Who will govern artificial intelligence?

Learning from the history of strategic politics in emerging technologies

Author Jade Leung

College Linacre

Date of submission July 2019

Thesis submitted in partial fulfilment of the requirements for the degree of DPhil in International Relations in the Department of Politics and International Relations at the University of Oxford.

Abstract

Artificial intelligence (AI) is a strategic general purpose technology (GPT) with the potential to deliver vast economic value and substantially affect national security. The central claim motivating this work is that the development of a strategic GPT follows a distinct pattern of politics. By modelling this pattern, we can make predictions about how the politics of AI will unfold.

The proposed model follows a life cycle of a strategic GPT. It focuses on three actors – the state, firms, and researchers. Each actor is defined by their goals, resources and constraints. The model analyses the relationships between these actors – specifically, the synergies and conflicts that emerge between them as their goals, resources, and constraints interact.

Case studies of strategic GPTs developed in the U.S. – specifically aerospace technology, biotechnology, and cryptography – show that the model captures much of history accurately. When applied to AI, the model also does well to capture political dynamics to date and motivates predictions about how we could expect the politics of AI to unfold. For example, I predict that AI firms will be increasingly constrained by the legislative environment, and more pressured to serve national defense and security interests. Some will be caught in the cross-hairs of public critique and researcher push back; some, however, will willingly sell AI technologies to the state with little friction. Further, I predict that the political influence of researchers will shrink, going against what some may view as a rise in researcher influence given recent events of employee backlash in AI firms. In turn, the inclination and capacity for the state to exert control over AI's development and proliferation will likely grow, exercised via tools such as export controls.

Artificial intelligence is going to matter greatly, and indeed, already does. It matters, then, that we understand the politics that surrounds it, and that we ultimately lay the groundwork for the governance of a technology that is poised to be transformative.

Acknowledgements

I am grateful to many individuals for being so wonderfully supportive and constructively critical throughout this whole process. First and foremost, I am deeply thankful for the invaluable support from my supervisor Duncan Snidal, a truly courageous man who took a punt on supervising a strange girl with strange ideas about artificial intelligence. The quality and clarity of this work has benefitted immensely from his consistently insightful probing, his strong encouragement to continually refine my arguments, and his timely asking of the 'so what' question.

To my colleagues at the Centre for the Governance of Artificial Intelligence and the Future of Humanity Institute, I have benefitted in countless ways from our discussions and have valued the luxury of being able to tap into their expertise. In particular, I want to thank: Allan Dafoe, for the prominent leadership of his thinking on AI security and governance issues, and in particular for his crystal clarity of thinking on matters of state power and leverage with respect to AI; Sophie-Charlotte Fischer for her impressively thorough knowledge of the history of American defense technology policy and export controls; Remco Zwetsloot for his on-the-pulse insight into Washington DC's activities on AI; Jeffrey Ding for his uniquely broad expertise on China's AI development and politics; Ben Garfinkel for his beautifully precise thinking on framing AI as a general purpose technology; and Nathan Calvin for his incredibly thorough historical research on the first two waves of AI.

I have had the privilege of having this work reviewed by experts who are true intellectual leaders in their fields, and who were stunningly generous with their time and feedback. In particular, I want to thank Allan Dafoe and Pepper Culpepper for assessing this work at the Confirmation of Status stage; our discussions and their feedback were instrumental in refining the concept of a strategic general purpose technology and clarifying my claims on the influence of researchers, among other things. I then had the invaluable opportunity to discuss this work in depth with my

examiners, Allan Dafoe and Gillian Hadfield, both among the top experts in this field who I most deeply respect and learn the most from; our discussion and their feedback were immensely helpful, particularly in refining the predictions on the future of AI politics. Further, the case study on biotechnology is only as thorough as it is thanks to expert input from Catherine Rhodes and Andrew Snyder-Beattie. Finally, I am thankful to Richard Danzig for his close review and comments on a final draft; I remain humbled that someone with his experience and breadth of knowledge took the time to offer his gentle yet sharp comments.

Finally, to my family and friends, I am grateful to them – as in life – for knowing me so embarrassingly well throughout this entire journey. To Markus Anderljung, words fall short of my gratitude for his brilliant brain and heart, and his brilliant partnership. Finally, I am thankful to the Rhodes Trust, for their generous and unwavering support of my work, but more importantly, of my beliefs and intuitions on what impactful work needed to be done in this world.

Table of contents

1 Introduction

It is a rare and momentous occasion in the history of human civilisation when we discover a technology that has the potential to radically change the course of progress. The creation of artificial intelligence may be one such occasion.

Bringing into existence machines that automate intelligence could radically shift the dynamics of our global economy and society. The transformative potential of AI has been likened to electricity, fire, and nuclear fission[1]. Already, the opportunities posed by AI that exist today are as broad-ranging as they are rapidly expanding, covering a range of sectors – including healthcare, education, finance, and agriculture – across several stages of innovation – from fundamental research breakthroughs to consumer-facing technologies. At the cutting edge, AI is propelling innovation itself via automating scientific experiments, generating insights from scientific papers, and optimising engineering designs[2]. As posited by I. J. Good, AI

[1] The most notable examples include:

- Google CEO Sundar Pichai referred to AI as "one of the most important things humanity is working on. It is more profound than…electricity or fire." - Clifford, C. (2018). Google CEO: A.I. is more important than fire or electricity. *CNBC*. Retrieved from https://www.cnbc.com/2018/02/01/google-ceo-sundar-pichai-ai-is-more-important-than-fire-electricity.html.
- Andrew Ng, former Chief Scientist at Baidu and founder of the Google Brain Deep referred to AI as "the new electricity" in an address at Stanford University. - Stanford Graduate School of Business. (2017). *Andrew Ng: Artificial Intelligence is the New Electricity*. Retrieved from https://www.youtube.com/watch?v=21EiKfQYZXc.
- Sam Altman, President of Y Combinator and founder of OpenAI, likened AI to nuclear fission. - Clifford, C. (2017). Top Silicon Valley exec on why Mark Zuckerberg and Elon Musk are both right about A.I. *CNBC*. Retrieved from https://www.cnbc.com/2017/09/11/y-combinators-sam-altman-zuckerberg-and-musk-both-right-on-a-i.html.

[2] Notable examples include:

- Researchers developed a robotic system that can autonomously develop scientific genome hypotheses, conduct experiments to test the hypotheses, and reach conclusions about the hypothesis to inform further hypothesis formation. - King, R. D. et al. (2009). The Automation of Science. *Science*, 324(5923), 85. https://doi.org/10.1126/science.1165620
- An AI system used language processing algorithms to analyse thousands of peer-reviewed articles related to amyotrophic lateral sclerosis (ALS), which enabled it to correctly predict five previously unknown genes related to the disease. - Hinchliffe, E. (2016). IBM's Watson supercomputer discovers 5 new genes linked to ALS. *Mashable UK*. Retrieved from https://mashable.com/2016/12/14/ibm-watson-als-research/#c6wvytOVaGqK
- Machine learning algorithms supported by advanced mechanical simulations developed new designs for mechanical equipment. - Tayarani-N., M. H., Yao, X., & Xu, H. (2015). Meta-Heuristic Algorithms in Car Engine Design: A Literature Survey. *IEEE Transactions on Evolutionary Computation*, 19(5), 609–629. https://doi.org/10.1109/TEVC.2014.2355174

could be the 'last invention [we] need ever make' in order to create systems that can innovate equivalently or better than humans can[3].

For all its promise, AI has caught the attention of the world's most powerful actors. To date, over two dozen countries have released national AI strategies expressing clear intentions to invest heavily in AI as a matter of national interest[4]. The two nations at the forefront of this pursuit are the U.S. and China. Both countries have invested significant political and financial capital in AI, placing it central to their respective pursuits of leadership on the world stage. In July 2017, the Chinese government published the State Council's New Generation AI Development Plan setting the goal of China becoming the world's primary AI innovation centre by 2030. The plan also outlined substantial investments and government support to enable this vision[5]. The People's Liberation Army have simultaneously articulated a long-term goal of moving towards 'unmanned, intangible, silent warfare' and have already capitalized on AI to build unmanned weapon systems including aircraft, drones, and submarines[6].

