was later discovered in the forensic examination of early versions of Stuxnet. When the Russia-attributed hacker group, Shadow Brokers, leaked malware, EternalBlue, reportedly developed by the NSA's Tailored Access Group, one of the suite tools was later repurposed into the SMB exploit that led to the WannaCry and NotPetya attacks. The use of the Duqu malware in future campaigns was tied to its use in Stuxnet by the NSA and IDF units. As such, the proliferation of exploits itself follows a supply chain, where APT groups may share malware, intentionally during an ongoing campaign, or otherwise, after disclosure helps other APTs to adapt malware families to their objectives. If fingerprints for TriangleDB appear in future malware families, detection was not a deterrent for the commissioned APT group.

Lessons from the Equation Group leak may suggest that whether Operation Triangulation was an NSA-sponsored campaign, or a false flag by the FSB used as a casus belli, export control may not hinder APT groups in contrast to commercial actors, as the underlying malware can be repurposed, and the disclosure of the campaign may not deter future campaigns. Operation Triangulation outlines the motivation for examining the resource capabilities of, and proximity to the state sponsor with the unattributed APT group behind Operation Triangulation.

69. Kaspersky Inc Global Research and Analysis Team, *Equation: The Death Star of Malware Galaxy* [in en-US], February 2015, https://securelist.com/equation-the-death-star-of-malware-galaxy/68750/.

China-attributed APT groups

The complexity of the PRC's governance structures and so-called strategic pragmatism, where political power has remained centralised within the CCP, but operational ownership of cyber campaigns is multi-layered at national, regional, and local levels, underline the challenges in constructing accurate assessments of Chinese cyber power.

Two principal challenges arise. First, of the organisation and assessment of China-attributed APT groups, which are specific to each security research group's nomenclature and classification. Second, of applying the concept of 'privateness' in establishing role-based boundaries of private and public actors in the Chinese polity.

Cybersecurity research firms leverage threat intelligence as a marketing product for selling defence infrastructure. Threat intelligence teams work towards these commercial goals by following the activities of APTs in 'threat clusters', which track behaviours of several APT groups as a cluster. Different naming conventions for APT groups are used by cybersecurity firms, where researchers use monikers such as *Typhoon, *Panda, *Bronze, Storm-*, etc to identify and assess threat from Chinese APTs. The intelligence and data reported by these threat intelligence teams are mainly limited to TTPs, in particular, identified domains for staging infrastructure and command-and-control servers, fingerprinting, and other indicators of compromise to assist potential customers in their cybersecurity, but do not address strategic changes in the initiatives of APTs, such as expansion of targets and objectives over long-running networks. Sharing threat intelligence between different cybersecurity firms is inconsistent due to market competition. The group MustangPanda was identified by

cybersecurity company CrowdStrike in 2018 as targeting US NGOs to secure China's interest in Mongolia. By 2023, ESET Research reported that MustangPanda's IoT malware was traced to European, Australian and Taiwanese targets. A new group, CeranaKeeper, was further identified by ESET to share malware with MustangPanda, targeting cloud-based SaaS in Thailand.

FireEye, another cybersecurity firm, attributes to APT41, expansive, dual-use operations on cybercrime and espionage, with targets in South East Asia, Europe, and the US. Despite FBI sanctions on some identified APT41 personnel in China and Malaysia in 2020, according to Google's Threat Analysis Group, APT41 resurfaced to mount a multifaceted campaign in 2023, deploying web shells to gain access to specific, widely used webservers, custom malware for lateral movement in a network after initial entry, and common tooling for database exfiltration. According to threat intelligence teams, APT41 is reportedly sponsored jointly by the PLA and the Ministry for State Security.

VoltTyphoon, named by Microsoft, deployed living off the land techniques on US and UK cloud infrastructure, according to the previously mentioned joint Five Eyes advisory in 2024. The same group has been identified in various other cluster names by competitors of Microsoft's Azure Defender product, such as Palo Alto networks and CrowdStrike. As such, the detection capabilities of different tech platforms and software vendors conflict with each other, resulting in no single database of common tooling or malware. For example, open data platforms such as the MITRE framework identify APTs, but common malware payloads, such as PlugX among others, which provides remote access to targets, are not a defining

attribute. Given the availability of public data reorganised based on tooling interdependence over time may help security researchers synthesise APT activity more rigorously.

The second challenge addresses the Chinese offensive cyber ecosystem, where hypotheses on APT-state proximity can help analysts assess how China mobilises its cyber power. Over 50 APT groups linked with the Chinese state, with overlapping intelligence-gathering and cybercrime-based tactics, shared tools, infrastructure, personnel, and a combination of military and civilian personnel identified in Western sanctions, show considerable network complexity. Multiple Chinese state actors operate comprehensively across an offensive cyber ecosystem, with military, civilian, and military-civilian units. A hierarchical, yet distributed set of actors involves ministries, regional government offices, and local policing units for domestic and foreign espionage. Until at least 2021, the coordination of industry, academia, and government was made possible through so-called 'fusion centres' to centralise intellectual property provisioning,[70] led by military and government personnel in official and unofficial capacities, prone to 'kingmaker' style competitions in bidding for APT work.[71] Other APT groups less proximal with the state signaled by China's national cybersecurity strategy expand activities to cover comprehensive ground, with the underlying strategic intent not immediately apparent. InsiktGroup has described the use of compromised IoTs globally in China-attributed espionage campaigns.

Given these complex networks, high levels of effort redundancy from

70. *The Chinese Communist Party's Military-Civil Fusion Policy* [in en-US], technical report (US Department of State), https://2017-2021.state.gov/military-civil-fusion/.

71. Norris, *Chinese Economic Statecraft: Commercial Actors, Grand Strategy, and State Control*.

multiple sources involved in intelligence-gathering becomes structural, which may be beneficial in establishing intelligence veracity when various public actors cooperate. However, storing, assessing, and converting volumes of intelligence and stolen data into intelligence products or replicated IP comes at high resource cost and potentially, a lack of systematisation and communicating intent between the various intelligence bodies, whose interests may be in conflict. Different sponsors within the state may base commissions to APT groups on how deeply their intelligence or military personnel and resources are within these APT groups. Considerations of acquiring, managing, and sharing exfiltrated data can further put public-private actor dynamics in perspective. For example, classification and declassification methodologies applied to resulting intelligence may vary between military and government sponsored units. While military units may consume products such as exploits or stolen data from third parties, outsourcing full or partial operational responsibilities to APT groups may not meet clearance compliance requirements and military hierarchical expectations. Evidence on declassification processes in military and government units can reveal more context of their embedding within, or outsourcing to, APT groups; tight coupling, for example, may reflect greater capacity for mobilisation and indicate a well-resourced campaign.

Addressing these challenges can provide systematic heuristics for analysts, based on historical evidence. In June 2024, reports circulated of a breach in US Internet Service Providers and telecommunications responsible[72]for legal wiretapping of persons under surveillance, attributed to Salt-

72. Robert, Sarah Krouse McMillan, Dustin Volz Aruna Viswanatha, *Exclusive | U.S. Wiretap Systems Targeted in China-Linked Hack* [in en-US], Section: Politics, October 2024, https://www.wsj.com/tech/cybersecurity/u-s-wiretap-systems-targeted-in-china-linked-hack-327fc63b.

Typhoon. To ascertain strategic intent the 2018 compromise of the CIA's communications service by the Chinese and Iranians may prove instructive. The 2018 counterintelligence campaign resulted in the expulsion and execution of informants to the CIA; China's strategic interests vis-a-vis HUMINT on US territory may indicate its interest in counterespionage about its personnel at risk. A competing hypothesis, using the example of APT1's compromise of the US Office of Personnel Management, that used a previous breach of healthcare providers to corroborate targets, may indicate that US surveilled personnel, regardless of nationality, can prove potential future targets. SaltTyphoon's long-term access to and exfiltration from compromised ISP boxes may indicate the nature of the commission, and proximity to the MSS.

Similarly, APT-41's effort intensity and long-term connectivity in developing capabilities, despite sanctions, may suggest a close relationship with state actors who may have overlooked criminal activity in exchange for capabilities. Alignment away from the state may intensify APT cybercrime in instances where close coupling is not a strategic priority of the state, or in other words, attribution and reprisals such as sanctions do not impose sufficient cost to deter. On the other hand, in some states, the personnel retention preferences of state actors may allow for cybercrime in their sponsored APTs. Typically state actors cannot satisfy the profit-seeking preferences of APT groups and may overlook dual use of espionage and cybercrime tooling, up to some threshold, where sponsorship must satisfy the state's strategic interests in exchange for utility from cybercrime.

4.3.5 Conclusion

Network interdependence reduces the operational costs of espionage campaigns when common tooling and infrastructure are deployed in dual-use operations, such as cybercrime, and when the target's defensive infrastructure is compromised at low cost to initial access. APT groups cooperate with one another to develop common infrastructure and tooling. Furthermore, trust relationships with state sponsors allow APT groups close proximity to the state and to leverage the state's resources. APT groups may increase their proximity to the state by signalling trust through the deployment of sophisticated capabilities. To mediate the conflict between their trust relations with state sponsors, as well as the trust from cooperation on shared infrastructure and tooling, APT groups must choose strategies of cooperation and defection as profit-seeking agents with advanced capability development.

Lower connectivity with the state and node proximity protect the APT group from volatile state policies, and incentivise mercenary behaviour. A state outsourcing the full exploit chain, from development, staging, deployment, and exfiltration, to a more private APT group, faces the risk of the group's defection, as the group's stochastic behaviour and high levels of dispersion reduce the coercive effects of state governance. State reliance on private actor cooperation may signal high resources but an inability to convert resources into internal capability. Absent 'patriotic' intent notable in sabotage and influence operations, APT groups must constantly balance tensions in their incentives vis-a-vis private and public actors.

As argued in Chapter 3, there is no dominant steady state in network

trust dynamics that maintains stability, and as such, offensive campaigns may only intensify. If APTs revert to proprietary staging and data storage infrastructure, they will need to afford the costs of breaking interdependence through either greater proximity with public actor networks, or deploying malware into dual-use cybercrime as a revenue stream, such as ransomware, to sustain activities. As the development of capabilities becomes more expensive, and requires more personnel specialism, APTs may successfully bargain with state sponsors to leverage dual-use, as seen in Chinese, Russian, and North Korean APTs, where APTs comprising state and private actors engage in espionage as well as cybercrime. Continued use of shared infrastructure, conversely, through attribution and disclosure, will only add to a group's notoriety, and the reputational gains in some offensive networks this brings may offset against the loss from detection and burned capabilities.

The organisation of the state actors' intelligence capabilities in great powers, and the relationship with their APT groups, is reflected in state-state relationships. Cooperation in intelligence-sharing and capability development may help allied states improve their national cyber power collectively. The different intelligence agencies within a state's apparatus buy, sell, and share offensive capabilities for achieving the objective of their security alliances. APT groups may or may not have visibility of the 'product', which is the post-analysis report of exfiltration, purchased by one state actor being circulated between other state actors inside a state's intelligence community, but also between allied agencies. Competition for resources, such as budgets and leadership access, between the intelligence actors of a state may seem parochial, but indicate their incentives for cooperation

with APTs, or positioning APT groups in closer proximity.

Applications of the trust-interdependence-power framework in the analyses of APT behaviour open up future empirical work. Time-series analyses of the MITRE ATT&CK database, which records APT activity as individual groups as well as threat clusters, can be cross-referenced based on common tooling and infrastructure to evaluate the proximity of APT groups to state actors, and help ascertain state offensive cyber power. Despite state capacities to mobilise cyber power effectively through private actor relationships, the state must still convert the utility from cyber power into strategic advantage.

In particular, great powers stake private and public computing resources on emerging technologies, such as vulnerability detection through large language models, for both defensive and offensive purposes. Higher compute may offset exploit discovery costs and change military-civilian engagement for espionage and the global commercial exploit sector significantly. As such, states must compete not just in cyberspace directly, but also through cyberspace in other competition domains to leverage its cyber power. The next section discusses these strategies and their impact on trusted information networks.

4.4 Structural volatility: how power competitions undermine trust dynamics

4.4.1 Overview

States project national power in cyberspace, a domain with a high conflict escalation threshold, through cooperative or coercive competition strategies. A distributed, decentralised World Wide Web has transformed into collections of ecosystems with centralised nodes of power through private actors, such as technology platforms. Information flows passing through these nodes serve as targets for competing states to leverage network dynamics and fulfil strategic objectives. Great power competition in cyberspace systematically decreases trust: as states vie to embed themselves in economically or politically advantageous positions, they destabilise information networks, creating structural volatility. In particular, the section contrasts the cyber competition strategies of the US and China in three cases: cooperation on internet governance advancing norms and standards; explicit coercion, by developing offensive cyber, technological, legal, and regulatory levers; and implicit coercion, by using adjacent economic and political statecraft to reduce access to underlying technologies and exploit interdependence. Cyber conflict literature often adopts realist methods to maximise leverage, while ignoring the structural implications of competition. Policy and strategy implications discuss dynamics of an evolving cyberspace where lower trustworthiness, in the long term, benefits neither competing states nor their societies.

4.4.2 Introduction

Offence-defence cyber operations lead to 'system instability'.[73] Amongst the powers competing in cyberspace with the US, nation-states like China have a greater incentive to invest in a stable cyberspace, as opposed to adversaries like Russia; arguably, in order to secure national interests while serving a strong domestic tech industry.[74] Contrasting strategic logics debate the magnitude and likelihood of stability: intelligence-gathering offensive cyber operations exacerbate instability, but damage-motivated operations maintain relative stability.[75] However, maintaining open access and tech protocols requires competitors to cooperate, so restraint is built into conflict in cyberspace.[76] Political incentives to compete in cyber and cyber-assisted domains misalign with an interoperable, decentralised Internet.[77] This section seeks to provide a link between stability in cyberspace as a socio-technical information system, and strategic stability, containing escalation in great power relations.[78]

By introducing the concept of 'structural volatility' in cyberspace, this section contributes to a contested literature on cyber instability. Stability is variously understood in a technical sense, encompassing network-preserving attributes such as reliability; in a political sense preserving balance of

73. Buchanan, "The Cybersecurity Dilemma: Network Intrusions."
74. Lindsay and Cheung, "From Exploitation to Innovation."
75. Lindsay, "Restrained by design: the political economy of cybersecurity'."
76. J.S. Nye and Cyber power [in en] (Harvard Kennedy School, Belfer Center for Science / International Affairs, 2010); Lindsay, "Restrained by design: the political economy of cybersecurity'."
77. Zúñiga et al., "The geopolitics of technology standards."
78. L. Chuanying, "Forging Stability in Cyberspace" [in en], in *Survival: Global Politics and Strategy*, 2020, Routledge. (April 2020).

power;[79] or through a rights-based approach centred on minimizing individual cyber harms.[80] As great powers approach parity in some domains, pursue regional hegemony to coerce neighbours, and establish influence to project power elsewhere, 'structural volatility' offers an integrated approach to stability[81] great power cyber competition[82] erodes trusted information flows, rendering the costs of instability unpredictable for all other actors in cyberspace. A structurally volatile cyberspace makes policymakers' efforts to anticipate security costs and pursue deterrence in the appropriate context increasingly challenging.

Competition strategies are directed in cyberspace as a stand-alone domain, and through cyberspace, as a facilitator of information flows in other competition domains, linking stability in and of cyberspace respectively. Coercive strategies[83] target the security and reliability of information flows between actors, while cooperative strategies push markets, norms, and governance in service of great power polities to retain privileged access to information flows.[84] Actors defect on existing networks and seek new cooperations to maintain strategic advantage. The resulting changes to networks topologies in cyberspace decreases trust. In other interdepen-

79. F. Rugge, *Confronting an "Axis of Cyber"?: China, Iran, North Korea, Russia in Cyberspace* [in en], 2018, 181; A. Klimburg and L. Faesen, "A Balance of Power in Cyberspace" [in en], in *Governing Cyberspace: Behavior, Power and Diplomacy*, ed. D. Broeders and Bvd Berg (Rowman & Littlefield, 2020).

80. Buchanan and Cunningham, "Preparing the Cyber Battlefield: Assessing a Novel Escalation Risk in a Sino-American Crisis."

81. M. Dunn Cavelty and A. Wenger, "Cyber security meets security politics: Complex technology, fragmented politics, and networked science" [in en], *Contemporary Security Policy* 41, no. 1 (2020): 5–32.

82. Gioe and Smith, *Great Power Cyber Competition: Competing and Winning in the Information Environment*.

83. Valeriano, "Cyber Coercion as a Combined Strategy."

84. C. Ruhl, *Cyberspace and Geopolitics* [in en]; S.C. Hofmann and P. Pawlak, "Governing cyberspace: policy boundary politics across organizations"' [in en], *Review of International Political Economy* 30, no. 6 (2023): 2122–2149.

dent, socio-technical systems, such as the global financial system, political competitions impact market volatility. Market prices are observable to all participants, and measurable through volatility indices, but measuring stability in cyberspace is less straightforward, has long-term effects, and is hard to articulate, complicating states' domestic and foreign policy postures, and a key limitation in empirically validating the concept.

The argument proceeds as follows: great powers such as the US and China deploy coercive and cooperative strategies to compete in cyberspace, challenging the security, reliability and governability of information flows. Key private actors in global supply chains that facilitate information flows become targets of competition. Networked actors in the supply chain, such as downstream consumers, cannot anticipate the impact of these strategies due to limited visibility, and may defect to reduce uncertainty. Defection reduces trust in networks. Unpredictable political behaviour exacerbates defections, and at some threshold, threatens network and system stability. Actors are unable to anticipate the costs of continued cooperation with the remaining network, due to instability, continuing volatile behaviour.

China has sought to impose costs of security on the US through a 'pragmatic' strategy[85] of subsidizing exports, 'choking' information networks, increasing military cyber capability, proposing new Internet architectures at multilateral fora, creating security alliances, and containing domestic private power with anti-trust regulations.[86] Leveraging its domestic political economy in an 'all of nation' effort offers non-aligned powers alternatives to US-centric standards, but risks domestic political and economic volatil-

85. Inkster, "Power Versus Pragmatism: Unlearned Lessons in Dealing with China'."
86. Zhang, "Weaponizing Antitrust During the Sino-US Tech War'."

ity.[87] US counter-strategies of trade tariffs and sanctions, diversifying supply chains, with proposals to ban Chinese hardware in critical national infrastructure, ban Chinese software in electric vehicles, and moratoria on imported spyware, arise from a vastly different domestic political economy, as alliances forged during a period of unipolarity have evolved and domestic institutions become less stable. The risk of 'political pathologies... rather than sound strategic logic' driving competition[88] endangers the conception of cyberspace as a socio-technical institution.[89]

Balancing risks of conflict escalation with costs of entanglement guides deterrent logic.[90] American efforts to contain multipolarity and deter warfighting strategies may provoke unpredictable political behaviour. Schelling's tenets of stability gleaned from mutually assured destruction, strategies of brinkmanship, and signalling intent have arguably broken down in cross-domain competition vis-a-vis non-nuclear state[91] and non-state powers[92].[93] Rising, non-aligned powers gravitating towards a model of 'strategic choice'[94] must align with great powers of compatible interests for security guarantees. In response, the US and its free-rider allies must find significant resources to evoke concessions from formal and informal security blocs, beyond a strategy of persistent engagement fuelling an 'arms race',[95] absent

87. Zhang, "Agility Over Stability: China's Great Reversal in Regulating the Platform Economy'."
88. John J Mearsheimer, "Structural realism," *International relations theories: Discipline and diversity* 83 (2007): 77–94.
89. Lindsay, "Restrained by design: the political economy of cybersecurity'."
90. Nye, "Deterrence and Dissuasion in Cyberspace."
91. Cunningham, "Strategic Substitution: China's Search for Coercive Leverage in the Information Age'."
92. Rowland, Rice, and Shenoi, "The anatomy of a cyber power'."
93. C. Malkasian, *America's Crisis of Deterrence, in Foreign Affairs* [in en], 2024.
94. Leonard, Krastev, and Mark, *Living in an à la carte world: What European policymakers should learn from global public opinion, ECFR*.
95. Klimburg and Faesen, "A Balance of Power in Cyberspace."

international cooperation. The costs of competition can be short-term but severe, targeting key private actors in global supply chains, and long-term and preference-forming.

Section 4.4.3 outlines great power competition strategies in cyberspace as viewed in Chinese scholarship and policy. Section 4.4.4 develops the impact of competition strategies on trust with regards security, reliability, and governability. To conclude, the section explores strategic implications of a structurally volatile cyberspace in future competition scenarios.

4.4.3 Strategies of great power cyber competition

Cooperation and competition are generally seen as separate strategic instruments to further national interests in international relations literature. However, China's regional diplomacy efforts in South East Asia,[96] guided by a 'good neighbour policy'[97],[98] cooperative alliances in Africa[99] and Russia are means to establish influence and challenge the West, through foreign aid, security and military alliances, and supply chain interdependence. Cooperation, such as regional diplomacy and influence-building in so-called non-aligned states, and domestic industry partnerships, is a competition instrument that aligns with China's 2017 cybersecurity strategy as well as its wider 'cross-domain coercion'.

Key supply chain actors serve as strategic targets for great powers, such

96. H. Le Thu, "China's dual strategy of coercion and inducement towards ASEAN" [in en], *The Pacific Review* 32, no. 1 (2019): 20–36.

97. P. Fenghua, L. Zhiyong, and G. Yuejing, "Analysis of China's surrounding geopolitical environment from the perspective of economy and trade: Based on social network analysis[J" [in en], *Geographical Research* 34, no. 4 (2015): 775–786.

98. Huang, *China's Asymmetric Statecraft*.

99. T. Heidger and D. Higgins, "In Africa, Great Power Competition Requires a Great Strategy for Information Operations" [in en], in *Great Power Cyber Competition. 2024* (Routledge).

as in intelligence-gathering in support of economic competition. By establishing themselves as attractive markets, great powers induce or coerce industry actors into subscribing to preferred domestic suppliers in their supply chains, even if the private actor has located principal operations in a different jurisdiction. Rising and middle powers may leverage alliances to capitalise on these advantages. In 2018, iPhone processing chips were allegedly compromised by an Apple supplier in China, Sun Micro, to exfiltrate embedded data.[100] In 2023, some Chinese ministries discouraged iPhone usage, following incorporation of TSMC chips, citing security concerns.[101] Despite GCHQ-led technical evaluations exonerating Huawei equipment of backdoors, the UK followed the US in diversifying its 5G supply chain. Conversely, Huawei developed HarmonyOS to break with its dependence on Google's Android.[102]

Competitive dynamics are also mediated through supply chain actors indirectly. Less-resourced, smaller private actors are cheaper targets and may be leveraged for exploiting a dependent, more powerful private actor; the SolarWinds breach affected Microsoft and many US government departments as a result. Indirect coercion imposes costs on the smaller actor. Contradicting perspectives between political institutions and empirical evidence may fail to contain the effects of coercion beyond the intended target. Espionage can be misinterpreted as preparation for a more serious attack; China's centralised command structure combining the PLA and non-PLA capabilities across offence-defence cyber capabilities may struggle to con-

100. J. Robertson and M. Riley, "China Used a Tiny Chip in a Hack That Infiltrated U.S" [in en], *Companies, in Bloomberg.com*, 2018,
101. *China orders government workers to stop using iPhones amid heightened tensions with US | South China Morning Post* [in en].
102. Fujino, *Huawei breaks free from Google ecosystem with homegrown OS, Nikkei Asia*.

tain 'mission creep' in cyber coercion.[103] Competitive strategies may have different intentions and outcomes, motivating ex post defections.

In contrast to cross-domain cyber coercion and deterrence,[104] competitors may use non-cyber means for cyber coercion. Strategies to project cyber power (See Table4.1) are therefore interdependent events in great power competition. 'Public-public cooperation' and 'indirect, cross-domain coercion' are interdependent: alliances between public actors on governance initiatives, for example, may assist coercion in another domain, and vice-versa. China's veto on US-led motions on the illegal Russian invasion on Ukraine at the UN Security Council reinforces Russia's alleged military dependence on China and its allies. Similarly, 'private-public cooperation' is required for 'direct coercion'. Intelligence agencies cooperate with exploit vendors for covert, direct coercion. Legislative instruments like export control coerce private actors to align with a great power in restricting market access to offensive cyber capabilities.

Chinese scholarship views the US as the aggressor with outsised influence,[105] and asserts the potential for Chinese governance and norm propa-

103. B. Buchanan and F.S. Cunningham, *Preparing the Cyber Battlefield: Assessing a Novel Escalation Risk in a Sino-American Crisis* [in co], ed. Cyberspace et al. (Edinburgh University Press, 2023).
104. B. Valeriano, *Cyber Coercion as a Combined Strategy', in Cyber Strategy: The Evolving Character of Power and Coercion* [in en], ed. B. Valeriano, B. Jensen, and R.C. Maness (Oxford University Press, 2018), 0.
105. Z. Ningnan, "US Cybersecurity Situation Overview" [in en], *China Information Security* 2024, no. 1 (2023): 60–64; T. Lan, "US Department of Defense 2023 Cyber Strategy Perspective" [in en], *China Information Security* 2024, no. 1, 85–88; 王怡青and杨莹莹, "New trends in the U.S. Department of Defense's 2023 Cyber Strategy and its impact and inspiration on China" [in en], *Internet World* 2023, no. 11, 20–25.

Cooperation		**Coercion**	
Private-Public	Public-Public	Explicit	Implicit
Economic inducements to key players in global supply chains	Alignment on governance initiatives	Covert: Deploying offensive cyber capabilities directly on adversaries or allies, or indirectly through supply chain actors	Cross-domain coercion: Using competition strategies in adjacent power domains
Directly or indirectly supporting private actor-led cyber campaigns	Shared offence-defence capabilities with allies	Overt: Regulatory and legal levers on private actors	Cross-domain coercion: Using regional cooperation in one domain to coerce allies in other domains

Table 4.1: A taxonomy for great power cooperation and coercion strategies

gation,[106] in the perceived absence of international laws in cyberspace, as a complement to its model of 'cyberspace sovereignty'. Ideologically-guided discourse on strategic stability[107] arise from a self-defensive view,[108] moti-

106. Y. Li and Z. Xiuzan, "China's solution to "ideological governance" of global cyberspace" [in en], *Journal of Zhengzhou University (Philosophy and Social Sciences Edition* 51, no. 1 (2018): 70–75; Z. Huang and Y. Ying, "Chinese approaches to cyberspace governance and international law in cyberspace" [in en], in *Research Handbook on International Law and Cyberspace* (Edward Elgar Publishing, 2021), 547–563; L. Shu, "Internet extreme risk prevention and great power game" [in en], *Journal of Tongji University (Social Science Edition* 33, no. 4 (2022): 48–57; L. Yan and W. Yuanshan, "Multiple risks and countermeasures of data sovereignty security in the context of cyber warfare" [in en], *information magazine* 42, no. 5 (2023): 54–60.

107. 王 守 都, "Discussion on the Strategic Stability of China-US Cyberspace——Analysis of Political Factors in the Field of US Domestic Cybersecurity and Governance during the Trump Period" [in en], *Information security and communication confidentiality* 2019, no. 11, 46–59.

108. S. Yi and J. Tianjiao, "Offense-defense balance in cyberspace and the construction of cyber deterrence" [in en], *World Economy and Politics* 2018, no. 2, 49–70.

vated by China's defence vis-a-vis the Russia-Ukraine conflict,[109] the pre-emptive threat from US cyber capability,[110] cross-domain competition,[111] and analyses of great power security strategies.[112] In particular, it accuses the US of brinkmanship[113] and weakening deterrence,[114] of side-lining Chinese industry where companies have disclosed covert US action and restricting competition.[115] Acknowledging growing internal complexity and strained power relations, it paints a pessimistic view of escalation in the absence of institutionalization, using bilateral interdependence as at once the instigator and container of Chinese cyber power.[116] Notably, these academic views show a greater sensitivity to Western literature on cyber stability than Western sensitivities to Chinese political and cultural nuances defining strategy.

Government policy corroborates scholarship on China's 'all of nation'

109. L. Ping, "From the Russian-Ukrainian conflict to the trend of cyberspace weaponization and its impact" [in en], *China Information Security* 2022, no. 6, 65–69.
110. 刘. 郭海, "US cyberspace combat capabilities and development trends" [in en], *China Information Security* 2022, no. 2, 64–67; D. Wumei, *Current Status of US Cyberspace Combat Forces* [in en], vol. 44 (National Defense Science / Technology, 2023), 92–103.
111. L. Chengliang, W. Jie, and D. Debin, "The spatial domain and balance of power of China and the United States" [in en], *Journal of Natural Resources* 35, no. 11 (2020): 2596–2612; Chuanying, "Forging Stability in Cyberspace"; 张舒, "Observation on the cyberspace situation in the context of great power competition in 2023" [in en], *China Information Security* 2024, no. 1, 57–59.
112. Z. Zhihua, C. Rongying, and Z. Lingke, "Analysis and enlightenment of network information security strategies of major developed countries" [in en], *Modern Intelligence* 37, no. 1 (2017): 172–177; Z. Jie, L. Yanhua, and H. Zhichao, "A Brief Analysis of the UK's Cyber Warfare Force" [in en], *Information Security and Communications Privacy* 2021, no. 4, 1–8.
113. 王帆, "US Strategy Towards China: Strategic Tipping Point and Restrictive Competition" [in en], *Contemporary World and Socialism* 2020, no. 1, 137–145.
114. B. Zhe, G. Yuetao, and C. Xiaofei, "Research on the Weakening Trend of US Cyber Deterrence Strategy" [in en], *Information security and communication confidentiality* 2023, no. 7, 1–11.
115. "A historical review of cyber attacks by US intelligence agencies - based on information disclosed by the global cybersecurity community" [in en], *Industrial Information Security* 2023, no. 2, 87–93.
116. 李雨萱, "The cohesion of China's power in cyberspace in the new era" [in en], *China Military to Civilian* 2024, no. 13, 18–20.

efforts. Tax breaks, procurement policies, subsidies, and small fines favour China's domestic tech industry. Growing situational awareness in partnership with Chinese cybersecurity firms are a key part of defence operations since 2017 through the China Cybersecurity Industry Alliance. CERT centralises incident reporting. Other private actors such as state-sponsored hacker groups and APTs have a more complex relationship, as revealed in the 2024 I-SOON leaks, where the state must balance costs from third parties' offence against its own defence. Global campaigns such as Stone Panda's 'Cloud Hopper' campaign targeted managed service providers, compromising dependents in the supply chain. Pervasive economic espionage against the US (APT41, APT1) aside, China has targeted US allies through APT relationships, with APT33 campaigns on Middle Eastern aerospace and APT27 cross-sector campaigns in APAC.