For the U.S., the pursuit of AI has become central to their strategy for retaining military dominance as outlined in the 'Third Offset Strategy'[7]. This has manifested in initiatives such as the Algorithmic Warfare Cross-Functional Team whose remit is to 'accelerate DOD's

---

[3] Good, I. J. (1966). Speculations Concerning the First Ultraintelligent Machine. In F. L. Alt & M. Rubinoff (Eds.), *Advances in Computers* (Vol. 6, pp. 31–88). Elsevier. https://doi.org/10.1016/S0065-2458(08)60418-0

[4] Future of Life Institute. (n.d.). National and International AI Strategies. Retrieved December 11, 2018, from https://futureoflife.org/national-international-ai-strategies/

[5] Ding, J. (2018). *Deciphering China's AI Dream: The context, components, capabilities and consequences of China's strategy to lead the world in AI*. Future of Humanity Institute. Retrieved from https://www.fhi.ox.ac.uk/wp-content/uploads/Deciphering_Chinas_AI-Dream.pdf

[6] Kania, E. B. (2017). *Testimony before the U.S.-China Economic and Security Review Commission: Chinese Advances in Unmanned Systems and the Military Applications of Artificial Intelligence - the PLA's Trajectory towards Unmanned, "Intelligentized" Warfare*. The Long Term Strategy Group. Retrieved from https://www.uscc.gov/sites/default/files/Kania_Testimony.pdf

[7] Carter, A. (2016). *Keynote Address: The Path to the Innovative Future of Defense*. Presented at the Center for Strategic and International Studies: Assessing the Third Offset Strategy: Progress and Prospects for Defense Innovation, CSIS Headquarters, Washington, D.C. Retrieved from https://csis-prod.s3.amazonaws.com/s3fs-public/event/161028_Secretary_Ashton_Carter_Keynote_Address_The_Path_to_the_Innovative_Future_of_Defense.pdf

integration of big data and machine learning'[8], DARPA's $2 billion investment in the AI Next Campaign[9], and the Pentagon's Joint Artificial Intelligence Center[10]. In response to China's rise in AI, the Trump Administration appears to be focused on accelerating these efforts[11]. Notably, in August 2018 President Trump approved the National Defense Authorization Act triggering the creation of a National Security Commission for Artificial Intelligence[12] and a 580% increase from $16 million to $93.1 million in AI defense investment[13].

The intensifying race between the U.S. and China to lead at the frontier of AI may be the defining great power competition of our time. Yet it is important to bear in mind that this is not the first time a technology has become a focal point of competition between powerful actors, nor will this be the first time that the perceived strategic importance of a technology has shaped the political posturing of presidents and the objectives of national economic and defense strategies. If we look, then, to the history of powerful actors pursuing strategic technologies, we can attempt to map the politics of AI as it is unfolding today onto an empirical reality.

---

[8] In the memorandum establishing Project Maven, Robert Work (32nd US deputy secretary of defense) states: "As numerous studies have made clear, the Department of Defense (DoD) must integrate artificial intelligence and machine learning more effectively across operations to maintain advantages over increasingly capable adversaries and competitors." - Work, R. (2017). *Establishment of an Algorithmic Warfare Cross-Functional Team (Project Maven)*. Department of Defense. Retrieved from http://dodcio.defense.gov/Portals/0/Documents/Project%20Maven%20DSD%20Memo%2020170425.pdf

[9] Harwell, D. (2018). Defense Department pledges billions toward artificial intelligence research. *The Washington Post*. Retrieved from https://www.washingtonpost.com/technology/2018/09/07/defense-department-pledges-billions-toward-artificial-intelligence-research/?utm_term=.1e1dfd2c7c61

[10] Leung, J., & Fischer, S.-C. (2018). JAIC: Pentagon debuts artificial intelligence hub. *Bulletin of the Atomic Scientists*. Retrieved from https://thebulletin.org/2018/08/jaic-pentagon-debuts-artificial-intelligence-hub/

[11] Metz, C. (2018). Artificial Intelligence Is Now a Pentagon Priority. Will Silicon Valley Help? *The New York Times*. Retrieved from https://www.nytimes.com/2018/08/26/technology/pentagon-artificial-intelligence.html

[12] McCain, J. S. National Defense Authorization Act for Fiscal Year 2019, Pub. L. No. H.R.5515 (2018). Retrieved from https://www.congress.gov/bill/115th-congress/house-bill/5515/text

[13] Cassano, J. (2018). Pentagon's Artificial Intelligence Programs Get Huge Boost in the NDAA. *Sludge*. Retrieved from https://readsludge.com/2018/08/15/pentagons-artificial-intelligence-programs-get-huge-boost-in-the-ndaa/

This history, however, requires some disentangling – for while technological leadership has always been central to political power, its pursuit has become more complex. Specifically, there are three contextual factors which have, of late, made the act of strategic technology pursuit a less than straightforward negotiation of private and public interests between states, firms, and researchers.

First, technology is fundamental to securing a nation's strategic advantage – and in today's world, those at the steering wheel of technological innovation are no longer state-funded labs and nationally embedded firms. Rather, the drivers of strategic technology development are global corporations serving global interests and operating across global markets. Their incentives are commercial first and foremost; serving national interests are ancillary goals for these private actors.

Second, in today's world, frontier research is being conducted by non-state actors. Leading research labs are increasingly funded by private capital and sit within private firms. When they are publicly funded, this is typically done at arms-length – a stark contrast from the days of government laboratories and defense-funded research groups. Further, the culture among researchers is evermore a transnational phenomenon, defined by core principles such as the freedom of exchange and movement across national borders.

Finally, the tactics available for pursuing technological leadership are constrained by tightening interdependence between states. The effects of globalization entrench such interdependencies via transnational trade, global supply chains, multilateral institutions, and international norms and agreements. The more intertwined that states become, the more ill-suited traditional great power tactics are; retreating into one's borders has become much costlier and therefore less viable for any state, even the most powerful. Thus, great power competition in today's world is more a task of navigating economic advantage in international markets rather than building up national military strength.

In short: in order to understand the pursuit of power on the global stage, one must look to the politics between the state, firms and researchers at a national level – for technological pursuit has become a site of intertwined economic and security interests that inevitably link these national politics to international dynamics. States are now more reliant on multinational firms to produce world-leading commercial technologies that serve both national economic and defense interests. Firms are faced with the challenge of balancing their ambitions for global growth with their sensitivity to the interests of the state; after all, the state shapes the regulatory environment that bounds their activities. In a high-technology industry, research talent becomes a critical constraining input; as such, questions of whether research is publicly and privately funded, and what strings come attached with each, become important.

Deciphering these political dynamics is the central focus of this work. Specifically, my primary claim is that for a particular type of strategic technology, analogous to AI, a predictable pattern of politics unfolds between the state, firms and researchers as the technology progresses through a life cycle of development and deployment. I call these *strategic general purpose technologies* (strategic GPTs) – a general purpose technology which has the potential to deliver vast economic value and substantially affect national security, and is consequently of central political interest to states, firms, and researchers. By homing in on specific cases of the technology life cycle of strategic GPTs, we can observe a given actor's behaviours and the dynamics of their relationships with other actors. This provides a basis for making more general claims about the pattern of politics that emerge as actors pursue a strategic GPT.

In this work, we find that this pattern is indeed somewhat predictable across historical cases of strategic GPTs. Specifically, predictable synergies emerge between actors – the state depends on firms for access to cutting edge commercial technologies, and both the state and firms invest resources into creating a supportive research and commercial environment for

the technology at hand. In turn, predictable conflicts also emerge between actors. As the technology matures, the state consistently seeks to prevent both firms and researchers from proliferating knowledge, talent, and technologies to overseas adversaries. Further, firms sometimes face backlash from both the public and researchers on ethical dilemmas, such as the decision of whether to sell technologies to the state for defense and security purposes.

In extrapolating to the contemporary case of AI, we can motivate predictions of what we can expect to unfold in the politics of AI. For example, contrary to a common view of AI firms being too powerful to regulate, this work predicts that these firms will increasingly face legislative restrictions imposed on them by the state, particularly in the form of tools such as export controls, and particularly motivated by the state's prioritisation of national security concerns. The AI industry is also predicted to bifurcate into firms who are unwilling to work with the state on ethical grounds, versus firms who would have no qualms doing so and who would face minimal backlash in doing so. Finally, despite AI researchers currently being framed as relatively powerful actors, history would suggest that we should expect the power of researchers to wane with time.

In the following sections, I first lay the theoretical groundwork upon which this research builds (section 1.1). I then define the research objectives and the methodology used in carrying out this work (section 1.2). Chapter 2 covers the technology life cycle model which describes the general case of the politics surrounding the pursuit of a strategic GPT. Chapters 3, 4 and 5 turn to historical cases of such technologies as empirical grounding for the model. Chapter 6 offers an analysis and discussion of these case studies through the lens of the model. We then analyse the case of AI in Chapter 7, framing events to date and prospective events to come. I conclude in Chapter 8.

1.1 Theorising the politics of strategic general purpose technologies

The politics of strategic general purpose technologies is a story about power – specifically, powerful actors and how they wield their political capital to strengthen and maintain their power. Each of these actors – the state, technology firms, and researchers – has to some extent been conceptualized in literature vis a vis the dimensions of their power; we look to these literatures to ground the development of the model that follows.

Firstly, in section 1.1.1, we step through how international relations scholarship has grappled with the emergence of large private firms as political actors. This literature examines the impact of multinational companies on the nature of power and authority, specifically traditional state power and public authority. Further, in this new configuration of public and private authorities, this literature addresses their respective limits and interdependencies, drawing or redrawing bounds around what firms can and can't do as political actors, and what this means for their relationship with the state.

Then, in section 1.1.2, we analyse the role of the state as framed in response to these rising private powers. We focus specifically on the evolution of defense and technology policy in the U.S. – given the growth of private companies as the primary developers of American technologies, this literature looks at how the U.S. government adapted to the prominence of commercial firms[14].

Finally, in section 1.1.3 we turn to the researchers. Researchers, and research communities, have historically been neglected in political science and international relations literature. At best they have been conceptualized as actors with limited political influence and whose relevance is restricted to narrow expert-based policymaking contexts. Alternatively, researchers framed as professionals have been conceptualized as economic actors with some

[14] A sincere thank you to my colleague Sophie-Charlotte Fischer for pointing me towards this literature.

influence on the behavior of firms as their employers. This section draws together these two conceptions of researchers as an actor and underlines their insufficiencies in view of the role that researchers play in the development of strategic general purpose technologies[15].

1.1.1 The private firm as a political actor

The modern multinational corporation emerged as a distinct political actor in international relations scholarship in response to the impacts of globalization (section 1.1.1.1). In efforts to theorise this new form of a global private power, the role of the state in exercising authority over private firms became a focal point of debate (section 1.1.1.2). As we move to present day discussions, the relationship between public and private actors in international politics and global governance is most commonly described as a complex interdependence between the two actors, both at a national and international scale (section 1.1.1.3).

1.1.1.1 Globalization and its impact on international relations

The drivers, impacts, and consequences of modern globalization reverberated through international relations (IR) scholarship beginning in the early 1970s[16]. The fundamental premise of state-centrism in IR theory was challenged by several scholars who observed the internationalisation of economic, social and cultural forces and concluded that certainly, politics would be disrupted in turn. Keohane and Nye framed this as a shift towards a state of 'complex interdependence' between nation states and emerging non-state actors[17]. Specifically, the phenomenal growth of multinational enterprises brought private actors into the spotlight as the bearers and beneficiaries of globalization, which in turn ascribed them

[15] A sincere thank you to my colleague Toby Shevlane for pointing me towards this literature.
[16] Barnett, M., Pevehouse, J., & Raustiala, K. (2017). *The Future of Global Governance*. Geneva, Switzerland: Graduate Institute of International Development Studies and Social Trends Institute.; Beck, U. (2000). What is globalization? Cambridge: Polity Press.; Cerny, P. G. (1995). Globalization and the changing logic of collective action. *International Organisation*, *49*(4), 595–625. https://doi.org/10.1017/S0020818300028459; Weiss, T. G., & Wilkinson, R. (2014). Rethinking Global Governance? Complexity, Authority, Power, Change. *International Studies Quarterly*, *58*(1), 207–215. https://doi.org/10.1111/isqu.12082
[17] Keohane, R. O., & Nye, J. S. (1977). *Power and interdependence: world politics in transition*. Boston: Little, Brown.; Keohane, R. O., & Nye, J. S. (1989). *Power and interdependence* (2nd ed.). New York: Longman.

with forms of power and authority to challenge the state[18]. Some surmised IR scholarship during this period as 'increasingly contaminated and often overshadowed with the private logic of the global economy'[19].

Strands of IR scholarship adapted in the face of these challenges. In particular, the global governance literature evolved to acknowledge and integrate the rise of non-state actors. Governance – 'the rules, structures and institutions that guide, regulate and control social life'[20] – came to be understood as a domain which featured a plurality of actors, including firms. In turn, governance institutions were faced with increasingly complex problems to which effective solutions required capacities beyond states alone[21]. Governance therefore could no longer be the exclusive domain of national governments. Rather, a host of scholars – most notably Rosenau and Czempiel in their seminal text, *Governance without Government*[22] – urged legitimation of non-state actors as new forms of governance authority and capacity[23]. Rosenau further argued that the core of global governance concerns 'the acquisition of authoritative decision-making capacity by non-state and supra-state actors'[24]. Weiss described

---

[18] Vernon, R. (1971). Sovereignty at bay: the multinational spread of U.S. enterprises. London: Longman.
[19] Evans, P. (1997). The Eclipse of the State? Reflections on Stateness in an Era of Globalization. *World Politics*, *50*(1), 62–87.
[20] Barnett, M. N., & Duvall, R. (2005). *Power in Global Governance*. Cambridge, UK: Cambridge University Press. Retrieved from http://search.ebscohost.com/login.aspx?direct=true&db=nlebk&AN=129339&site=ehost-live&authtype=ip,uid
[c] Held, D. (2016). Elements of a theory of global governance. *Philosophy & Social Criticism*, *42*(9), 837–846. https://doi.org/10.1177/0191453716659520; Weiss, T. G. (2000). Governance, good governance and global governance: Conceptual and actual challenges. *Third World Quarterly*, *21*(5), 795–814. https://doi.org/10.1080/713701075; Weiss, T. G. (2009). What Happened to the Idea of World Government. *International Studies Quarterly*, *53*(2), 253–271. https://doi.org/10.1111/j.1468-2478.2009.00533.x
[22] Rosenau, J. N., & Czempiel, E. O. (1992a). *Governance without government: order and change in world politics*. Cambridge: Cambridge University Press.
[23] A non-exhaustive list of scholars making this claim include: Hall, R. B., & Biersteker, T. J. (2002). *The emergence of private authority in global governance*. Cambridge, UK: Cambridge University Press.; Koenig-Archibugi, M. (2010). Understanding the Global Dimensions of Policy. *Global Policy*, *1*(1), 16–28. https://doi.org/10.1111/j.1758-5899.2009.00009.x; Lake, D. A. (2010). Rightful Rules: Authority, Order, and the Foundations of Global Governance. *International Studies Quarterly*, *54*(3), 587–613. https://doi.org/10.1111/j.1468-2478.2010.00601.x; Rosenau, J. N. (1995). Governance in the Twenty-first Century. *Global Governance*, *1*(1), 13–43.; Stoker, G. (1998). Governance as theory: five propositions. *International Social Science Journal*, *50*(155), 17–28. https://doi.org/10.1111/1468-2451.00106; Weiss, T. G., & Wilkinson, R. (2014). Rethinking Global Governance? Complexity, Authority, Power, Change. *International Studies Quarterly*, *58*(1), 207–215. https://doi.org/10.1111/isqu.12082
[24] (Rosenau & Czempiel, 1992b)

global governance as 'doing internationally what governments do at home' in the 'absence of sovereign authority relationships that transcend national frontiers'[25]. Non-state actors became at the very least necessary partners to achieve effective global governance in what was a more decentralised and fragmented world order in which states were framed as constrained, insufficient, and thus dependent on other actors[26].