To establish influence, China advances norms and security frameworks through national initiations, regional alliances, common-interest emerging powers partners and multilateral fora, vis-a-vis BRI, APEC, Global Security Initiative, BRICS, SCO, and the UN; bilateral partnerships address counterterrorism and cybercrime. In particular, China has exported and invested in surveillance systems, such as facial recognition technologies used in domestic security, to BRI partners, African nations as part of infrastructure investment, and strategic partners such as Pakistan, where cooperation with the US has strained, Venezuela, and Iran. Governance and standards proposals on TCP/IP protocols at the UN ITU complemented a China Standards 2035 strategy of 'decentralizing' Internet away NIST-influenced

standards, sparking Western concerns of Internet fragmentation.[117]

Government publications indicate a consolidation of the domestic cyber posture. The annual cybersecurity report issued by the Chinese Ministry of Industry and Information Technology (MIIT) indicates coercive campaigns based on cooperation with industry and academia. Additionally, the 'three pillars' of Cybersecurity and Standardization Laws 2017, national cybersecurity strategy, and other MIIT-issued publications, such as the 2024 Cybersecurity Review Measures, identify regional and national oversight on critical information infrastructure providers to comply with time-bound reviews of vulnerable technologies. PLA offensive cyber campaigns are more coherent, mediated from the overarching Cyberspace Administration through to the military and government departments; the Strategic Support Force reorganised into Information and Cyber Support Forces trickle down into regional policing structures, and military units share infrastructure and personnel overlaps with APT groups.[118] Within the ISF, 3PLA Unit 61486 commands Western theatres, with units in 3PLA and 4PLA responsible for electronic warfare, possibly reorganised from 2PLA's Unit 61398, identified in Mandiant's APT1 report on the US OPM attack.

China's comprehensive strategic mechanisms in the last decade bolster domestic security capabilities, complementing competitions with the US across cyber, space, sea, and energy, by additionally leveraging power relations with APAC and non-aligned states. Other competitions, such as dominance over undersea cabling, further destabilise global cyberspace. Volatility is defined in relation with stability; information networks are

117. S. Hoffmann, D. Lazanski, and E. Taylor, "Standardising the splinternet: how China's technical standards could fragment the internet" [in en], *Journal of Cyber Policy* 5, no. 2 (2020): 239–264.
118. Pukhraj Singh, "China's Military Cyber Operations" [in en].

stable when the information flows in the network are maintained through cooperation between nodes. When defection between nodes threatens the integrity of a network structure by collapsing or radically transforming power hubs, the network is unstable; unpredictability in defections creates network volatility. The next section details how volatility becomes structural as a result of great power competitions.

4.4.4 Structural volatility and trust in cyberspace

An 'arms race' model of cyber conflict, where great powers steadily up the ante with cyber deterrents, is preferable on balance, strategic logic goes, as cyber conflict keeps a check on escalation in other domains.[119] Free-riders and security allies of great powers, also exposed to interdependent networks which act as attack surfaces, are more vulnerable, but defecting to break interdependence and mitigate against this exposure would diminish the ability of the great power to project power.[120] Future defence costs rise with growing complexity from defensive infrastructure needed to deter the worst effects of coercion. Structuralists suggest that nation-states positioned to 'weaponise' interdependent networks will be able to afford competition. Determining structural advantage in great power competitions in the short and medium term, however, neglects how networks evolve in the longer term due to the same competition strategies, and influence future competition.

119. Lindsay and Gartzke, "Coercion through Cyberspace: The Stability-Instability Paradox Revisited."
120. Farrell and Newman, "Weaponized Interdependence."

Network effects of competition impact structures in cyberspace

First, the arms-race model may lead policymakers into a tradeoff on security investments in the present versus contending with higher future security costs. It implies that with increasing complexity and degrading security, trust will become an increasingly expensive property of networked information systems. The cost of losing trust is specific to the relative position of an actor in the network. Multiple defections in a network may lead to collapse of a network with certain topologies, but not of the underlying system. For example, loss of trust may be less expensive close to a 'hub' rather than a 'spoke', given the hub's advantage of information volume, but a defecting hub can fragment the network.[121] With multiple collapsed networks, the system itself may be under threat. Rising and middle powers may lack the resources to observe these dynamics and the expected cost. Non-aligned states may seek new alliances with great power security guarantors for bridging this asymmetry.

Second, the logic of balancing power in an arms-race model must account for private actor relations with the state. As key private powers in global supply chains reach dominant status in their home jurisdictions, they can challenge the host state's coercive strategies owing to their structural advantage in global supply chains,[122] more effectively in liberal democracies. In authoritarian systems, given the lack of internal political competition, state clampdown of private power can be a pyrrhic victory, compromising domestic political and economic stability for fear of 'political re-

121. R. Axelrod and W.D. Hamilton, "The Evolution of Cooperation" [in en], *Science* 211, no. 4489 (1981): 1390–1396; Nowak, "Five rules for the evolution of cooperation."
122. Chen and Evers, ""Wars without Gun Smoke": Global Supply Chains, Power Transitions, and Economic Statecraft'."

placement'.[123] Dominant supply chain actors are subject to similar power dynamics vis-a-vis challengers; while dominants can afford defences against direct coercion, smaller downstream actors are more exposed. Coercers exploit the dominant actor's dependence by coercing smaller dependents, who are incentivised to merge with dominants in the absence of anti-trust and competition protections.

Third, cyber campaigns have strategic intent,[124] of which power projection may be one. Despite the China's limited success in using cyber espionage to replicate US military capability,[125] it has nonetheless continued with offensive cyber campaigns, undeterred by public attribution. Repetitive coercion suggests signalling:[126] first, of knowledge that interdependence ensures mutual detriment from Western economic reprisals to direct coercion, where the transition to sanctioning companies over individuals risks supply chain interoperability; second, of a calculus of faith in achieving strategic objectives through cyber means over time, given recent reports of the PLA consolidating its information warfare setup;[127] third, of confidence in its own influence, such that US allies and non-aligned states may apply punitive counter-strategies with decreasing enthusiasm, as seen in the economic domain with the EU's deliberation in balancing climate goals with following US tariffs on Chinese EVs. Unsurprisingly, cyber coercion has intensified,[128] impacting trusted networks.

Fourth, the risk of misreading strategic intent, from both competitors

123. Acemoglu and Robinson, "Economic Backwardness in Political Perspective."
124. Harknett and Smeets, "Cyber campaigns and strategic outcomes."
125. Gilli and Gilli, "Why China Has Not Caught Up Yet."
126. Lonergan, "Cyber Operations, Accommodative Signaling, and the De-Escalation of International Crises'."
127. Nouwens, *China's new Information Support Force, IISS*.
128. J. Healey and R. Jervis, *The Escalation Inversion and Other Oddities of Situational Cyber Stability* [in en], ed. Cyberspace et al. (Edinburgh University Press, 2023).

and allies. A competitor misinterpreting signalling in cyberspace risks escalation in other domains; in cases where espionage and 'operational preparation' are indistinguishable, strategic logic has no obvious de-escalation path even after detection.[129] An ally misinterpreting signalling may feel tacitly supported in applying additional coercive strategies against its great power ally's private and public competitors. Similarly, private and semi-private actors such as mercenaries and APTs may misinterpret signalling as approval for coercion. Ambiguous signalling may be construed as a coercive tool, albeit a dangerous one, even when the ambiguity is unintentional, arising from domestic political instability or reactionary foreign policy. Ambiguous signals help great powers exploit their public-public and public-private security alliances. Therefore, stability in cyberspace is dependent on stable political behaviour and trustworthy networks.

Furthermore, network effects that exacerbate power inequities are caused by network topologies, but also by the competitors' perceived value of information networks facilitate. The incentives to stabilise must be less expensive than the value derived from a competition strategy, in turn determined by the priority of a national objective. The China-attributed 2024 breach of major US ISPs, which has allowed access to court-warranted surveillance targets allegedly exploits vulnerable Cisco routers, weakened a large market of dependent non-targets. Coercion would be more expensive if Cisco did not sell in the Chinese market; conversely, Cisco would be less resourced to meet security costs. Given the economic and political value of the information flows facilitated by some key networks, complete fragmentation would entail expensive redundancy for intelligence-gathering, and

129. Buchanan and Cunningham, *Preparing the Cyber Battlefield: Assessing a Novel Escalation Risk in a Sino-American Crisis*.

incur a high cost of breaking interdependence. The benefits in national security, for example, on critical national infrastructure, may be weighed against the potential for diminishing power in other domains, especially for middle powers: diversifying the UK telecommunications supply chain from Huawei began in 2020 after a rejected tender to rollout 5G, but BT hardware reliance persisted for several years afterwards.

Given the structural implications of great powers shaping network topologies directly or indirectly, the strategic value of information networks surmised from their competition behaviour, and the resulting effect on the behaviour of rising powers, a fragmented Internet, where cyberspace splits up due to opposing polities' regulatory regimes, is unlikely to emerge as a consequence of cyber power competition, as it befits neither great power's strategic interests. The Great Firewall is better understood as a tool of suppressing domestic political dissent, rather than a defensive competition strategy.[130] Similarly, blocking social media apps is a punitive response to rising private power, rather than a direct enactment of strategic intent in power competition. While great powers may be placed to incur the costs of breaking interdependent information networks in cyberspace, the disadvantage to competition may prove too expensive; the impact of the disadvantage for non-aligned powers is incurred in the resource costs to build new, trusted networks.

Loss of trust and cyberspace instability

To build and maintain trust in a network, the underlying technology protocols serving information flows must be able to preserve the properties

130. J. Quinn, "A Peek over the Great Firewall: A Breakdown of China's New Cybersecurity Law" [in en], *SMU Science and Technology Law Review* 20 (2017): 407.

of information passing between two nodes. Each node must be able to signal 'trustworthiness' to the sender within or outside cyberspace, for instance, through evidence of adopting such protocols, which is accepted by the sender, if it preserves the sender's expectation of information value, and a transaction occurs. This economic nature of information exchange must be upheld by the political act of signalling and acceptance for, at least, the duration of the transaction. In networked information systems in cyberspace, for example, the political and economic transaction is validated by means of an access policy.

When the political aspect of signalling and accepting the recipient node's trustworthiness becomes unreliable over repeated transactions, or the economic aspect of the sender's valuation is distorted through some onward transaction conducted by the receiver, the sender perceives the receiver's behaviour to be unstable, and nodes suffer from a loss of trust. This may manifest in lower fidelity transactions, such as by withholding public information or disclosing private information, or stopping information flows altogether. In the case of structural volatility, the cost of suffering this loss of trust becomes unpredictable, as the receiver's behaviour becomes unpredictable over time.

Unpredictability may arise from increasing costs for the receiver to signal trustworthiness, or some external political strain applied by its interdependent nodes. The sender's requirements may also be satisfied more cheaply through another node. Such structural dynamics of information flows in cyberspace underpin power competitions. In particular, stability in networked information systems constituting cyberspace requires that information flows satisfy expectations of security, reliability, and governability

between nodes. Socio-technical actors in cyberspace, such as infrastructure-supplying private actors, are subject to contracts, such as service level agreements or compliance requirements, from other public and private actors that guarantee these expectations to be met up to some threshold. However, the impact of competition strategies undermine these expectations.

In particular, as security of the information flow is compromised through coercion, the sender can no longer accept the receiver's signals to maintain confidentiality, integrity, or availability of the information therein. Reliability, measured through consistency metrics or uptime, may be lost if either node defects to disclose private information, restrict public information, or stop information flows. Finally, governance, depending on the location of the nodes within a network as being subject to different jurisdictions across the underlying system, can cause defection and loss in trust. Against growing private power, governance may yield to self-regulation, and defection arises from a loss in trust in the hub, such as a tech platform. State coercion over private power may not always be obvious, especially for consumers of platforms outside the state's jurisdictions.

The cost of instability for the actor nodes in the network become unpredictable when defections in the network can result in collapse of information flows between the two nodes, with the rest of the network having to bear costs of security, reliability and governance; or result in collapse of the network itself, in which case the defecting nodes must bear the cost of signalling for new information transactions with nodes in another network; or of the system itself, where all information flows cease. If trust in a network created some public good, collapse can result in a tragedy of

the commons scenario, where nodes other than great powers must bear the cost of competition.

In all three cases, trust is lost. However, constituent nodes may not know the threshold at which a flow, or the network, or the system collapses, or cannot observe other nodes, making the costs of instability either unpredictable or unaffordable. The effects of structural volatility are already felt, for example, in pricing cyber insurance premiums, where insurers feel reluctant to take on the liability of insuring against perceived 'cyberwar'.[131] Similarly, policymakers may find that offence-defence resource allocations become tactical and short-termist. End-users of technology products in supply chains suffer downstream impact from direct coercion. Critical and civilian national infrastructure, in attempts to diversify supply chains to mitigate exposure to interdependent networks, runs the risk of more expensive technology from private actors who bear the costs of coercion instead. Changes in governance between jurisdictions passes on cost of compliance to private actors incentivised to retain market access.

Unpredictable political behaviour in great power competition can exacerbate instability and related costs for all actors. Ambiguous signalling can cause defections due to misinterpretation or a higher relative cost of interpretation. If the ambiguity in signalling is intentional, it can be interpreted by the competitor as having exhausted deterrence logic, and provoke unpredictable behaviours in return. But ambiguity in signalling can also be a byproduct of poorly estimating target security and reliability, as well as the impact to dependents of the target, as a result of limited intelligence gathering. Distinguishing intent ex post may be impossible, leading

131. J. Wolff, "The role of insurers in shaping international cyber-security norms about cyber-war" [in en], *Contemporary Security Policy* 45, no. 1 (2024): 141–170.

the competitor to misjudge the signaller's capabilities. While many unpredictable behaviours in cyberspace may not escalate into war-fighting, but merely reflect political misalignment, making defensive investment models unreliable will compel other actors in committing to higher security costs.

Ambiguous signalling by a great power has security implications for free-riding rising and middle power allies in addition to exposure by association, and coercion in expending resources against a common adversary. The great power signals investment in offence as a matter of strategic priority, prompting the smaller power to align its strategy or free-ride on security benefits, covering its deficits in decreasing its attack surface, decreasing reliance in cyberspace for securing national interests, or de-prioritizing cybersecurity in civil applications. The great power influences rising and middle powers operationally through security alliances in the role of a stakeholder. In liberal democracies, it may be amongst many private and public stakeholders, spreading accountability of the effects of cyber campaigns, while in authoritarian systems the accountability is limited in reporting to the state sponsor. As a result, responsible behaviour in cyberspace has higher associated costs to satisfy all stakeholder requirements, but given plausible deniability and the role of secrecy in cyber campaigns, smaller powers may struggle to allocate resources in offensive cyber campaigns efficiently.

4.4.5 Conclusion: Instability in and of cyberspace

The implications of volatility change based on the roles assumed by the state. In power competitions, the state may find a structurally volatile cyberspace to its advantage in three scenarios. First, when the leverage gained from a competition strategy is significant enough to outweigh the

maximum costs from instability it may incur. In particular, in campaigns aimed at shorter-term, tactical gains, the value of information extracted or exposed may be greater than the cost of developing and deploying software exploits. Rising and middle powers may favour tactical campaigns to achieve strategic ends piecemeal, given the relative lower cost. Influence campaigns, which convert adversarial high-trust networks into low-trust networks, may have a relative higher upfront cost in development time and resources needed to cause multiple network defections, but pay off in entrenching information flows favourably in the longer term.

Second, when the cost of competing in another domain exceeds the cumulative costs from volatility imposed and incurred. As great powers reach parity in military or economic domains, the costs of structural volatility become acceptable to them as a necessity of cross-domain coercion. As China bolsters its military power through leverage established across domains, such as trade, or uses economic leverage through foreign investment to influence rising powers in adopting favourable norms, the relative costs of cyber and cyber-assisted coercion lower in the longer term. The security preferences of influenced rising and middle powers change towards strategic alignment with potential consequences for regional governance and norms. While regional hegemony and the threat of cross-domain coercion may temper regional conflict escalation, as the costs of a regional rising power defecting may be affordable, the competing great power may inject stimulus into more expensive competition domains.

Third, when volatility favours the state's public-private alliances. Firstly, with semi-private actors, such as hacker groups, who are incentivised to exploit poorer security and reliability for profit, exacerbating volatility and

giving the sponsor state cover. Secondly, for private companies which leverage volatility for profit by providing mitigations to consumers in interdependent supply chains. A more volatile cyberspace can be weaponised by home jurisdictions of key supply chain actors to gain economic power.

In intelligence-gathering, the state interprets volatility depending on whether it interacts with allies or adversaries. An agency may sell a vulnerability equity to an ally for a lower price, offset by the cost of expected volatility from private knowledge of some ongoing direct coercion. Similarly, an agency may disclose a vulnerability where it deems that the maximum cost of volatility incurred will be offset by the security costs imposed through the adversary's frequent use of the vulnerable technology. However, gaining this ex-ante information systematically may be expensive given the absence of international cooperation on the equities process. The role of secrecy and domestic coercive instruments would cause an equities market failure with conflicting incentives between policy and intelligence actors to correct it. Additionally, time involved in developing equity risks losing a race condition, when an adversary launches offence capability causing tantamount damage, as pre-emptive defences require disclosure to the tech provider. Intelligence agencies are not always favoured by the volatility to which they must contribute.

In policymaking, the state is incentivised to implement governance to secure national interests, by prioritizing defence investments to protect its citizens, protecting its economic interests by diversifying supply chains, and measuring volatility to anticipate future costs. To either induce stability or lower the relative costs of instability, the state uses regulatory or legal levers on the private sector to raise minimum standards for secure and reliable

technology. However, as private power grows in liberal democracies, the costs of instability may be passed on from the state to the citizen through the private actor. Bargaining with the state to compensate for perceived losses incurred from regulation, the private actor passes the cost of lost trust to the citizen through poorer security and reliability of technology products.

The same costs are likely to be assumed by the state in state-led and owned industries, allowing more authoritarian states to coerce already low-trust societies. Even with China's pragmatic strategies evolving from top-down hierarchies into partnership-based domestic industries, private power remains throttled, and the citizen cannot leverage buying into domestic tech markets to foster trust in information networks. In contrast, digital societies in liberal democracies, faced with incurring the costs of volatility can, in response, help rebuild trust through domestic institutions, industry, and civil society. In particular, the risks from emerging technologies will require successful bargaining with the state to temper the increasingly pernicious effects of volatility.

Chapter 5

Conclusion: Who profits?

Who profits?

In what circumstances could structural volatility benefit the development or disclosure of vulnerability equities, and when can coordination help? Factors such as the extent of the target's use of vulnerable technology, costs of perceived harms and disclosure, and benefits from value added and deployment, contribute to decision-making on optimal disclosure time in the equity process.[1] However, results from the trust model show that decisions to disclose, develop, or deploy, must consider timing as well as network structure, based on actor interaction.

Whether the equity is deployed on a specific competitor, shared with an intelligence ally, or disclosed are strategic decisions based on the equity holder's connectivity and position in the network. As discussed in the previous section, retaining the equity runs the risk of disclosure by a

1. Tristan Caulfield, Christos Ioannidis, and David Pym, "The U.S. Vulnerabilities Equities Process: An Economic Perspective" [in en], in *Decision and Game Theory for Security*, ed. Stefan Rass et al., Lecture Notes in Computer Science (Cham: Springer International Publishing, 2017), 131–150, ISBN: 978-3-319-68711-7, https://doi.org/10.1007/978-3-319-68711-7_8.

competitor, which leaves the equity holder open to coercion. Furthermore, disclosure may disadvantage an uninformed ally. As costs of interpreting signals become unpredictable, highly connected agents may unilaterally decide the fate of the equity; cooperation in disclosure efforts reduces the cost for all agents in the network.

In particular, structural volatility can benefit retainment when an equity-holding state actor is able to leverage volatile networks to create conditions where the strategic competitor discloses its own equity posture. Based on the model's results, more randomly dispersed nodes are less impacted by network policy interventions, and as such, may defect with lower cost to the remaining network. The equity-holder may decide to target actors who are loosely allied with its direct competitor, and coerce these allies into defection to reveal the competitor's equity posture for some marginal advantage.

Highly connected actors in a network can lead critical decision-making on how disclosure of an equity can exacerbate or contain short- and long-term volatility, and whether this can be leveraged to the advantage of other actors in the network. For example, given private knowledge of an ongoing coercive campaign, a dominant intelligence agency can offload an equity to a loosely connected actor at low cost, if the agency determines that the volatility costs imposed on the actor from disclosure are higher than equity value. While policies like GCHQ claiming to disclose 90% of equities can create short-term volatility by creating exposure windows for consumers of the affected vendor in mitigating risk from unpatched vulnerabilities, intelligence agencies can still use this volatility to their benefit. By coercing vendors to withhold patching until some optimal time, agencies can define

a strategic approach to disclosure based on assessments of the target's capacity to defend itself and prevent allies from defecting. In these cases, coordination between intelligence agencies and allies can balance risks from short and long term volatility to meet their strategic objectives.

In the US and the UK, inter-agency coordination mediates decision-making on disclosure or retainment through an equities board, who may cooperate with their international allies for vulnerabilities in large-scale technologies or critical supply chains. Additional complexity arises from the expansion of the ownership for offensive cyber activity within state actors. In the US, for example, the critical role of the NSA in taking central responsibility for campaigns has evolved into tens more agencies over 30 years. Resource conflicts between agencies can skew decision-making towards network hubs, which stewardship can mitigate.

Future work on the equities process may motivate modeling equities in a commodity market-like platform between networked agencies, with the oversight board as a market-correcting steward, for example, where strategic differences in valuing equities does not impose punitive costs in less connected actors due to information asymmetries arising from their highly connected peers. In practice, however, these decisions can take a tactical nature due to on agency rivalries and the hierarchies in state actor relations. As such, any calls for transparency from civil society, and cooperation through legal regimes and other instruments, such as coordinated disclosure between allies or at multilateral levels,[2] conflict with the state's incentives to adopt a more strategic decision-making approach,

2. Teodora Delcheva Soesanto, Yasser El-Shimy, and Jennie Bradley Stefan, *Time to talk: Europe and the Vulnerability Equities Process* [in en-GB], March 2018, https://ecfr.eu/article/commentary_time_to_talk_europe_and_the_vulnerability_equities_process/.

and must be more specific. Given the preferences of US and UK intelligence agencies to position their work in the context of 'responsible cyber power',[3] transparency on optimal disclosure times may address multilateral concerns, but transparency on equity postures or strategic advantage from leveraging connectivity would be counterproductive to competition.

As such, the answer to the central research question of who profits from the dynamics of leverage in cyberspace involves contextual and strategic considerations. In models like the cybersecurity dilemma, optimising offence-defence costs takes a central role, and overlooks actors' varying conceptions of profit. This approach may lead analysts to consider profit vis-a-vis actors who impose the highest coercive costs while minimising costs of their own defence, for example, by offsetting the benefits received from public goods that cooperation creates. However, these models are limited in explaining how agents update preferences and change their contributions in networks as their visibility of network dynamics changes. Therefore, structural considerations, such as the level of effort agents have the capacity to expend, and when, must be supplied in answer. For espionage campaigns, in particular, the resources expended in intelligence-gathering, but also converting intelligence into competitive advantage, is specific on a case-by-case basis, but above all is indicative of the importance the state places on the national objective and intent fulfilled by the campaign. In this sense, who profits from espionage takes on a more strategic nature than tit-for-tat strategies in escalating cyber conflict.

3. *Responsible Cyber Power in Practice (HTML) - GOV.UK*, April 2023, https://www.gov.uk/government/publications/responsible-cyber-power-in-practice/responsible-cyber-power-in-practice-html.

Conclusion

In October 2024, Bill Burns, the Director of the CIA, outlined the threats his agency must safeguard against in preparing itself for an 'age of strategic competition', by selectively declassifying intelligence gathered through espionage, intended to leverage adversarial and allied relationships towards US interests.[4] Burns' admissions of the CIA's challenges makes the themes explored in this thesis — of a dynamic theory of cyber power, the mobilisation of cyber power by nation-states to conduct espionage in order to strategically compete, and the effects of the dynamics of leverage on networks in cyberspace — urgent and policy-relevant.

Although this thesis is grounded against the backdrop of US-China strategic competition, the dynamics presented here may be adapted to the context of great power competition more widely, but also to strategic cooperation-defection contests in smaller environments with clear hegemon-challenger network structures. In addition, the development of emerging technologies in the field of artificial intelligence and quantum computing may benefit from further analysis, in particular where the implicit but crucial dimension on time on leveraging trust relations, breaking interdependences, and power transitions can lead to an acceleration in competitive advantage at more tactical levels, such as decision-making on equities and the cost of balancing defensive security policies with other forms of cyber statecraft. In particular, unpredictable political leadership in great power competition, and its impact on cyberspace, non-aligned powers, and civil

4. William J. Burns, "Spycraft and Statecraft: Transforming the CIA for an Age of Competition Essays" [in eng], *Foreign Affairs* 103, no. 2 (2024): 74–85, accessed October 23, 2024, https://heinonline.org/HOL/P?h=hein.journals/fora103&i=284.

society actors vis-a-vis renewed motivations for espionage operations, remains an ongoing and critical concern.

To summarise, this thesis has presented a dynamic approach to theories of cyber power, where nation-states leverage their relationships with partner and competitor states, as well as various private actors, to mobilise cyber power and conduct digital espionage in order to strategically compete. In answering the central research question — what are the dynamics of leverage in cyberspace, and who profits — the thesis finds that actors can leverage a structurally volatile cyberspace in their strategic favour, by adapting their domestic and international security policy responses based on structural considerations at optimal times. In particular, multilateral efforts to advance trust-based cyber norms is complementary to strategic cyber power competition.

In developing a theory of cyber statecraft, and situating digital espionage within it, this thesis has sought to make four contributions. In Chapter 2, a conceptual framework links political, economic, and technological notions of trust and power as variables, linked through interdependent information flows, in information systems. By presenting trust as a process between actors, who leverage interdependence as trust is established to gather power, the framework contextualises the cyber domain as a tool and medium of statecraft. In doing so, it invokes complex network structures of public and private actors, where strategies of cooperation and defection are grounded in a dynamic network structure, and actor agency, though with limited visibility of the network, updates as the structure evolves. Giving explicit properties to cooperation and coercion in cyberspace, the chapter looks at the political and economic incentives of state actors as they com-

pete strategically across domains. The challenge of ascertaining strategic intent behind espionage is illustrated in the context of a covert, coercive competition strategy, amongst others.

In Chapter 3, this thesis has sought to substantiate these claims through a game theoretic model of cooperation. Whilst extant game theory treatments of international relations pursue an agent-centric view of power relations, the model presented uses concepts from dynamic international political economy to include structural considerations. The innovation is in constructing a tractable model that allows network participants to show stochastic behaviour, as well as investigating incentives to invest in cooperation and defection outcomes over a long run of games, so that actors can update their strategies based on forward planning. In setting up public-private actor network games, multiple defections do not always lead to networks collapsing, but variability in behaviour creates network volatility. Unlike games in static structures, or between agents with fixed preferences, the model shows no dominant steady state, and as such, no lasting structural power outcomes for actors, making trust-building and stability concerns that interventions such as stewardship can address.

In Chapter 4, this thesis has contributed to cyber power theory using dynamism in agency and network structure. Measures of cyber power presently use qualitative methodologies that neglect the political and economic contexts of competing states. Extant cyber power theories tend to be grounded in realist treatments arising from deterrence, arms control, and war-fighting literatures, where the state's strategies are based on agency, rather than structure additionally. An initial framework presents interdependence of knowledge of software vulnerabilities and tooling used

to conduct, which is weaponised by great power competitors due to their structural advantages. This static approach is then extended to look at espionage networks more broadly. In particular, the application of the conceptual framework to relations between state actors and private actors, such as advanced persistent threat groups, argues that the use of interdependent tooling may signal the structural properties of state-private relationships, such as how closely linked APT groups might be to state sponsors, which defines the operational characteristics of espionage campaigns, and may help determine strategic intent.

Finally, using model outcomes and by examining strategies of great power competition in and through cyberspace, the introduction of the concept of structural volatility aims to reconcile debates in literature on linking strategic stability with the stability of information flows in cyberspace. Unstable political behaviour in the context of power competitions between state actors risks instability in cyberspace by undermining trust between information flows. As competitions intensify, the effects of a structurally volatile will be felt more widely than by competing actors in cyberspace. This concept introduces policy dimensions to the overall thesis, where states must allocate policy resources to balance implications of their foreign policies in cyberspace with securing domestic objectives, such as national security and defence. Governance and policymaking in democratic political systems are well-positioned to contain the negative effects of structural volatility by building trustworthy information systems. Conversely, espionage operations may not always benefit from structural volatility, as the costs of developing offensive capabilities become asymmetric, and the costs of escalation in cyberspace are passed on to technology consumers.