Conceptions of power in IR also evolved to reflect the rise of non-state actors. Power was traditionally thought of as the ability to create or disrupt order in the international system – a coercive, zero-sum game between nation states[27]. However, as the nature of the international system evolved, so did the field's understanding of power. Strange described power as 'the ability to create or destroy not order but wealth[28]. Lukes famously articulated the 'missing faces' of power – decision-making power, non-decision-making power, and ideological power[29]. Barnett and Duvall build on this to propose a taxonomy of power as 'the production, in and through social relations, of effects that shape the capacities of actors to determine their circumstances and fate'[30]. Notably, these forms of power are accessible to private actors, positioning them as central to international politics rather than peripheral. The way in which multinational corporations exert power has been examined by scholars across time, from an era of large national enterprises such as oil companies and manufacturing firms

---

[25] (T. G. Weiss, 2009)
[26] Acharya, A. (2016). The Future of Global Governance: Fragmentation May Be Inevitable and Creative. *Global Governance*, *22*(4), 453–460.; Biermann, F., Pattberg, P., van Asselt, H., & Zelli, F. (2009). The Fragmentation of Global Governance Architectures: A Framework for Analysis. *Global Environmental Politics*, *9*(4), 14–40. https://doi.org/10.1162/glep.2009.9.4.14; Kaul, I., & United Nations Development Programme. (2003). *Providing global public goods: managing globalization*. New York ; Oxford: Oxford University Press.; Krahmann, E. (2003). National, Regional, and Global Governance: One Phenomenon or Many? *Global Governance*, *9*(3), 323.; Ruggie, J. (2014). Global Governance and "New Governance Theory": Lessons from Business and Human Rights. *Global Governance*, *20*(1), 5–17.
[27] Dahl, R. A. (1957). The concept of power. *Behavioral Science*, *2*(3), 201–215. https://doi.org/10.1002/bs.3830020303
[28] Strange, S. (1991). Big Business and the State. *Millennium - Journal of International Studies*, *20*(2). Retrieved from https://ezproxy-prd.bodleian.ox.ac.uk:7218/doi/abs/10.1177/03058298910200021501#articleCitationDownloadContainer
[29] Lukes, S. (2005). *Power: A Radical View* (Second edition). New York: Palgrave Macmillan. Retrieved from http://search.ebscohost.com/login.aspx?direct=true&db=nlebk&AN=197447&site=ehost-live&authtype=ip,uid
[30] Barnett, M., & Duvall, R. (2005). Power in International Politics. *International Organization*, *59*(1), 39–75. https://doi.org/DOI: 10.1017/S0020818305050010

to the technology corporations of today. As these private actors have scaled from operating within the framework of national markets, laws and financial systems to globalized ones, both the form and the strength of the power that they exert has substantially affected the landscape of international politics[31].

1.1.1.2 The erosion versus the evolution of the state

What does this mean for the nation state? Two dominant hypotheses have been put forward by IR scholars. One claims that state sovereignty and power have been eroded by globalization, and national governments have been weakened and undermined. The other counters that the state remains ever important, but the nature of their role has evolved.

The argument for the erosion of the state is intimately linked with the rise of private actors. Multinational corporations were framed as the rising forms of authority, with the locus of power on the international stage being transferred from public to private institutions[32]. The growth of international markets and the strengthening of transnational economic forces drove the retreat of the state as big businesses took hold of the reins in their stead. Vernon famously described sovereignty as being 'at bay', driven by the 'basic asymmetry between multinational enterprises and national governments' and warning that 'the apocalyptic projections of the future of multinational enterprise will grow more plausible' if governments

---

[31] Beck, U. (2005). Power in the global age: a new global political economy. Cambridge: Polity.; Bieler, A., Higgott, R., & Underhill, G. (1999). *Non-State Actors and Authority in the Global System*. London: Routledge. Retrieved from http://ebookcentral.proquest.com/lib/oxford/detail.action?docID=165773; DeNardis, L. (2009). Protocol politics: the globalization of Internet governance. Cambridge, Mass.: MIT Press.; Strange, S. (1988). States and markets. London: Pinter.; Strange, S. (1991). Big Business and the State. *Millennium - Journal of International Studies*, *20*(2). Retrieved from https://ezproxy-prd.bodleian.ox.ac.uk:7218/doi/abs/10.1177/03058298910200021501#articleCitationDownloadContainer

[32] Clark, I. (1999). *Globalization and international relations theory*. Oxford: Oxford University Press.; Cutler, A. C., Haufler, V., & Porter, T. (1999a). *Private authority and international affairs*. Albany: State University of New York Press.; Julius, D. (1990). *Global companies and public policy: the growing challenge of foreign direct investment*. London: Pinter.; O'Brien, R. (2000). *Contesting global governance: multilateral economic institutions and global social movements*. Cambridge: Cambridge University Press.; Ōmae, K. (1995). *The end of the nation state: the rise of regional economies*. London: HarperCollins.; Rodrik, D. (1997). *Has globalization gone too far?* Washington, D.C.: Institute for International Economics.; Rosecrance, R. N. (1999). *The rise of the virtual state: wealth and power in the coming century*. New York: Basic Books.; Schmidt, V. A. (1995). The New World Order, Incorporated: The Rise of Business and the Decline of the Nation-State. *Daedalus*, *124*(2), 75–106.; Strange, S. (2000). *The retreat of the state: the diffusion of power in the world economy*. Cambridge: Cambridge University Press.

do not find a way to regain the basis of their sovereignty[33]. Strange painted one such projection in which 'markets…are the masters over the governments of states'[34] and states become 'merely the handmaidens of firms'[35]. Others have postulated that the loss of government control over corporations was an inevitable outcome of the increasing economic interdependence and technological advances driving globalization[36].

Several mechanisms were proposed for how globalization ultimately weakened the role of the state. The most prominent was the prediction of a race to the bottom – as corporations grew and their operations scaled across national borders, states would be left with no choice but to compete in order to attract firms to their shores[37]. This compromises the ability of national governments to exercise their political will independently from companies. Their fiscal and industrial policies become constrained by what Freidman coined the neoliberal 'Golden Straitjacket', forcing states to harmonize with the lowest common denominator in order to remain competitive[38]. Other mechanisms included concern over the private capture of governments, and the scale mismatch between the resources available to private firms relative to national governments[39]. As multinational corporations continue to grow, some

[33] (Vernon, 1971)
[34] (Strange, 2000)
[35] Strange, S. (1997). The Future of Global Capitalism; or Will Divergence Persist Forever? In C. Crouch & W. Streeck (Eds.), *Political Economy of Modern Capitalism: Mapping Convergence and Diversity*. London, United Kingdom: SAGE Publications. Retrieved from http://ebookcentral.proquest.com/lib/oxford/detail.action?docID=537777
[36] Cooper, R. N. (1968). *The economics of interdependence: economic policy in the Atlantic community* (1st ed.). New York: Published for the Council on Foreign Relations by McGraw-Hill.; Fukuyama, F. (1992). *The end of history and the last man*. London: Hamish Hamilton.; Haas, E. B. (1964). *Beyond the nation-state: functionalism and international organization*. Stanford, Calif: Stanford University Press.; Kindleberger, C. P. (1970). *The international corporation: a symposium*. Cambridge, Mass: MIT Press.
[37] Held, D. (1999). *Global transformations: politics, economics and culture*. Cambridge: Polity Press.; Schmidt, V. A. (1995). The New World Order, Incorporated: The Rise of Business and the Decline of the Nation-State. *Daedalus*, *124*(2), 75–106.; Vernon, R. (1981). Sovereignty at Bay ten years after. *International Organization*, *35*(3), 517–529. https://doi.org/10.1017/S0020818300032562
[38] Friedman, T. L. (1999). *The Lexus and the olive tree*. London: HarperCollins.
[39] Barnet, R. J. (1975). *Global reach: the power of the multinational corporations*. London: Jonathan Cape.; Mikler, J. (2011). The Illusion of the "Power of Markets." *The Journal of Australian Political Economy*, (68), 41–61.

warn that they will become the 'leviathans of our time' – stateless economic actors with the ability to undermine state sovereignty[40].

In the wake of the retreating state, scholars have pointed to examples of private actors stepping up to the plate to provide the political and governance functions once considered exclusive to national governments. Haufler was one of the first to explore how the private sector created and maintained a governance framework for international economic transactions outside of the remit of the state[41]. Hall and Biersteker further articulated the nature of private authority in the international system, demonstrating how private international regimes can be formed by transnational corporations and businesses around a global issue area[42]. Vogel extended this work to the specific case of business regulation, tracing the rise of codes, regulations and standards among global firms and across global industries without the involvement of states[43]. Indeed, several forms of private-actor led governance, from supply chain regulation to industry standards have been analysed as examples of corporations filling the political lacunae left behind by states[44].

---

[40] Chandler, A. D., & Mazlish, B. (2005). *Leviathans: multinational corporations and the new global history*. Cambridge: Cambridge.; Reinicke, W. H., & Witte, J. M. (2000). Interdependence, Globalization and Sovereignty: The Role of non-binding International Legal Accords. In D. Shelton (Ed.), *Commitment and compliance: The role of non-binding norms in the international legal system*. Oxford University Press on Demand.

[41] Haufler, V. (2001). *A public role for the private sector: industry self-regulation in a global economy*. Washington, District of Columbia: Carnegie Endowment for International Peace.

[42] (Cutler et al., 1999a; Hall & Biersteker, 2002)

[43] Vogel, D. (2008). Private Global Business Regulation. *Annual Review of Political Science*, *11*(1), 261–282. https://doi.org/10.1146/annurev.polisci.11.053106.141706

[44] Bottomley, S. (2007). *The constitutional corporation: rethinking corporate governance*. Aldershot: Ashgate.; Gessner, V. (2012). Enabling global business transactions: Relational and legal mechanisms. In G. Morgan & R. Whitley (Eds.), *Capitalisms and Capitalism in the Twenty-first Century*. Oxford University Press.; May, C. (2015b). Who's in charge? Corporations as institutions of global governance. *Palgrave Communications*, *1*, 15042.; Parker, C. (2002). *The open corporation: Effective self-regulation and democracy*. Cambridge University Press.; Pattberg, P. (2005). The Institutionalization of Private Governance: How Business and Nonprofit Organizations Agree on Transnational Rules. *Governance*, *18*(4), 589–610. https://doi.org/10.1111/j.1468-0491.2005.00293.x; Scherer, A. G., & Smid, M. (2000). The downward spiral and the US model business principles-Why MNEs should take responsibility for the improvement of world-wide social and environmental conditions. *MIR: Management International Review*, *40*, 351–371.; Scherer, A. G., Palazzo, G., & Baumann, D. (2006). Global Rules and Private Actors: Toward a New Role of the Transnational Corporation in Global Governance. *Business Ethics Quarterly*, *16*(4), 505–532.; Zadek, S. (2004). The Path to Corporate Responsibility. *Harvard Business Review*, *82*(12), 125–132.

Others have pushed back against 'the myth of the powerless state', holding that states remain the central drivers of the norms, processes and outcomes of international politics and global governance. They were critical of what they saw as overstatements of the growing power of multinational corporations and the concomitant decline of the nation state[45]. Rather, they saw this shift as a conscious reorientation of the state's role in an era of globalization. The marketization of all aspects of society and state functions was framed as a deliberate policy choice, a 're-regulation' as opposed to an unwilling process of deregulation and loss of control[46]. Braithwaite coined this 'regulatory capitalism' in which 'the corporatization of the world is…a product of [state] regulation' and ultimately reflects 'the reciprocal relationship between corporatization and regulation'[47]. Others have termed this the 'substitutability principle' – the notion that states can and will substitute different governance structures and different policy tools to create those structures, which may include delegating traditionally state functions to non-state actors[48].

Indeed, ten years after publishing *Sovereignty at Bay* – a cornerstone text for those who believed in the narrative of the eroding state – Vernon recounted numerous threats to multinational

---

[45] Bell, S. (2009). *Rethinking governance: the centrality of the state in modern society*. Cambridge: Cambridge University Press.; Drezner, D. W. (2007). *All politics is global: explaining international regulatory regimes*. Princeton, N.J.: Princeton University Press.; Gilpin, R. (1976). *U.S. power and the multinational corporation: the political economy of foreign direct investment*. London: Macmillan.; Huntington, S. P. (1973). Transnational Organizations in World Politics. *World Politics*, 25(3), 333–368. https://doi.org/10.2307/2010115; Hymer, S. (1972). The Multinational Corporation and the Law of Uneven Development. In J. Bhagwati, *Economics and the World Order - From the Nineteen Seventies to the Nineteen Nineties*. New York: Macmillan.; Mandel, E. (1967). International Capitalism and Supra Nationality. In R. Miliband & J. Saville, *The Socialist Register*. London: Merlin Press.; Weiss, L. (1998). *The myth of the powerless state: governing the economy in a global era*. Cambridge: Polity Press.

[46] Jordana, J., Levi-Faur, D., & University of Manchester. Centre on Regulation and Competition. (2004). *The politics of regulation: institutions and regulatory reforms for the age of governance*. Cheltenham: Edward Elgar.; Tiberghien, Y. (2007). *Entrepreneurial states: reforming corporate governance in France, Japan, and Korea*. Ithaca: Cornell University Press. Retrieved from http://www.loc.gov/catdir/toc/ecip0713/2007011004.html; Thatcher, M. (2007). *Internationalisation and economic institutions: comparing European experiences*. New York; Oxford: Oxford University Press. Retrieved from http://www.loc.gov/catdir/toc/ecip077/2006102400.html; Vogel, S. K. (1996). *Freer markets, more rules: regulatory reform in advanced industrial countries*. Ithaca; London: Cornell University Press.

[47] Braithwaite, J. (2008). *Regulatory capitalism: how it works, ideas for making it work better*. Cheltenham, UK; Northampton, MA: Edward Elgar.

[48] Drezner, D. W. (2004a). The Global Governance of the Internet: Bringing the State Back In. *Political Science Quarterly*, *119*(3), 477–498. https://doi.org/10.2307/20202392; Krasner, S. (1976). State Power and the Structure of International Trade. *World Politics*, *28*(3), 317. https://doi.org/10.2307/2009974; Most, B. A., & Starr, H. (1984). International Relations Theory, Foreign Policy Substitutability, and "Nice" Laws. *World Politics*, *36*(3), 383–406. https://doi.org/10.2307/2010380

corporations that were launched in the 1970s which undermined their growing power[49]. In turn, Vernon found that 'governments [were] better informed and better equipped than they have ever been' in that they have an 'increasing number of options for securing the capital, technology, or access to markets they require' via their influence over corporations. He ultimately framed this as a shift not towards the decline of the state, but rather towards an evolution of the state in which their bargaining power is wielded in more ambiguous ways, reflecting the conscious balancing act that governments are going through to reorient in a world of big business[50]. With some reluctance, 'gradually, almost imperceptibly, governments are being reconciled to a modified concept of sovereignty in the economic field' in which an increasingly crowded international political arena demands that they 'redefine the scope of the autonomy that sovereignty demands'[51].

The extent to which the state can reverse this evolution of their role is unresolved. On the one hand, some claim that states consciously delegate authority to private actors and thus can retract this as they see fit[52]. Others see this evolution as an inevitable choice that states are forced to make, however deliberate, when faced with the stark choice between benefitting from the economic gains of allowing for the emergence of private authorities versus retaining their sovereignty at the cost of economic and technological marginalization. Indeed, Vernon noted that governments have been reluctant to exercise their authority where it would appear

[49] Vernon cites the 'spate of nationalizations, the codes of conduct, the U.S. legislation against bribery, and the demands and resolutions of the General Assembly' signified a societal retaliation against the growth of big business, fuelled by a larger revulsion 'against the effects of industrialization, against the symbols of entrenched authority, against the impersonal tyranny of big bureaucracies'. See: (Vernon, 1981)
[50] Vernon reflects that instead of defaulting to outright nationalization, governments have been more inclined to settle for more indirect arrangements in order to exert influence over corporations such as gifting some of the equity to favoured members of the local private sector, expanding state-owned enterprises, and issuing contracts to allow multinationals to manage their properties without formal ownership.
[51] Note that Vernon frames this as a reorientation that is carried out somewhat begrudgingly by states: 'They are aware, for example, that without international cooperation none of them is any longer capable of ensuring the existence of secure banks or of policing their securities markets against fraud. They accept, however, reluctantly, the need for some cooperation among central banks in the maintenance of an orderly foreign exchange market.' See: Vernon, R. (1991). Sovereignty at Bay: Twenty Years After. *Millennium*, *20*(2), 191–195. https://doi.org/10.1177/03058298910200021201
[52] (Drezner, 2004a, 2007)

to matter in a world of multinational enterprises – namely, in agreeing on international regimes, processes and standards that would enforce requirements on corporations to deliver on public goods, adopt responsibilities to contribute to the national defense base, and provide information to consumer groups and labour unions across all jurisdictions in which they operate[53]. Perhaps, he suggested, this is an indication that states are not confident in, but rather are begrudging and uncertain of the implications of their evolving role.

1.1.1.3 Twenty-first century governance: a case of interdependence

The dynamics of international politics as we observe it today appears to have eased into a state of interdependence between public states and private firms. Powerful enterprises and powerful governments operate two systems in parallel – each legitimated by a form of authority and popular consent, each critical to the functioning of a globalized world, and each thus necessary to each other.