This thesis also presents several limitations in its analyses, which may motivate future work. Foremost, no political economy can be complete without the assessment of the impact of competition strategies, such as espionage, on civil society. Digital espionage campaigns are more far-reaching than in strategic competition; the impact of direct coercion on political and economic targets that undermines trust in democratic institutions through influence-building and information manipulation that radically transform societal discourse.

Second, the role of more intangible factors, such as institutional memory and the extent to which ideology guides strategy, particularly in relations between state actors. Relations between state actors inside a state or between states are often conducted through a framework of shared history and long-standing alliances that outlive strategic benefits. As such, sound strategic logic may be overlooked in lieu of maintaining the status quo. In particular, the nature of political leadership, and the resilience of economic systems in response, pose a lesser disadvantage in cyberspace engagement than in traditional international relations. Scholarship in cultural, sociological, and anthropological literatures such as shared identity and institutional culture in explaining relations of trust where economic reasoning fails may yet provide a richer picture of trust and defection than theories of international political economy. In the near-decade since conceiving solutions to the cybersecurity dilemma, based on fostering trust in information networks, great powers have nonetheless exploited their structural power as regional or global hegemons, signalling, at best, ambiguity towards cyber norms in their revealed preferences. Thin technological and economic framings of trust, where cooperation and defection strategies such

as tit-for-tat or win-stay-lose-shift continue to serve policy rationales disproportionately. The lack of political and policymaking will in understanding adversarial states' evolution into their present political and economic institutions may ultimately lead to escalation in cyber conflict arising from misinterpretation priced into policy methodologies.

Finally, the disparate narratives between different communities in international security lack a common vocabulary, concept development, and methodologies in analysing cyber conflict. The gulf between, for example, the attitudes in military culture towards cyberspace, one of excessive offensive as deterrence and excessive access restriction as defence owing to hierarchical cultures, could not be greater than with attitudes on Internet policy in the academic community. Whilst methodological pluralism encourages the discovery of new points of convergence, and reveal divergences to further scrutiny, disagreements on preliminaries and objectives may play to the disadvantages of multidisciplinary scholarship.

Nonetheless, the contributions made in this thesis add to the many voices and attempts across disciplines which, despite conceptual differences, have long advocated for the value of trust-building in information networks. Empirical work based on open source data, as well as systematising threat intelligence, can use concepts such as the trust framework and model, and structural volatility, to contain irresponsible behaviour in cyberspace. Evidence generated from this work must support policy work at technological, social, national and multilateral levels. Intensifying espionage and investment in offensive cyber capabilities will not, and cannot, be contained, but escalation need not be the inevitable result, if states engage with the idea that their incentives to maintain a balance of power in cyberspace are

contingent on their efforts to build trust.

Bibliography

Ablon, Lillian, and Martin Libicki. "Hacker's Bazaar: The Markets for Cybercrime Tools and Stolen Data." *Defense Counsel Journal* 82 (2015): 143. https://heinonline.org/HOL/Page?handle=hein.journals/defcon82&id=143&div=&collection=.

Acemoglu, Daron, Azarakhsh Malekian, and Asu Ozdaglar. "Network security and contagion." *Journal of Economic Theory* 166 (2016): 536–585.

Acemoglu, Daron, and Asuman Ozdaglar. "Opinion dynamics and learning in social networks." *Dynamic Games and Applications* 1 (2011): 3–49.

Acemoglu, Daron, Asuman Ozdaglar, and Alireza Tahbaz-Salehi. "Systemic Risk and Stability in Financial Networks." *American Economic Review* 105, no. 2 (2015): 564–608.

Acemoglu, Daron, and James A. Robinson. "Economic Backwardness in Political Perspective" [in en]. *American Political Science Review* 100, no. 1 (February 2006): 115–131. ISSN: 1537-5943, 0003-0554, accessed August 28, 2024. https://doi.org/10.1017/S0003055406062046. https://www.cambridge.org/core/journals/american-political-scien

ce-review/article/economic-backwardness-in-political-perspective/7DE0FEDD01FA04387AB1F4689CF7944B.

Adair, Steven, Sean Koessel, and Tom Lancaster. *The Nearest Neighbor Attack: How A Russian APT Weaponized Nearby Wi-Fi Networks for Covert Access* [in en-US], November 2024. https://www.volexity.com/blog/2024/11/22/the-nearest-neighbor-attack-how-a-russian-apt-weaponized-nearby-wi-fi-networks-for-covert-access/.

Adamsky, D. *The Russian Way of Deterrence: Strategic Culture, Coercion, and War', in The Russian Way of Deterrence* [in en]. Available at: 2023. https://doi.org/10.1515/9781503637832.. https://doi.org/10.1515/9781503637832..

Adner, R. "Ecosystem as Structure: An Actionable Construct for Strategy"' [in en]. Available at: *Journal of Management* 43, no. 1 (2017): 39–58. https://doi.org/10.1177/0149206316678451.. https://doi.org/10.1177/0149206316678451..

Ahmed, Ali, Amit Deokar, and Ho Cheung Brian Lee. "Vulnerability disclosure mechanisms: A synthesis and framework for market-based and non-market-based disclosures." *Decision Support Systems* 148 (September 2021): 113586. ISSN: 0167-9236. https://doi.org/10.1016/j.dss.2021.113586. https://www.sciencedirect.com/science/article/pii/S0167923621000968.

Allodi, Luca, Fabio Massacci, and Julian Williams. "The Work-Averse Cyberattacker Model: Theory and Evidence from Two Million Attack Signatures" [in en]. _Eprint: https://onlinelibrary.wiley.com/doi/pdf/10.1111/risa.13732,

Risk Analysis 42, no. 8 (2022): 1623–1642. ISSN: 1539-6924. https://doi.org/10.1111/risa.13732. https://onlinelibrary.wiley.com/doi/abs/10.1111/risa.13732.

Anxun and Chinese APT Activity - ReliaQuest. [in en]. Available at: 2024. https://www.reliaquest.com/blog/anxun-and-chinese-apt-activity/..

Axelrod, R., and W.D. Hamilton. "The Evolution of Cooperation" [in en]. *Science* 211, no. 4489 (1981): 1390–1396.

Aylett-Bullock, Joseph, Carolina Cuesta-Lazaro, Arnau Quera-Bofarull, Miguel Icaza-Lizaola, Aidan Sedgewick, Henry Truong, Aoife Curran, Edward Elliott, Tristan Caulfield, Kevin Fong, et al. "JUNE: open-source individual-based epidemiology simulation." *Royal Society open science* 8, no. 7 (2021): 210506.

Baldwin, David A. "Interdependence and power: a conceptual analysis." *International Organization* 34 (October 1980): 471–506. ISSN: 1531-5088, 0020-8183. https://doi.org/10.1017/S0020818300018828.

———. "Power Analysis and World Politics: New Trends versus Old Tendencies" [in en]. *World Politics* 31, no. 2 (January 1979): 161–194. ISSN: 1086-3338, 0043-8871, accessed October 30, 2024. https://doi.org/10.2307/2009941. https://www.cambridge.org/core/journals/world-politics/article/power-analysis-and-world-politics-new-trends-versus-old-tendencies/7B639F6FA5AA7F763D183E1626D91CBB.

Banks, William C. "Cyber Espionage and Electronic Surveillance: Beyond the Media Coverage The 2016 Randolph W. Thrower Symposium Re-

defined National Security Threats: Tensions and Legal Implications" [in eng]. *Emory Law Journal* 66, no. 3 (2016): 513–526. https://heinonline.org/HOL/P?h=hein.journals/emlj66&i=531.

Barnett, Michael, and Raymond Duvall. "Power in International Politics." Publisher: [MIT Press, University of Wisconsin Press, Cambridge University Press, International Organization Foundation], *International Organization* 59, no. 1 (2005): 39–75. ISSN: 0020-8183. https://www.jstor.org/stable/3877878.

Beauchamp-Mustafanga, Nathan. "Exploring Chinese Thinking on Deterrence in the Not-So-New Space and Cyber Domains | The National Bureau of Asian Research (NBR)" [in en]. In *Modernizing Deterrence: How China Coerces, Compels, and Deters*, edited by Roy D. Kamphausen. People's Liberation Army Conference. The National Bureau of Asian Research, February 2023. https://www.nbr.org/publication/exploring-chinese-thinking-on-deterrence-in-the-not-so-new-space-and-cyber-domains/.

Beckley, Michael. "The Power of Nations: Measuring What Matters." *International Security* 43, no. 2 (November 1, 2018): 7–44. ISSN: 0162-2889, accessed May 1, 2024. https://doi.org/10.1162/isec_a_00328. https://doi.org/10.1162/isec_a_00328.

Ben-Gad, M., and A. Finkelstein. "On Intelligence Equities"' [in en]. *Draft* 0, no. 9.1 (2022).

Bernsen, W. *Same Same, but Different, Margin Research* [in en]. Available at: 2024. https://margin.re/2024/02/same-same-but-different/.

Betz, D. "Cyberpower in Strategic Affairs: Neither Unthinkable nor Blessed"' [in en]. Available at: *Journal of Strategic Studies* 35, no. 5 (2012): 689–711. https://doi.org/10.1080/01402390.2012.706970.. https://doi.org/10.1080/01402390.2012.706970..

Black, Crofton, and Omer Benjakob. "How a Secretive Swiss Dealer Is Enabling Israeli Spy Firms" [in en]. *Haaretz*. https://www.haaretz.com/israel-news/security-aviation/2023-05-14/ty-article-magazine/.highlight/global-surveillance-the-secretive-swiss-dealer-enabling-israeli-spy-firms/00000188-0005-dc7e-a3fe-22cdf2900000.

Blagden, David. "Deterring Cyber Coercion: The Exaggerated Problem of Attribution." Publisher: Routledge _eprint: https://doi.org/10.1080/00396338.2020.1715072 *Survival* 62, no. 1 (January 2, 2020): 131–148. ISSN: 0039-6338. https://doi.org/10.1080/00396338.2020.1715072. https://doi.org/10.1080/00396338.2020.1715072.

Blanchard, Jean-Marc F., Edward D. Mansfield, and Norrin M. Ripsman. "The political economy of national security: Economic statecraft, interdependence, and international conflict." *Security Studies* 9, no. 1 (September 1999): 1–14. ISSN: 0963-6412, 1556-1852, accessed April 12, 2024. https://doi.org/10.1080/09636419908429393. http://www.tandfonline.com/doi/abs/10.1080/09636419908429393.

Borghard, Erica D., and Shawn W. Lonergan. "The Logic of Coercion in Cyberspace." *Security Studies* 26, no. 3 (2017): 452–481. https://doi.org/10.1080/09636412.2017.1306396. https://doi.org/10.1080/09636412.2017.1306396.

Bramoullé, Yann, and Rachel Kranton. "Public goods in networks." *Journal of Economic Theory* 135, no. 1 (2007): 478–494.

———. "Risk-sharing networks." *Journal of Economic Behavior & Organization* 64, nos. 3-4 (2007): 275–294.

Bramoullé, Yann, Rachel Kranton, and Martin D'amours. "Strategic interaction and networks." *The American Economic Review* 104, no. 3 (2014): 898–930.

Brazil, M. *Foreign Intelligence Hackers and Their Place in the PRC Intelligence Community, Jamestown* [in en]. Available at: March 2024. https://jamestown.org/program/foreign-intelligence-hackers-and-their-place-in-the-prc-intelligence-community/..

Broeders, D., L. Adamson, and R. Creemers. *Coalition of the Unwilling? Chinese and Russian Perspectives on Cyberspace'* [in en]. Available at: Rochester, NY, 2019. https://papers.ssrn.com/abstract=3493600.

Buchan, R., and I. Navarrete. "Cyber espionage and international law"" [in en]. In *Research Handbook on International Law and Cyberspace*, 231–252. Available at: Edward Elgar Publishing, 2021. https://www.elgaronline.com/edcollchap/edcoll/9781789904246/9781789904246.00021.xml..

Buchanan, B. "The Cybersecurity Dilemma: Network Intrusions" [in en]. In *Trust, and Fear in the International System, in King's*. College London, 2016.

———. *The Hacker and the State: Cyber Attacks and the New Normal of Geopolitics* [in en]. Available at: 2020. https://doi.org/10.2307/j.ctv3405w2m.. https://doi.org/10.2307/j.ctv3405w2m..

Buchanan, B., and F.S. Cunningham. *Preparing the Cyber Battlefield: Assessing a Novel Escalation Risk in a Sino-American Crisis* [in co]. Edited by Cyberspace, J.Shires Instability, R. Chesney, and M. Smeets. Edinburgh University Press, 2023.

Buchanan, Ben. "Strategic Espionage." In *The Hacker and the State*, 86–107. Cyber Attacks and the New Normal of Geopolitics. Harvard University Press, 2020. ISBN: 978-0-674-98755-5. https://doi.org/10.2307/j.ctv3405w2m.7. https://www.jstor.org/stable/j.ctv3405w2m.7.

Buchanan, Ben, and Fiona S. Cunningham. "Preparing the Cyber Battlefield: Assessing a Novel Escalation Risk in a Sino-American Crisis" [in English]. In *Cyberspace and Instability*, edited by James Shires, Robert Chesney, and Max Smeets. Accepted: 2023-04-12T05:30:58Z. Edinburgh University Press, 2023. https://library.oapen.org/handle/20.500.12657/62312.

Burns, William J. "Spycraft and Statecraft: Transforming the CIA for an Age of Competition Essays" [in eng]. *Foreign Affairs* 103, no. 2 (2024): 74–85. Accessed October 23, 2024. https://heinonline.org/HOL/P?h=hein.journals/fora103&i=284.

Cardon, E. "Fighting Alone is called Losing: The Unlearned Lessons of Fragmented Systems"' [in en]. *The Cyber Defense Review* 7, no. 1 (2022): 75–82.

Carr, M. "Public–private partnerships in national cyber-security strategies"' [in en]. *International Affairs (Royal Institute of International Affairs 1944* 92, no. 1 (2016): 43–62.

Cary, D., and K. Del Rosso. *Sleight of hand: How China weaponizes software vulnerabilities'* [in en]. Atlantic Council, 6 September. Available at: 2023. https://www.atlanticcouncil.org/in-depth-research-reports/report/sleight-of-hand-how-china-weaponizes-software-vulnerability/.

Caulfield, Tristan, Christos Ioannidis, and David Pym. "The U.S. Vulnerabilities Equities Process: An Economic Perspective" [in en]. In *Decision and Game Theory for Security*, edited by Stefan Rass, Bo An, Christopher Kiekintveld, Fei Fang, and Stefan Schauer, 131–150. Lecture Notes in Computer Science. Cham: Springer International Publishing, 2017. ISBN: 978-3-319-68711-7. https://doi.org/10.1007/978-3-319-68711-7_8.

Centre, UK National Cyber Security. *SVR cyber actors adapt tactics for initial cloud access* [in en]. https://www.ncsc.gov.uk/news/svr-cyber-actors-adapt-tactics-for-initial-cloud-access.

Cha, Victor D. "Collective Resilience: Deterring China's Weaponization of Economic Interdependence." *International Security* 48, no. 1 (July 1, 2023): 91–124. ISSN: 0162-2889. https://doi.org/10.1162/isec_a_00465. https://doi.org/10.1162/isec_a_00465.

Chen, L.S., and M.M. Evers. ""Wars without Gun Smoke": Global Supply Chains, Power Transitions, and Economic Statecraft"' [in en]. Available

at: *International Security* 48, no. 2 (2023): 164–204. https://doi.org/10.1162/isec_a_00473.. https://doi.org/10.1162/isec_a_00473..

Chengliang, L., W. Jie, and D. Debin. "The spatial domain and balance of power of China and the United States" [in en]. *Journal of Natural Resources* 35, no. 11 (2020): 2596–2612.

China orders government workers to stop using iPhones amid heightened tensions with US | South China Morning Post [in en].

Chuanying, L. "Forging Stability in Cyberspace" [in en]. In *Survival: Global Politics and Strategy*. 2020, Routledge. April 2020.

Cifci, H. *Comparison of National-Level Cybersecurity and Cyber Power Indices: A Conceptual Framework* [in en]. Available at: 2022. https://doi.org/10.21203/rs.3.rs-2159915/v1.. https://doi.org/10.21203/rs.3.rs-2159915/v1..

Clark, D.D. *Characterizing cyberspace: Past, present and future. Working Paper* [in en]. Available at: 2010. https://dspace.mit.edu/handle/1721.1/141692..

Cohen, J.E. "Cyberspace as/and Space"' [in en]. *Columbia Law Review* 107 (2007): 210.

Coppola, Michael. *Google: Stop Burning Counterterrorism Operations* [in en], June 2024. https://poppopret.org/2024/06/24/google-stop-burning-counterterrorism-operations/.

Cunningham, F.S. "Strategic Substitution: China's Search for Coercive Leverage in the Information Age"' [in en]. *International Security* 47, no. 1 (2022): 46–92.

Damm, J. "The Internet and the Fragmentation of Chinese Society"' [in en]. Available at: *Critical Asian Studies* 39, no. 2 (2007): 273–294. https://doi.org/10.1080/14672710701339485.. https://doi.org/10.1080/14672710701339485..

Deibert, Ronald J. "Subversion Inc: The Age of Private Espionage." Publisher: Johns Hopkins University Press, *Journal of Democracy* 33, no. 2 (2022): 28–44. ISSN: 1086-3214, accessed October 30, 2024. https://muse.jhu.edu/pub/1/article/852743.

Dellago, Matthias, Daniel W Woods, and Andrew C Simpson. "Characterising 0-Day Exploit Brokers" [in en]. In *21st Workshop on the Economics of Information Security*. June 2022.

Devanny, Joe, Ciaran Martin, and Tim Stevens. "On the strategic consequences of digital espionage." Publisher: Routledge _eprint: https://doi.org/10.1080/237388 *Journal of Cyber Policy* 6, no. 3 (September 2021): 429–450. ISSN: 2373-8871. https://doi.org/10.1080/23738871.2021.2000628. https://doi.org/10.1080/23738871.2021.2000628.

Drezner, Daniel W. *The Sanctions Paradox* [in fr]. Cambridge Books, Cambridge University Press, number 9780521644150. 1999.

Dunn Cavelty, M. "Europe's cyber-power"' [in en]. Available at: *European Politics and Society* 19, no. 3 (2018): 304–320. https://doi.org/10.

1080/23745118.2018.1430718.. https://doi.org/10.1080/23745118.2018.1430718..

Dunn Cavelty, M., and A. Wenger. "Cyber security meets security politics: Complex technology, fragmented politics, and networked science" [in en]. *Contemporary Security Policy* 41, no. 1 (2020): 5–32.

Elliott, Karen, Fabio Massacci, and Julian Williams. "Action, inaction, trust, and cybersecurity's common property problem." *IEEE Security & Privacy* 14, no. 1 (2016): 82–86.

Ellsberg, Daniel. "Risk, ambiguity, and the Savage axioms." *The quarterly journal of economics* 75, no. 4 (1961): 643–669.

———. *The doomsday machine: Confessions of a nuclear war planner*. Bloomsbury Publishing USA, 2017.

———. "The theory and practice of blackmail." *Lecture at the Lowell Institute, Boston, MA, March* 10 (1959).

Farrell, H., and A.L. Newman. "Of Privacy and Power: The Transatlantic Struggle over Freedom and Security"' [in en]. In *Of Privacy and Power*. Available at: Princeton University Press, 2019. https://doi.org/10.1515/9780691189956.. https://doi.org/10.1515/9780691189956..

———. "Weaponized Interdependence: How Global Economic Networks Shape State Coercion"' [in en]. Available at: *International Security* 44, no. 1 (2019): 42–79. https://doi.org/10.1162/isec_a_00351.. https://doi.org/10.1162/isec_a_00351..

Farrell, Henry, and Abraham L. Newman. "Weaponized Interdependence: How Global Economic Networks Shape State Coercion." *International Security* 44, no. 1 (July 1, 2019): 42–79. ISSN: 0162-2889, accessed July 17, 2023. https://doi.org/10.1162/isec_a_00351. https://doi.org/10.1162/isec_a_00351.

Fenghua, P., L. Zhiyong, and G. Yuejing. "Analysis of China's surrounding geopolitical environment from the perspective of economy and trade: Based on social network analysis[J" [in en]. *Geographical Research* 34, no. 4 (2015): 775–786.

Fick, N. "Confronting Reality in Cyberspace: Foreign Policy for a Fragmented Internet" [in en]. Available at: *Council on Foreign Relations*, 2022. https://www.jstor.org/stable/resrep42123..

Forsyth, J.W., and B.E. Pope. "Structural Causes and Cyber Effects: Why International Order is Inevitable in Cyberspace"' [in en]. *Strategic Studies Quarterly* 8, no. 4 (2014): 112–128.

Fujino, I. *Huawei breaks free from Google ecosystem with homegrown OS, Nikkei Asia* [in en]. Available at: 2024. https://asia.nikkei.com/Business/China-tech/Huawei-breaks-free-from-Google-ecosystem-with-homegrown-OS..

Gartzke, E., and J.R. Lindsay. "Weaving Tangled Webs: Offense, Defense, and Deception in Cyberspace"' [in en]. Available at: *Security Studies* 24, no. 2 (2015): 316–348. https://doi.org/10.1080/09636412.2015.1038188.. https://doi.org/10.1080/09636412.2015.1038188..

Gilli, Andrea, and Mauro Gilli. "Why China Has Not Caught Up Yet: Military-Technological Superiority and the Limits of Imitation, Reverse Engineering, and Cyber Espionage." *International Security* 43, no. 3 (February 2019): 141–189. ISSN: 0162-2889. https://doi.org/10.1162/isec_a_00337. https://doi.org/10.1162/isec_a_00337.

Gioe, David V, and Margaret W Smith. *Great Power Cyber Competition: Competing and Winning in the Information Environment*. Taylor & Francis, 2024.

Global Research and Analysis Team, Kaspersky Inc. *Equation: The Death Star of Malware Galaxy* [in en-US], February 2015. https://securelist.com/equation-the-death-star-of-malware-galaxy/68750/.

Buying Spying: How the commercial surveillance industry works and what can be done about it [in en-us], February 2024. https://blog.google/threat-analysis-group/commercial-surveillance-vendors-google-tag-report/.

Group, Insikt. *Charting China's Climb as a Leading Global Cyber Power'* [in en]. Recorded Futures. Available at: 2023. https://www.recordedfuture.com/charting-chinas-climb-leading-global-cyber-power.

Grzegorzewski, M., and C. Marsh. "A Strategic Cyberspace Overview: Russia and China"' [in en]. In *Great Power Cyber Competition*. Routledge, 2024.

Guzzini, Stefano. "Structural power: the limits of neorealist power analysis." *International Organization* 47, no. 3 (1993): 443–478. https://doi.org/10.1017/S0020818300028022.

Harknett, R.J., and M. Smeets. "Cyber campaigns and strategic outcomes" [in en]. *Journal of Strategic Studies* 45, no. 4 (2022): 534–567.

Harnisch, Sebastian, and Kerstin Zettl-Schabath. "Secrecy and Norm Emergence in Cyber-Space. The US, China and Russia Interaction and the Governance of Cyber-Espionage." Publisher: Routledge _eprint: https://doi.org/10.1080/17419166.2022.2097074, *Democracy and Security* 19, no. 1 (January 2, 2023): 82–110. ISSN: 1741-9166. https://doi.org/10.1080/17419166.2022.2097074. https://doi.org/10.1080/17419166.2022.2097074.

Hart, Jeffrey. "Three Approaches to the Measurement of Power in International Relations." *International Organization* 30, no. 2 (April 1976): 289–305. ISSN: 1531-5088, 0020-8183. https://doi.org/10.1017/S0020818300018282. https://www.cambridge.org/core/journals/international-organization/article/abs/three-approaches-to-the-measurement-of-power-in-international-relations/F4D580931E934A85351E9406832D354C.

Harvey, C.J., and C.L. Moore. "Cyber statecraft by net states: the case of Meta, 2016–2021"' [in en]. Available at: *Journal of Cyber Policy* 0, no. 0 (2023): 1–21. https://doi.org/10.1080/23738871.2023.2249008.. https://doi.org/10.1080/23738871.2023.2249008..

Haslam, Jonathan. *Near and Distant Neighbors: A New History of Soviet Intelligence*. Macmillan, 2015.

Healey, J., and R. Jervis. *The Escalation Inversion and Other Oddities of Situational Cyber Stability* [in en]. Edited by Cyberspace, J.Shires Instability, R. Chesney, and M. Smeets. Edinburgh University Press, 2023.

Heidger, T., and D. Higgins. "In Africa, Great Power Competition Requires a Great Strategy for Information Operations" [in en]. In *Great Power Cyber Competition. 2024*. Routledge.

Hilbe, Christian, Štěpán Šimsa, Krishnendu Chatterjee, and Martin A Nowak. "Evolution of cooperation in stochastic games." *Nature* 559, no. 7713 (2018): 246–249.

Hoffmann, S., D. Lazanski, and E. Taylor. "Standardising the splinternet: how China's technical standards could fragment the internet" [in en]. *Journal of Cyber Policy* 5, no. 2 (2020): 239–264.

Hofmann, S.C., and P. Pawlak. "Governing cyberspace: policy boundary politics across organizations"' [in en]. *Review of International Political Economy* 30, no. 6 (2023): 2122–2149.

Holland, J., and E. Staunton. ""BrOthers in Arms": France, the Anglosphere and AUKUS"' [in en]. Available at: *International Affairs* 100, no. 2 (2024): 712–729. https://doi.org/10.1093/ia/iiae016.. https://doi.org/10.1093/ia/iiae016..

Houghton, J. and Siegel, M. "Advancing Cybersecurity Using System Dynamics Simulation Modeling for Analysing and Disrupting Cybercrime Ecosystem and Vulnerability Markets" [in en]. Interdisciplinary Consortium for Improving Critical Infrastructure Cybersecurity. MIT Sloan School of Management, 2014.

Householder, Allen D., Jeff Chrabaszcz, Trent Novelly, David Warren, and Jonathan M. Spring. "Historical Analysis of Exploit Availability Timelines" [in en]. 2020. https://www.usenix.org/conference/cset20/presentation/householder.

Huang, Yuxing. *China's Asymmetric Statecraft: Alignments, Competitors, and Regional Diplomacy*. UBC Press, February 15, 2023. ISBN: 978-0-7748-6814-3. Google Books: xCSpEAAAQBAJ.

Huang, Z., and Y. Ying. "Chinese approaches to cyberspace governance and international law in cyberspace" [in en]. In *Research Handbook on International Law and Cyberspace*, 547–563. Edward Elgar Publishing, 2021.

Iii, E Lincoln Bonner. "Cyber Power in 21st-Century Joint Warfare," 2014.

Imhof, Lorens A, Drew Fudenberg, and Martin A Nowak. "Evolutionary cycles of cooperation and defection." *Proceedings of the National Academy of Sciences* 102, no. 31 (2005): 10797–10800.

"A historical review of cyber attacks by US intelligence agencies - based on information disclosed by the global cybersecurity community" [in en]. *Industrial Information Security* 2023, no. 2, 87–93.

Inkster, N. "Measuring Military Cyber Power"' [in en]. Available at: *Survival* 59, no. 4 (2017): 27–34. https://doi.org/10.1080/00396338.2017.1349770.. https://doi.org/10.1080/00396338.2017.1349770..

———. "Power Versus Pragmatism: Unlearned Lessons in Dealing with China"' [in en]. *The Cyber Defense Review* 7, no. 1 (2022): 41–50.

Ioannidis, Christos, David Pym, Julian Williams, and Iffat Gheyas. "Resilience in information stewardship." *European journal of operational research* 274, no. 2 (2019): 638–653.

Jackson, Matthew O, and Yves Zenou. "Games on networks." In *Handbook of game theory with economic applications*, 4:95–163. Elsevier, 2015.

Jensen, B. "The Cyber Character of Political Warfare"' [in en]. *The Brown Journal of World Affairs* 24, no. 1 (2017): 159–172.

Jiang, Y. *Cyber-Nationalism in China. Challenging Western media portrayals of internet censorship in China* [in en]. Available at: 2012. https://doi.org/10.1017/9780987171894.. https://doi.org/10.1017/9780987171894..

Jianwei, Zhuge, Gu Lion, Duan Haixin, and Taylor Roberts. "Investigating the Chinese Online Underground Economy." In *China and Cybersecurity: Espionage, Strategy, and Politics in the Digital Domain*, edited by Jon R. Lindsay, Tai Ming Cheung, and Derek S. Reveron, 0. Oxford University Press, May 2015. ISBN: 978-0-19-020126-5. https://doi.org/10.1093/acprof:oso/9780190201265.003.0004. https://doi.org/10.1093/acprof:oso/9780190201265.003.0004.

Jie, Z., L. Yanhua, and H. Zhichao. "A Brief Analysis of the UK's Cyber Warfare Force" [in en]. *Information Security and Communications Privacy* 2021, no. 4, 1–8.

Joint Cybersecurity Advisory: People's Republic of China State-Sponsored Cyber Actor Living off the Land to Evade Detection. Technical report Ver 1.1. Five Eyes, June 2023. Accessed July 17, 2023. https://media.defense.gov/2023/May/24/2003229517/-1/-1/0/CSA_PRC_State_Sponsored_Cyber_Living_off_the_Land_v1.1.PDF.