As Strange and colleagues note, fierce industrial competition inevitably requires government allies just as national economic development requires corporate allies. When these public and private goals converge, the relationship between states and firms can be cooperative. More broadly, when the achievement of one's goals are dependent on the actions of the other, states and firms find themselves inevitably dependent on each other's strategies[54]. Braithwaite terms this 'mega-corporate capitalism' – a symbiosis between large corporations and strong governments[55]. Globalization scholars couch this interdependence in terms of shared sovereignty and authority between states and non-state actors[56]. Global governance scholars have applied this to the concept of regimes and regime complexes, where a regime refers to

[53] (Vernon, 1981, 1991)
[54] Stopford, J. M. (1991). *Rival states, rival firms: competition for world market shares*. Cambridge: Cambridge University Press.
[55] (Braithwaite, 2008)
[56] Martell, L. (2007). The Third Wave in Globalization Theory. *International Studies Review*, *9*(2), 173–196. https://doi.org/10.1111/j.1468-2486.2007.00670.x

the 'rules, norms, principles and procedures that constitute the control mechanisms through which order and governance in particular issue areas are sustained'. They conceptualize regime creation as a joint effort between state and non-state actors, rendering global governance the product of interdependent relationships between them[57].

In examining contemporary forms of global governance, scholars have demonstrated this interdependence playing out in practice. Ronit and Schneider, for example, found that voluntary arrangements between private actors to produce public goods emerge 'in the shadow of the state' such that the efficacy of these arrangements require the support of the government in the form of recognition and regulatory functions[58]. Falkner found that private governance institutions such as the International Organization for Standardization (ISO) gains considerable strength and legitimacy with the participation of states, and that states exercise considerable influence over the operation of these private institutions[59]. Büthe and Mattli focused on the development of international regulation and found that the delegation of regulatory authority from governments to the private sector is viewed favourably by both the state and the firms largely for the lack of technical expertise and financial resources in-house within the government[60]. On standards, Abbott, Snidal and others showed that states have moved towards softer forms of governance instead of legally binding standards, relying

[57] Haas, E. B. (1980). Why Collaborate?: Issue-Linkage and International Regimes. *World Politics*, *32*(3), 357–405. https://doi.org/10.2307/2010109; Hasenclever, A., Mayer, P., & Rittberger, V. (1997). *Theories of international regimes*. Cambridge: Cambridge University Press.; Krasner, S. D. (1983). *International regimes*. Ithaca: Cornell University Press.; Orsini, A., Morin, J.-F., & Young, O. (2013). Regime Complexes: A Buzz, a Boom, or a Boost for Global Governance? *Global Governance*, 19(1), 27–39.; Rittberger, V., & Mayer, P. (1993). *Regime theory and international relations*. Oxford: Clarendon Press.; Young, O. R. (1980). International Regimes: Problems of Concept Formation. *World Politics*, *32*(3), 331–356. https://doi.org/10.2307/2010108

[58] Ronit, K., & Schneider, V. (1999). Global Governance through Private Organizations. *Governance*, *12*(3), 243–266. https://doi.org/10.1111/0952-1895.00102; Ronit, K., & Schneider, V. (2000). *Private organisations in global politics*. London: Routledge.

[59] Indeed, it may be in the state's interest to encourage private self-regulation to save them the task of negotiating international standards, and to avoid paying the costs of implementation and compliance. See: Falkner, R. (2003). Private Environmental Governance and International Relations: Exploring the Links. *Global Environmental Politics*, *3*(2), 72–87. https://doi.org/10.1162/152638003322068227

[60] Büthe, T., & Mattli, W. (2011). *The new global rulers: the privatization of regulation in the world economy*. Princeton, NJ: Princeton University Press.

on a combination of public and private actors to implement and enforce these standards in a cooperative, interdependent fashion[61].

Beyond interdependence, the dichotomy between the public and private spheres is becoming increasingly blurred. The public sphere has become more privately operated, and the private sphere has become more publicly accountable. As observed by Dicken, 'nation states, whilst essentially political institutions, have become increasingly involved in economic matters…[while] transnational corporations, though fundamentally economic in function, have become increasingly political in their actions and impact'[62]. We see the privatization of the state play out in several domains, from the use of private organizations for core state functions such as national security[63] and peace-keeping[64], through to the enlisting of private actors to deliver core public goods such as human and citizenship rights[65] and labour and environmental standards[66]. Conversely, private actors are increasingly expected to uphold public roles and responsibilities. The political responsibility of private firms has been conceptualized under several different headings, including corporate social responsibility[67],

---

[61] Abbott, K. W., & Snidal, D. (2000). Hard and Soft Law in International Governance. *International Organization*, *54*(3), 421–456. https://doi.org/DOI: 10.1162/002081800551280; Abbott, K. W., & Snidal, D. (2010). International regulation without international government: Improving IO performance through orchestration. *The Review of International Organizations*, *5*(3), 315–344. https://doi.org/10.1007/s11558-010-9092-3; Mörth, U. (2004). *Soft law in governance and regulation: an interdisciplinary analysis*. Cheltenham: Edward Elgar.; Shelton, D. (2003). *Commitment and compliance: the role of non-binding norms in the international legal system*. Oxford: Oxford University Press.

[62] Dicken, P. (1998). *Global shift: transforming the world economy* (3rd ed.). London: Paul Chapman.

[63] Abrahamsen, R., & Williams, M. C. (2009). Security Beyond the State: Global Security Assemblages in International Politics. *International Political Sociology*, *3*(1), 1–17. https://doi.org/10.1111/j.1749-5687.2008.00060.x; Abrahamsen, R., & Williams, M. C. (2011). *Security beyond the state: private security in international politics*. Cambridge: Cambridge University Press.

[64] Dunfee, T. W., & Fort, T. L. (2003). Corporate hypergoals, sustainable peace, and the adapted firm. *Vand. J. Transnat'l L.*, *36*, 563.; Fort, T. L., & Schipani, C. A. (2002). The role of the corporation in fostering sustainable peace. *Vand. J. Transnat'l L.*, *35*, 389.

[65] Kinley, D., & Tadaki, J. (2003). From talk to walk: The emergence of human rights responsibilities for corporations at international law. *Va. J. Int'l L.*, *44*, 931.; Williams, O. F. (2000). *Global Codes of Conduct. An idea Whose Time has Come*. University of Notre Dame Press.

[66] Scherer, A. G., & Smid, M. (2000). The downward spiral and the US model business principles-Why MNEs should take responsibility for the improvement of world-wide social and environmental conditions. *MIR: Management International Review*, *40*, 351–371.; Young, I. M. (2004). Responsibility and Global Labor Justice. *Journal of Political Philosophy*, *12*(4), 365–388. https://doi.org/10.1111/j.1467-9760.2004.00205.x

[67] Carroll, A. B. (1991). The pyramid of corporate social responsibility: Toward the moral management of organizational stakeholders. *Business Horizons*, *34*(4), 39–48. https://doi.org/10.1016/0007-6813(91)90005-G

corporate sustainability[68], corporate citizenship[69], corporate philanthropy[70], and business ethics[71]. Ultimately, these literatures have extended the view of the private firm to include their role in designing rules that are of the public interest and contributing to the stabilisation of society and international politics.

1.1.2 The evolution of the state's role in technology policy

It used to be the case that the U.S. government had comprehensive influence over the activities of technology firms headquartered on American soil. National economic strength was the foundation of military strength, and national economic actors were presumed to be central to the pursuit of the military goals of the state. The firms developing strategic technologies were thus largely nationally bound, dependent on the state as R&D funders and customers, and thus naturally aligned with the state's interests[72].

If one looks at the U.S. government now, much has changed about their capacity to control, acquire, and ultimately take advantage of cutting edge technologies to pursue national defense and security goals. In this section, we trace the evolution of the role and capacities of the state as a technology investor, developer, and consumer, beginning with the growth of the military industrial complex (section 1.1.2.1) to its effective dismantling (section 1.1.2.2). This culminates in the period that the U.S. government finds themselves in today, challenged with the need for substantial institutional reform in the face of high technology

---

[68] Sharma, S., & Starik, M. (2002). *Research in corporate sustainability: The evolving theory and practice of organizations in the natural environment*. Edward Elgar Publishing.
[69] Crane, A. (2008). *Corporations and citizenship*. Cambridge: Cambridge University Press. Retrieved from http://www.loc.gov/catdir/enhancements/fy0834/2008019385-t.html; Matten, D., & Crane, A. (2005). Corporate Citizenship: Toward an Extended Theoretical Conceptualization. *Academy of Management Review*, 30(1), 166–179.
[70] Porter, M. E., & Kramer, M. R. (2002). The competitive advantage of corporate philanthropy. *Harvard Business Review*, *80*(12), 56–68.
[71] Cavanagh, G. F. (2004). Global Business Ethics: Regulation, Code, or Self-Restraint. *Business Ethics Quarterly*, *14*(4), 625–642. https://doi.org/10.5840/beq200414436
[72] Evans, P. (1997). The Eclipse of the State? Reflections on Stateness in an Era of Globalization. *World Politics*, *50*(1), 62–87.; Vernon, R. (1968). Economic Sovereignty at Bay. *Foreign Affairs*, *47*(1), 110–122. https://doi.org/10.2307/20039358

multinationals which are developing technologies of national interest, but are increasingly beyond the state's control (section 1.1.2.3).