Kaminska, Monica. "Restraint under conditions of uncertainty: Why the United States tolerates cyberattacks" [in en]. *Journal of Cybersecurity* 7, no. 1 (February 2021): tyab008. ISSN: 2057-2085, 2057-2093. https://doi.org/10.1093/cybsec/tyab008. https://academic.oup.com/cybersecurity/article/doi/10.1093/cybsec/tyab008/6162971.

Kello, L. "The Meaning of the Cyber Revolution: Perils to Theory and Statecraft"' [in en]. Available at: *International Security* 38, no. 2 (2013): 7–40. https://doi.org/10.1162/ISEC_a_00138.. https://doi.org/10.1162/ISEC_a_00138..

Klimburg, A., and L. Faesen. "A Balance of Power in Cyberspace" [in en]. In *Governing Cyberspace: Behavior, Power and Diplomacy*, edited by D. Broeders and Bvd Berg. Rowman & Littlefield, 2020.

Klimburg, Alexander. "Mobilising Cyber Power." *Survival* 53, no. 1 (February 1, 2011): 41–60. ISSN: 0039-6338, accessed October 20, 2023. https://doi.org/10.1080/00396338.2011.555595. https://doi.org/10.1080/00396338.2011.555595.

Korczynski, M. "The Political Economy of Trust"' [in en]. Available at: *Journal of Management Studies* 37, no. 1 (2000). https://doi.org/10.1111/1467-6486.00170.. https://doi.org/10.1111/1467-6486.00170..

Kot, S.F., and Brian. *Why Does the Global Spyware Industry Continue to Thrive? Trends, Explanations, and Responses, Carnegie Endowment for International Peace* [in en]. Available at: 2023. https://carnegieendowment.org/2023/03/14/why-does-global-spyware-industry-continue-to-thrive-trends-explanations-and-responses-pub-89229.

Krahmann, Elke. "Private Military and Security Companies, Territoriality and the Transformation of Western Security Governance" [in en]. In *The Diffusion of Power in Global Governance: International Political Economy Meets Foucault*, edited by Stefano Guzzini and Iver B. Neumann, 38–70. London: Palgrave Macmillan UK, 2012. ISBN: 978-1-137-28355-9, accessed October 29, 2024. https://doi.org/10.1057/9781137283559_2. https://doi.org/10.1057/9781137283559_2.

Kramer, F.D., S.H. Starr, and L.K. Wentz, eds. *Cyberpower and National Security* [in en]. Available at: 2011. https://doi.org/10.2307/j.ctt1djmhj1.. https://doi.org/10.2307/j.ctt1djmhj1..

Kuehl, Daniel T. "From Cyberspace to Cyberpower: Defining the Problem" [in en]. In *Cyberpower and National Security*, edited by Franklin D. Kramer, Stuart H. Starr, and Larry K. Wentz. University of Nebraska Press, March 2011. ISBN: 978-1-59797-933-7 978-1-59797-423-3. https://doi.org/10.2307/j.ctt1djmhj1. http://www.jstor.org/stable/10.2307/j.ctt1djmhj1.

Kuehl, Starr, and Nye.

Kuper, Gabriel, Fabio Massacci, Woohyun Shim, and Julian Williams. "Who should pay for interdependent risk? Policy implications for security interdependence among airports." *Risk Analysis* 40, no. 5 (2020): 1001–1019.

Kuznetsov, Igor, Valentin Pashkov, and Leonid Bezvershenko. *Operation Triangulation: iOS devices targeted with previously unknown malware*. Technical report. Kaspersky, Inc. https://securelist.com/operation-triangulation/109842/.

Kydd, Andrew H. *Trust and Mistrust in International Relations*. Princeton University Press, June 5, 2018. ISBN: 978-0-691-18851-5. https://doi.org/10.1515/9780691188515. https://www.degruyter.com/document/doi/10.1515/9780691188515/html.

Lambach, Daniel. "The Territorialization of Cyberspace*." *International Studies Review* 22, no. 3 (September 1, 2020): 482–506. ISSN: 1521-9488, 1468-2486. https://doi.org/10.1093/isr/viz022. https://academic.oup.com/isr/article/22/3/482/5488469.

Lan, T. "US Department of Defense 2023 Cyber Strategy Perspective" [in en]. *China Information Security* 2024, no. 1, 85–88.

Langner, Ralph. "Cyber Power: An Emerging Factor in National and International Security." *Horizons: Journal of International Relations and Sustainable Development*, no. 8 (2016): 206–218. ISSN: 2406-0402, ac-

cessed October 20, 2023. JSTOR: 48573698. https://www.jstor.org/stable/48573698.

Le Thu, H. "China's dual strategy of coercion and inducement towards ASEAN" [in en]. *The Pacific Review* 32, no. 1 (2019): 20–36.

Lecigne, Clement, and Maddie Stone. *Active North Korean campaign targeting security researchers*, 2023. https://blog.google/threat-analysis-group/active-north-korean-campaign-targeting-security-researchers/.

Lemay, A. "Survey of publicly available reports on advanced persistent threat actors"' [in en]. Available at: *Computers & Security* 72 (2018): 26–59. https://doi.org/10.1016/j.cose.2017.08.005.. https://doi.org/10.1016/j.cose.2017.08.005..

Leonard, T.G.A., Ivan Krastev, and Mark. *Living in an à la carte world: What European policymakers should learn from global public opinion, ECFR* [in en]. Available at: 2023. https://ecfr.eu/publication/living-in-an-a-la-carte-world-what-european-policymakers-should-learn-from-global-public-opinion/..

Lessig, L. "The Zones of Cyberspace"' [in en]. Available at: *Stanford Law Review* 48, no. 5 (1996): 1403–1411. https://doi.org/10.2307/1229391.. https://doi.org/10.2307/1229391..

Levi, M., and L. Stoker. "Political Trust and Trustworthiness"' [in en]. Available at: *Annual Review of Political Science* 3 (2000): 475–507. https://doi.org/10.1146/annurev.polisci.3.1.475.. https://doi.org/10.1146/annurev.polisci.3.1.475..

Levy, I. *Equities Process'* [in en]. Available at, 2018. https://www.ncsc.gov.uk/blog-post/equities-process.

Li, Y., and Z. Xiuzan. "China's solution to "ideological governance" of global cyberspace" [in en]. *Journal of Zhengzhou University (Philosophy and Social Sciences Edition* 51, no. 1 (2018): 70–75.

Libicki, Martin. "The coming of cyber espionage norms." In *2017 9th International Conference on Cyber Conflict (CyCon)*, 1–17. ISSN: 2325-5374. May 2017. https://doi.org/10.23919/CYCON.2017.8240325. https://ieeexplore.ieee.org/abstract/document/8240325.

Lin, Herbert S. "Offensive Cyber Operations and the Use of Force." *Journal of National Security Law & Policy* 4 (2010): 63. https://heinonline.org/HOL/Page?handle=hein.journals/jnatselp4&id=65&div=&collection=.

Lind, Jennifer. "Back to Bipolarity: How China's Rise Transformed the Balance of Power." _Eprint: https://direct.mit.edu/isec/article-pdf/49/2/7/2479270/isec_a_0 *International Security* 49, no. 2 (October 2024): 7–55. ISSN: 0162-2889. https://doi.org/10.1162/isec_a_00494. https://doi.org/10.1162/isec%5C_a%5C_00494.

Lindsay, J.R. "Cyber Espionage"' [in en]. In *The Oxford Handbook of Cyber Security*, edited by P. Cornish, 0. Available at: Oxford University Press, 2021. https://doi.org/10.1093/oxfordhb/9780198800682.013.12.. https://doi.org/10.1093/oxfordhb/9780198800682.013.12..

———. "Restrained by design: the political economy of cybersecurity"' [in en]. Available at: *Digital Policy, Regulation and Governance* 19, no. 6 (2017): 493–514. https://doi.org/10.1108/DPRG-05-2017-0023.. https://doi.org/10.1108/DPRG-05-2017-0023..

Lindsay, Jon, and Erik Gartzke. "Coercion through Cyberspace: The Stability-Instability Paradox Revisited." In *The Power to Hurt: Coercion in Theory and in Practice*. (Oxford University Press, Forthcoming), August 25, 2016.

Lindsay, Jon R., and Tai Ming Cheung. "From Exploitation to Innovation: Acquisition, Absorption, and Application." In *China and Cybersecurity: Espionage, Strategy, and Politics in the Digital Domain*, edited by Jon R. Lindsay, Tai Ming Cheung, and Derek S. Reveron, 0. Oxford University Press, May 2015. ISBN: 978-0-19-020126-5. https://doi.org/10.1093/acprof:oso/9780190201265.003.0003. https://doi.org/10.1093/acprof:oso/9780190201265.003.0003.

Lonergan, S.W. "Cyber Operations, Accommodative Signaling, and the De-Escalation of International Crises"' [in en], edited by E.D. Lonergan. Available at: *Security Studies* 31, no. 1 (2022): 32–64. https://doi.org/10.1080/09636412.2022.2040584.. https://doi.org/10.1080/09636412.2022.2040584..

Malkasian, C. *America's Crisis of Deterrence, in Foreign Affairs* [in en], 2024.

Manantan, M.B. "The People's Republic of China's Cyber Coercion: Taiwan, Hong Kong, and the South China Sea"' [in en]. Available at:

Issues & Studies 56, no. 03 (2020): 2040013. https://doi.org/10.1142/S1013251120400135.. https://doi.org/10.1142/S1013251120400135..

Marczak, Bill. *Triangulation: Did "the NSA" fail to learn the lessons of NSO?* [In en], June 2023. https://medium.com/@billmarczak/triangulation-did-the-nsa-fail-to-learn-the-lessons-of-nso-5f36d251d02e.

Massacci, Fabio, Raminder Ruprai, Matthew Collinson, and Julian Williams. "Economic impacts of rules-versus risk-based cybersecurity regulations for critical infrastructure providers." *IEEE Security & Privacy* 14, no. 3 (2016): 52–60.

Masuda, Naoki, and Renaud Lambiotte. *A guide to temporal networks.* World Scientific, 2016.

Mattila, J.K. "A Model for State Cyber Power: Case Study of Russian Behaviour"' [in en]. Available at: *European Conference on Cyber Warfare and Security* 21, no. 1 (2022): 188–197. https://doi.org/10.34190/eccws.21.1.207.. https://doi.org/10.34190/eccws.21.1.207..

Maurer, T. *Cyber Mercenaries* [in nl]. Cambridge University Press, 2018.

McMillan, Dustin Volz, Robert, Sarah Krouse, Aruna Viswanatha. *Exclusive | U.S. Wiretap Systems Targeted in China-Linked Hack* [in en-US]. Section: Politics, October 2024. https://www.wsj.com/tech/cybersecurity/u-s-wiretap-systems-targeted-in-china-linked-hack-327fc63b.

Mearsheimer, John J. "Structural realism." *International relations theories: Discipline and diversity* 83 (2007): 77–94.

Miller, Seumas. "Cyberattacks and "Dirty Hands": Cyberwar, Cybercrime, or Covert Political Action?" In *Binary Bullets: The Ethics of Cyberwarfare*, edited by Fritz Allhoff, Adam Henschke, and Bradley Jay Strawser, 0. Oxford University Press, March 2016. ISBN: 978-0-19-022107-2. https://doi.org/10.1093/acprof:oso/9780190221072.003.0012. https://doi.org/10.1093/acprof:oso/9780190221072.003.0012.

Moussouris, Katie, and Michael Siegel. "The Wolves of Vuln Street:" [in en]. 2015.

Mueller, G.B. *Cyber Operations during the Russo-Ukrainian War'* [in en]. Available at: 2023. https://www.csis.org/analysis/cyber-operations-during-russo-ukrainian-war.

Mueller, M. *Will the Internet Fragment?: Sovereignty, Globalization and Cyberspace* [in en]. John Wiley & Sons, 2017.

Nash, John F, et al. "Equilibrium Points in N-person Games." *Proceedings of the National Academy of Sciences* 36, no. 1 (1950): 48–49.

Nedic, Angelia, and Asuman Ozdaglar. "Distributed subgradient methods for multi-agent optimization." *IEEE Transactions on Automatic Control* 54, no. 1 (2009): 48–61.

Ningnan, Z. "US Cybersecurity Situation Overview" [in en]. *China Information Security* 2024, no. 1 (2023): 60–64.

Norris, W.J. *Chinese Economic Statecraft: Commercial Actors, Grand Strategy, and State Control* [in en]. Available at: 2016. https://www.jstor.org/stable/10.7591/j.ctt18kr4kx..

Nouwens, M. *China's new Information Support Force, IISS* [in en]. Available at: 2024. https://www.iiss.org/online-analysis/online-analysis/2024/05/chinas-new-information-support-force/.

Nowak, Martin A. "Five rules for the evolution of cooperation." *science* 314, no. 5805 (2006): 1560–1563.

Nowak, Martin A, and Karl Sigmund. "Evolution of indirect reciprocity." *Nature* 437, no. 7063 (2005): 1291–1298.

Nye, J. "The End of Cyber-Anarchy? How to Build a New Digital Order."' [in en]. *Foreign Affairs* 101, no. 1 (2022): 32–42.

Nye, J.S., and Cyber power. [in en]. Harvard Kennedy School, Belfer Center for Science / International Affairs, 2010.

Nye, Joseph S. *Cyber Power*. Harvard Kennedy School, Belfer Center for Science and International Affairs ..., 2010. http://pakistanhouse.net/wp-content/uploads/2016/11/Cyber-security.pdf.

Nye, Joseph S., Jr. "Deterrence and Dissuasion in Cyberspace." *International Security* 41, no. 3 (January 2017): 44–71. ISSN: 0162-2889. https://doi.org/10.1162/ISEC_a_00266. https://doi.org/10.1162/ISEC_a_00266.

O'Brien, Robert, and Marc Williams. *Global Political Economy: Evolution and Dynamics* [in en]. Google-Books-ID: 37soEQAAQBAJ. Bloomsbury Publishing, October 2024. ISBN: 978-1-350-34787-8.

Oatley, T. "Toward a political economy of complex interdependence"' [in en]. Available at: *European Journal of International Relations* 25, no. 4 (2019): 957–978. https://doi.org/10.1177/1354066119846553.. https://doi.org/10.1177/1354066119846553..

Ottis, R., and P. Lorents. "Cyberspace: Definition and Implications"' [in en]. In *in. International Conference on Information Warfare and Security*. 2010.

Pauly, Reid B. C. "Damned If They Do, Damned If They Don't: The Assurance Dilemma in International Coercion." *International Security* 49, no. 1 (July 2024): 91–132. ISSN: 0162-2889. https://doi.org/10.1162/isec_a_00488. https://doi.org/10.1162/isec_a_00488.

Peixoto, Tiago P, and Martin Rosvall. "Modelling sequences and temporal networks with dynamic community structures." *Nature communications* 8, no. 1 (2017): 582.