1.1.2.1 World War II and the growth of the military industrial complex [1942 – 1990]

Prior to the 1940s, the responsibility for sustaining the U.S. defense industrial base fell for the most part on the shoulders of the government; the commercial industry was only drawn upon on occasion to supplement government owned arsenals during times of conflict. Then, the beginning of World War II marked a turn in the commercial industry towards full-scale military engagement. The demand for new wartime technologies spurred President Roosevelt to establish the War Production Board – a federal agency tasked with conscripting the largest U.S. industrial enterprises into wartime service. Commercial actors became critical to the U.S. war effort, serving as the 'Arsenal of Democracy' which enabled the U.S. to overwhelm its adversaries with its industrial capacity and power. National defense became the country's largest industry, skyrocketing to roughly 40% of GDP from a mere 3% in the 1930s[73].

As the war ended, the commercial industry – which had been substantially bolstered by government support and had built up significant industrial infrastructure during wartime – reoriented back toward commercial markets while still retaining their defense production capabilities. These companies, joined in later years by giants such as AT&T, General Electric, and IBM, moved fluidly between the commercial and military markets. They excelled for a time, having benefitted from continued financial backing from the Pentagon; in turn, these large industrial firms became a wartime legacy which grounded American economic dominance and international competitiveness for decades. President Eisenhower famously termed this 'the military industrial complex', which he actively supported via his New Look policy and via the Department of Defence's 'path to commercialization' efforts in the 1950s,

[73] Lynn, W. J. (2014). The End of the Military-Industrial Complex. *Foreign Affairs*, (November / December 2014). Retrieved from https://www.foreignaffairs.com/articles/united-states/end-military-industrial-complex

the latter of which was critical for enabling companies to incubate dual-use technologies[74]. The military industrial complex was further strengthened by the mobilization for the Cold War, which sparked the enactment of the *Defense Production Act* of 1950 as a mechanism to ensure that the government had access to commercial production capacities for its defense needs[75].

1.1.2.2 The end of the Cold War and the shrinking of state spending [1960 – present]

In the early 1960s, concerns about cost overruns ushered in the beginning of an extended and steady decline in the state's dominance in technology R&D spending. In 1960 U.S. expenditure on military R&D constituted one third of all R&D spending aggregated across all OECD member countries; by 1990 this had fallen to one seventh. In contrast, privately funded R&D had been growing 2.5 times faster than public R&D spending since 1960. By 1980, the aggregate of commercially funded R&D efforts in the U.S. overtook government-funded R&D programs.

Simultaneously, in the early 1960s the full force of the internationalisation of the global economy hit national markets and punctured national borders. Substantial improvements in transportation and communication technologies paired with an era of deregulation in trade and capital movements triggered the proliferation of multinational corporations. These enterprises took the form of clusters of private firms scattered across multiple countries, joined through ties of common ownership and an overarching global corporate strategy. Ford, Nestle, IBM and Philips were prominent examples at the time. In time, these

---

[74] Eisenhower's New Look policy is acknowledged to have set the stage for the blossoming of a unique defense industrial base and the creation of new dual-use commercial sectors in electronics, space, and computing. This led to many of the technological advances that went on to serve as the basis for U.S. military strength – including intercontinental ballistic missiles, nuclear-powered submarines, advanced bombes, reconnaissance satellites, electronics, and communications technology.

[75] Gansler, J. S., Greenwalt, W. C., & Lucyshyn, W. (2013). *Non-traditional Commercial Defense Contractors*. Retrieved from Center for Public Policy and Private Enterprise website: file:///C:/Users/Jade/Downloads/UMD_12010_Non-Traditional%20Commercial%20Defense%20Contractors_November%202013.pdf

enterprises adopted a global identity – the distinction between 'home' and 'foreign' markets started to blur and market incentives rewarded these businesses for pursuing strategies that ignored the constraints of geography in pursuit of larger markets and efficiency gains.

The U.S. government began to feel the tension between the political and nationally bounded state defense system, and the economic and nationally ambivalent private commercial system[76]. The state's response to this tension was twofold. Firstly, the U.S. commercial industry was bifurcated into those serving the civilian versus the military industrial bases. Those with a civilian focus found it increasingly costly to participate in the DOD market and turned instead towards emerging industries such as computers and electronics[77]. On the defense side, the Pentagon increasingly urged for consolidation and specialization in light of the shrinking post-war defense budget. From 1992 to 1997, a total of $55 billion in industry mergers took place, the results of which were the shifting out of large conglomerates from the defense industry and the emergence of a new cadre of defense-only firms which still dominate the industry today[78].

In parallel, the state began to focus on accessing commercial sources of innovation and technology products. In 1986 President Reagan created a Blue Ribbon Commission on Defense Management with the stated goals of reducing inefficiencies in the defense procurement and acquisition processes to better enable the DOD to access cutting edge technologies being developed in the commercial sector. This triggered a period of commercial item acquisition reform, which began in the early 1990s and resulted in a range

[76] This became particularly salient when multinational enterprises dominated industries that were considered of core national interest – including the development of science and technology for national defense, security, and leadership. See (Evans, 1997; Vernon, 1968)

[77] Increased barriers to participation for commercial firms included: the development of complicated government procurement and oversight requirements; greater government control over intellectual property; great export control restrictions; and a growing bias from the Pentagon against the use of commercial products.

[78] In 1993 the DOD invited industry leaders to the Pentagon to meet with then Deputy Secretary of Defense William Perry, who urged for industry consolidation. The main outcomes were the selling off of defense operations by large conglomerates, and the selling off of commercial operations by defense companies (as well as the acquisition of smaller defense companies). See (Lynn, 2014)

of efforts to incorporate commercial technologies and business practices into DOD systems and to entice commercial actors into the federal marketplace[79].

Despite the government's attempts to adapt to the changing nature of technology development, American prowess in science and technology took a significant downturn in the 1980s. Confronted with an increasingly multipolar world order, accelerating technological change, and reductions in barriers to trade and capital mobility, the position of American firms in the world market began to decline[80]. The U.S. government proved slow to adapt particularly in high technology industries, consequently losing ground to competitors abroad. Lewis Branscomb, a prominent adviser and scholar to the U.S. government on science and technology policy, observed that the U.S. government had failed to adapt to a world in which 'international competitiveness…are replacing military strength as the most urgent objectives of national and world-wide security'[81]. The decline in competitiveness of U.S. firms was thus not only a threat to American economic security, but to American national security[82].

1.1.2.3 The rise of technology multinationals [2000 - present]

The transition from state-led to industry-led R&D, combined with the decline in American technological leadership, created the conditions for political tensions between the state and firms that we see playing out today. Critically, significant cutbacks in state R&D capacity placed the U.S. government in a position of relying on multinational technology firms in

---

[79] Specific achievements include:
- Embedding commercial technologies into DOD weapons and command and control systems;
- The enactment of the Federal Acquisition Streamlining Act (FASA) in 1994 establishing a preference for commercial sector goods over specially produced ones;
- A Technology Reinvestment Program, led by the Department of Defense, which was focused on spinning out dual-use technologies from defense technologies; and
- The Advanced Technology Program, a federal-private cooperative effort led by the National Bureau of Standards and Technology.

See (Gansler et al., 2013; V. Ruttan, 2006).

[80] Branscomb, L. M. (1992b). U.S. scientific and technical information policy in the context of a diffusion-oriented national technology policy. *Government Publications Review*, *19*(5), 469–482. https://doi.org/10.1016/0277-9390(92)90050-L

[81] (Branscomb, 1992a)

[82] Alic, J. A. (1994). The dual use of technology: Concepts and policies. *Technology in Society*, *16*(2), 155–172. https://doi.org/10.1016/0160-791X(94)90027-2

order to meet core national economic and defense needs. By way of illustration, in 1987 the DOD accounted for 40% of R&D spending in the U.S.; by 2013 this had dropped to less than 20%. Comparably, the commercial sector has increased its R&D expenditure by over 200% during the same period, accounting for over 60% of R&D funding and over 70% of performance advances in key technology sectors[83]. Not only does the U.S. government not dominate U.S. R&D spending any longer; the U.S. is waning in global R&D spending as global commercial R&D continues to rise and evermore commercial technologies are being developed outside of the U.S..[84]

Within the commercial industry, U.S. defense companies – upon whom the government typically relies on for technology production – are also lagging further behind high technology multinational companies both in performance and levels of R&D investment. The combined R&D budgets of the five largest U.S. defense contractors amounts to less than half of what companies such as Microsoft and Google spend on R&D in a single year; from 2000 to 2012 R&D spending at defense firms dropped from 3.5% to 2% of sales compared to an average of 8% being invested in R&D at commercial technology companies. Google's market value alone – estimated at approximately $400 billion – is over double that of General Dynamics, Northrop Grumman, Lockheed Martin, and Raytheon combined[85]. As such, technologies that are of critical importance to the state – such as robotics and cybersecurity – are being developed in the commercial information technology industry, and the defense industry are struggling to compete.