Ping, L. "From the Russian-Ukrainian conflict to the trend of cyberspace weaponization and its impact" [in en]. *China Information Security* 2022, no. 6, 65–69.

Post, D.G. "Anarchy State and the Internet" [in en]. *Journal of Online Law, Article* 3 (1995).

Powers, S.M., and M. Jablonski. *The Real Cyber War: The Political Economy of Internet Freedom* [in en]. University of Illinois Press, 2015.

Pym, David J. "The Origins of Cyberspace." In *The Oxford Handbook of Cyber Security*, edited by Paul Cornish, 0. Oxford University Press,

November 2021. ISBN: 978-0-19-880068-2. https://doi.org/10.1093/oxfordhb/9780198800682.013.1. https://doi.org/10.1093/oxfordhb/9780198800682.013.1.

Quinn, J. "A Peek over the Great Firewall: A Breakdown of China's New Cybersecurity Law" [in en]. *SMU Science and Technology Law Review* 20 (2017): 407.

"Office of the Director of National Intelligence, 'US-Backed International Norms Increasingly Contested'" [in en]. Available at: *Report October*, 2022. https://www.dni.gov/files/images/globalTrends/GT2040/NIC-2021-02491_GT_Future_of_Int_Norms_22Mar22_UNSOURCED.pdf.

Responsible Cyber Power in Practice (HTML) - GOV.UK, April 2023. https://www.gov.uk/government/publications/responsible-cyber-power-in-practice/responsible-cyber-power-in-practice-html.

Rid, T. *Cyber War Will Not Take Place* [in en]. Oxford, UNITED STATES: Oxford University Press, Incorporated.(Accessed, 2013.

Riecke, Lena. "Unmasking the Term 'Dual Use' in EU Spyware Export Control." *European Journal of International Law* 34, no. 3 (August 2023): 697–720. ISSN: 0938-5428. https://doi.org/10.1093/ejil/chad039. https://doi.org/10.1093/ejil/chad039.

Robertson, J., and M. Riley. "China Used a Tiny Chip in a Hack That Infiltrated U.S" [in en]. *Companies, in Bloomberg.com*, 2018.

Rochberger, Lior, and Daniel Frank. *Operation Diplomatic Specter: An Active Chinese Cyberespionage Campaign Leverages Rare Tool Set to Target Governmental Entities in the Middle East, Africa and Asia.* Accessed October 30, 2024. https://unit42.paloaltonetworks.com/operation-diplomatic-specter/.

Rosen, J Ben. "Existence and uniqueness of equilibrium points for concave n-person games." *Econometrica: Journal of the Econometric Society*, 1965, 520–534.

Roumani, Yaman. "Patching zero-day vulnerabilities: an empirical analysis." *Journal of Cybersecurity* 7, no. 1 (January 2021): tyab023. ISSN: 2057-2085. https://doi.org/10.1093/cybsec/tyab023. https://doi.org/10.1093/cybsec/tyab023.

Rowland, J., M. Rice, and S. Shenoi. "The anatomy of a cyber power"' [in en]. Available at: *International Journal of Critical Infrastructure Protection* 7, no. 1 (2014): 3–11. https://doi.org/10.1016/j.ijcip.2014.01.001.. https://doi.org/10.1016/j.ijcip.2014.01.001..

Rugge, F. *Confronting an "Axis of Cyber"?: China, Iran, North Korea, Russia in Cyberspace* [in en], 2018.

Ruhl, C. *Cyberspace and Geopolitics* [in en].

Safdari, Hadiseh, Martina Contisciani, and Caterina De Bacco. "Reciprocity, community detection, and link prediction in dynamic networks." *Journal of Physics: Complexity* 3, no. 1 (2022): 015010.

Schmitt, M.N. "Cyber operations not per se regulated by international law" [in en]. In *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, 2017:168–176. Cambridge University Press.

Schneider, Fred, ed. *Trust in Cyberspace* [in en]. National Research Council. Google-Books-ID: mAslCrFPwAIC. National Academies Press, January 1999. ISBN: 978-0-309-06558-0.

Segal, A. *Huawei, 5G, and Weaponized Interdependence'* [in en]. Edited by D.W. Drezner, H. Farrell, and A.L. Newman. Available at: 2021. https://www.jstor.org/stable/10.7864/j.ctv11sn64z.10.

Shandler, Ryan, and Miguel Alberto Gomez. "The hidden threat of cyber-attacks – undermining public confidence in government." Publisher: Routledge _eprint: https://doi.org/10.1080/19331681.2022.2112796, *Journal of Information Technology & Politics* 20, no. 4 (October 2023): 359–374. ISSN: 1933-1681. https://doi.org/10.1080/19331681.2022.2112796. https://doi.org/10.1080/19331681.2022.2112796.

Sheldon, Robert, and Joe McReynolds. "Civil-Military Integration and Cybersecurity: A Study of Chinese Information Warfare Militias." In *China and Cybersecurity: Espionage, Strategy, and Politics in the Digital Domain*, edited by Jon R. Lindsay, Tai Ming Cheung, and Derek S. Reveron, 0. Oxford University Press, May 1, 2015. ISBN: 978-0-19-020126-5, accessed July 17, 2023. https://doi.org/10.1093/acprof:oso/9780190201265.003.0008. https://doi.org/10.1093/acprof:oso/9780190201265.003.0008.

Shu, L. "Internet extreme risk prevention and great power game" [in en]. *Journal of Tongji University (Social Science Edition* 33, no. 4 (2022): 48–57.

Shwartz, Maor. *The boom, the bust and the adjust* [in en], June 2023. https://medium.com/@maor_s/the-boom-the-bust-and-the-adjust-ea443a120c6.

———. "The Boom, the Bust and the Adjust." Medium, June 20, 2023. https://medium.com/@maor_s/the-boom-the-bust-and-the-adjust-ea443a120c6.

Simmons, Beth A., and Zachary Elkins. "The Globalization of Liberalization: Policy Diffusion in the International Political Economy" [in en]. *American Political Science Review* 98, no. 1 (February 2004): 171–189. ISSN: 1537-5943, 0003-0554, accessed October 22, 2024. https://doi.org/10.1017/S0003055404001078. https://www.cambridge.org/core/journals/american-political-science-review/article/abs/globalization-of-liberalization-policy-diffusion-in-the-international-political-economy/B5221E84026490BEAD28085A42D636C0.

Simon, Herbert A. "Notes on the Observation and Measurement of Political Power." *The Journal of Politics* 15, no. 4 (November 1953): 500–516. ISSN: 0022-3816. https://doi.org/10.2307/2126538. https://www.journals.uchicago.edu/doi/abs/10.2307/2126538.

Singh, Pukhraj. "China's Military Cyber Operations" [in en].

Smeets, M. "A matter of time: On the transitory nature of cyberweapons"' [in en]. Available at: *Journal of Strategic Studies* 41, no. 1–2 (2018): 6–32. https://doi.org/10.1080/01402390.2017.1288107.. https://doi.org/10.1080/01402390.2017.1288107..

Soesanto, Teodora Delcheva, Yasser El-Shimy, and Jennie Bradley Stefan. *Time to talk: Europe and the Vulnerability Equities Process* [in en-GB], March 2018. https://ecfr.eu/article/commentary_time_to_talk_europe_and_the_vulnerability_equities_process/.

Starr, Stuart H. "Towards an Evolving Theory of Cyberpower." In *The Virtual Battlefield: Perspectives on Cyber Warfare*, 18–52. IOS Press, 2009. https://doi.org/10.3233/978-1-60750-060-5-18. https://ebooks.iospress.nl/doi/10.3233/978-1-60750-060-5-18.

Stiennon, D Hodges, R., S Creese, G Neil, S.V. Stevenage, S. Black, H Meadows, S Creese, D Hodges, H. He, and W Pike. *Cyber Warfare: A Multidisciplinary Analysis*. 8:1210–1213. IEEE Computer Society, 2013.

Stolyarov, Vlad, and Dan Black. *Virus Bulletin :: Cybercrime turned cyber espionage: the many faces of the RomCom group*. Accessed October 30, 2024. https://www.virusbulletin.com/conference/vb2024/abstracts/cybercrime-turned-cyber-espionage-many-faces-romcom-group/.

Team, N. "i-SOON: Another Company in the APT41 Network"' [in en]. Available at: *Natto Thoughts*, 2023. https://nattothoughts.substack.com/p/i-soon-another-company-in-the-apt41.

The Chinese Communist Party's Military-Civil Fusion Policy [in en-US]. Technical report. US Department of State. https://2017-2021.state.gov/military-civil-fusion/.

Thompson, A. "Buying Silence: The Price of Internet Censorship in China"' [in en]. Available at: *Center for Security and Emerging Technology*, 2021. https://cset.georgetown.edu/article/buying-silence-the-price-of-internet-censorship-in-china/..

Thurner, Paul W., Christian S. Schmid, Skyler J. Cranmer, and Göran Kauermann. "Network Interdependencies and the Evolution of the International Arms Trade" [in en]. Publisher: SAGE Publications Inc, *Journal of Conflict Resolution* 63, no. 7 (August 2019): 1736–1764. ISSN: 0022-0027. https://doi.org/10.1177/0022002718801965. https://doi.org/10.1177/0022002718801965.

Tucker, David. "The End of Intelligence: Espionage and State Power in the Information Age" [in en]. In *The End of Intelligence*. Stanford University Press, August 2014. ISBN: 978-0-8047-9269-1. https://doi.org/10.1515/9780804792691. https://www.degruyter.com/document/doi/10.1515/9780804792691/html.

Tusikov, N. "Internet Platforms Weaponizing Chokepoints" [in en]. In *The Uses and Abuses of Weaponized Interdependence*, edited by D. Drezner, H. Farrell, and A. Newman, 133–148. Washington, DC: Brookings Institute Press, 2021.

"Data From Chinese Security Services Company i-Soon Linked to Previous Chinese APT Campaigns"' [in en]. 24 February. Available at: *Unit* 42 (2024). https://unit42.paloaltonetworks.com/i-soon-data-leaks/..

Valeriano, B. *Cyber Coercion as a Combined Strategy', in Cyber Strategy: The Evolving Character of Power and Coercion* [in en]. Edited by B. Valeriano, B. Jensen, and R.C. Maness. 0. Oxford University Press, 2018.

Valeriano, Brandon. "Cyber Coercion as a Combined Strategy." In *Cyber Strategy: The Evolving Character of Power and Coercion*, edited by Brandon Valeriano, Benjamin Jensen, and Ryan C. Maness, 0. Oxford University Press, May 15, 2018. ISBN: 978-0-19-061809-4. https://doi.org/10.1093/oso/9780190618094.003.0004. https://doi.org/10.1093/oso/9780190618094.003.0004.

Voo, J. *National Cyber Power Index 2020: Methodology and Analytical Considerations'* [in en]. Technical report. China Cyber Policy Initiative Reports [Preprint]. Available at: 2020. https://dash.harvard.edu/handle/1/37372389.

Waltz, K.N. "Structural Realism after the Cold War"' [in en]. *International Security* 25, no. 1 (2000): 5–41.

Wolff, J. "The role of insurers in shaping international cyber-security norms about cyber-war" [in en]. *Contemporary Security Policy* 45, no. 1 (2024): 141–170.

Wu, Xiangyu. "Essays on the economics of networks." PhD diss., Durham University, August 2022.

Wumei, D. *Current Status of US Cyberspace Combat Forces* [in en]. 44:92–103. National Defense Science / Technology, 2023.

Xiaohong, Yao. *Zhongguo meng: weilai guojia zhanlue yu Zhongguo jueqi [The China dream: future national strategy and China's rise* [in zh-Latn]. 15. Beijing: Dangdai Zhongguo, 2013.

Yan, L., and W. Yuanshan. "Multiple risks and countermeasures of data sovereignty security in the context of cyber warfare" [in en]. *information magazine* 42, no. 5 (2023): 54–60.

Yeo, G. "Trust and context in cyberspace"' [in en]. Available at: *Archives and Records* 34, no. 2 (2013): 214–234. https://doi.org/10.1080/23257962.2013.825207.. https://doi.org/10.1080/23257962.2013.825207..

Yi, S., and J. Tianjiao. "Offense-defense balance in cyberspace and the construction of cyber deterrence" [in en]. *World Economy and Politics* 2018, no. 2, 49–70.

Younger, Alex. *We must confront China over security — but co-operate with it too*, September 2023. https://www.ft.com/content/b01a5e6a-1a59-4eb1-8add-415e64dbda37.

Zhang, A.H. "Agility Over Stability: China's Great Reversal in Regulating the Platform Economy"' [in en]. *Harvard International Law Journal* 63 (2022): 457.

Zhang, A.H. *High Wire: How China Regulates Big Tech and Governs Its Economy* [in en]. Oxford University Press, 2024.

———. "Weaponizing Antitrust During the Sino-US Tech War"' [in en]. In *Chinese Antitrust Exceptionalism: How The Rise of China Challenges Global Regulation*, edited by A.H. Zhang. Oxford University Press, 2021.

Zhang, Xiao, Cristopher Moore, and Mark EJ Newman. "Random graph models for dynamic networks." *The European Physical Journal B* 90 (2017): 1–14.

Zhe, B., G. Yuetao, and C. Xiaofei. "Research on the Weakening Trend of US Cyber Deterrence Strategy" [in en]. *Information security and communication confidentiality* 2023, no. 7, 1–11.

Zhihua, Z., C. Rongying, and Z. Lingke. "Analysis and enlightenment of network information security strategies of major developed countries" [in en]. *Modern Intelligence* 37, no. 1 (2017): 172–177.

Zúñiga, Nicholas, Saheli Datta Burton, Filippo Blancato, and Madeline Carr. "The geopolitics of technology standards: historical context for US, EU and Chinese approaches." *International Affairs* 100, no. 4 (July 10, 2024): 1635–1652. ISSN: 0020-5850. https://doi.org/10.1093/ia/iiae124. https://doi.org/10.1093/ia/iiae124.

. "Observation on the cyberspace situation in the context of great power competition in 2023" [in en]. *China Information Security* 2024, no. 1, 57–59.

. "The cohesion of China's power in cyberspace in the new era" [in en]. *China Military to Civilian* 2024, no. 13, 18–20.

. "Discussion on the Strategic Stability of China-US Cyberspace——Analysis of Political Factors in the Field of US Domestic Cybersecurity and Governance during the Trump Period" [in en]. *Information security and communication confidentiality* 2019, no. 11, 46–59.

. "US Strategy Towards China: Strategic Tipping Point and Restrictive Competition" [in en]. *Contemporary World and Socialism* 2020, no. 1, 137–145.

and. "New trends in the U.S. Department of Defense's 2023 Cyber Strategy and its impact and inspiration on China" [in en]. *Internet World* 2023, no. 11, 20–25.

, . "US cyberspace combat capabilities and development trends" [in en]. *China Information Security* 2022, no. 2, 64–67.

Supplementary Material

Supplementary material