In practice, this has shifted control over the development and deployment of strategic technologies away from the state and towards these high technology multinational

[83] GAO. (2017). *Military Acquisitions: DOD Is Taking Steps to Address Challenges Faced by Certain Companies*. Retrieved from United States Governmance Accountability Office website: https://www.gao.gov/assets/690/686012.pdf

[84] The U.S. government as of 2013 accounts for approximately 11% of global R&D spending; the U.S. private sector accounts for 17%. See (Gansler et al., 2013)

[85] (Lynn, 2014)

companies. For one, from the perspective of these companies the state is but a minor customer among a global customer base of hundreds of millions of users[86]. The volume of funding in the commercial sector certainly dwarfs the investment capital and purchasing power exercised by the DOD, constraining the state's ability to exert much influence over technologies that are being developed outside of their remit and intended primarily for commercial and civilian use[87]. Further, several studies and reports, some commissioned by the government itself, have identified a host of challenges that deter commercial companies from selling their products and services to the DOD or further developing their products and services for military use[88].

Several cultural factors have also contributed to an increasingly fraught relationship between multinational technology companies and the U.S. government. Leaders of Silicon Valley companies have demonstrated an unwillingness to engage in contracts with the governments in protest of how their technologies could be used in defense and security contexts, expressing a deep distrust of the state. From the state's perspective, a return of a culture of risk aversion and a fear of the national security risk posed by globalized technology markets have eroded their relationships with multinational, high-growth companies[89]. Notwithstanding a few efforts on the part of the DOD to build bridges with Silicon Valley

---

[86] For the top innovative U.S. companies, the percentage of sales and revenue derived from DOD contracts in 2016 are less than 2%. See (GAO, 2017)

[87] Fitzgerald, B., & Parziale, J. (2017). As technology goes democratic, nations lose military control. *Bulletin of the Atomic Scientists*. Retrieved from https://thebulletin.org/2017/03/as-technology-goes-democratic-nations-lose-military-control/

[88] These challenges include:

- The complexity of DOD processes
- The unstable budget environment
- Long contracting timelines
- Intellectual property rights concerns
- Government-specific contract terms and conditions
- An inexperienced DOD contracting workforce
- Elaborate regulations for the acquisition of weapons, including auditing and oversight regulations which require the establishment of new and costly accounting systems beyond what would be needed for commercial business

See: (GAO, 2017; Lynn, 2014)

[89] (Fitzgerald & Parziale, 2017; Gasser et al., 2016; Lynn, 2014)

companies, the levels of antagonism between the government and technology firms may be at their worst since the advent of the acquisition reforms in the early 1990s[90].

Given this adversarial dynamic, recent IR scholarship has reinvigorated the debate about the power of big business and its implications for the state, pulling on threads of the original wave of literature responding to the novelty of globalization in the 1970s[91]. Some scholars mirror the claims of the all-powerful global corporation, characterizing technology companies as political actors who wield significant power beyond the control of the nation state; predictions of the decline of the nation state have followed with the rise of these 'private superpowers' increasingly capable of delivering core functions of the state[92]. Conversely, others frame these technology companies as ultimately constrained by external socio-political pressures and regulatory environments and as such remain in a state of interdependence with the government[93]. The concept of the *Entrepreneurial State,* popularized by Mazzucato in 2011, encapsulates the argument for why even the high-technology firms

---

[90] Such efforts include:

- The creation of the Defense Innovation Unit (DIU) in 2015 as an outreach effort focused on pursuing innovative ways to sustain and advance emerging technology capabilities, using OTAs to enter into agreements with industry for prototyping projects;
- The creation of the Defense Digital Service in 2016 to help the military incorporate practices such as 'bug bounties';
- Several provisions included in the National Defense Authorisation Act (NDAA) in 2016 and 2017 aimed at eliminating some contract terms and conditions that are burdensome to non-traditional defense contractors;
- Establishing industry outreach offices in high-technology areas across the country; and
- Piloting new streamlined ways of doing business with companies with desired completion period of 60 days;

See (Fitzgerald & Parziale, 2017; GAO, 2017)

[91] Mikler, J. (2018). *The political power of global corporations*. Cambridge, UK: Polity Press.; Moore, M., & Tambini, D. (2018). *Digital dominance: the power of Google, Amazon, Facebook, and Apple*. New York: Oxford University Press.

[92] Dasgupta, R. (2018). The demise of the nation state. *The Guardian*. Retrieved from https://www.theguardian.com/news/2018/apr/05/demise-of-the-nation-state-rana-dasgupta; Fuchs, D. A. (2007). *Business power in global governance.* Lynne Rienner Boulder, CO.; Fuchs, D. (2013). Theorizing the Power of Global Companies. In J. Mikler (Ed.), *The Handbook of Global Companies*. Chichester: John Wiley & Sons Inc.; Garton Ash, T. (2016). *Free speech: ten principles for a connected world.* London: Atlantic Books.; Noble, S. U. (2018). *Algorithms of oppression: how search engines reinforce racism*. New York: New York University Press.

[93] May, C. (2015a). *Global corporations in global governance*. Routledge.; Schwarz, J. A. (2017). Platform Logic: An Interdisciplinary Approach to the Platform-Based Economy. *Policy & Internet*, *9*(4), 374–394. https://doi.org/10.1002/poi3.159; Srnicek, N. (2017). *Platform capitalism*. Cambridge, UK; Malden, MA: Polity Press.

of today remain reliant on the nation state[94]. In the context of strategic GPTs, Mazzucato posits that the state remains central to technological innovation, particularly in making bets on technologies upon which the likes of Google and Apple rely on to fuel their latest technology products. This continues to be a live debate today.

1.1.3 Researchers and researcher influence in politics

In the context of developing and deploying cutting edge technologies, researchers are a distinct actor in the technology life cycle, serving particular interests and exercising a form of political influence. In literature, some elements of their distinctive nature as political actors have been captured. As a community of technical experts, researchers have been conceptualized as epistemic communities whose primary political relationship is with the state, and whose mechanisms of influence centre on pushing for specific policy measures (section 1.1.3.1). As employees of firms, researchers have alternatively been conceptualized as professionals whose interests and mechanisms of influence are mostly economic in nature (section 1.1.3.2).

Neither of these angles are sufficient to capture the role of researchers in a politicized technology life cycle, in which their interests are a combination of economic and social, and their mechanisms of influence are based on a combination of their relationships with their firms as employers and with the state as funders and legislators. Section 1.1.3.3 covers two example case studies in which researchers have been described in this manner.

1.1.3.1 Epistemic communities

The concept of epistemic communities was first introduced into IR literature in a 1992 special issue of International Organization titled 'Knowledge, Power, and International

[94] Mazzucato, M. (2011). *The entrepreneurial state*. London: Demos.

Policy Coordination"[95]. As originally conceived, epistemic communities are networks – often transnational – of knowledge-based experts with an authoritative claim to policy relevant knowledge within their domain of expertise. Members of the epistemic community share, among other things: common values or principled beliefs; shared knowledge and professional judgement within their area of expertise; and a common set of policy goals and convictions. Their authority rests on the individual members' reputation for impartial expertise; such individuals may be based within and move between multiple institutions across academia, government, and industry[96].

Epistemic communities are particularly relevant when expert input is considered important. This is often the case when a specific issue is both politically salient as well as uncertain in nature, where the uncertainty is believed to be partially resolvable with technical information[97]. The mechanism by which epistemic communities gain influence is thus in the provision of this information, particularly as inputs into shaping a state's policy choice[98]. Further, epistemic communities more generally circulate causal ideas and associated normative beliefs which shape the state's preferences and influences the form and content of state-led negotiated outcomes[99]. Notable case studies of this have been in the context of

[95] Haas, P. M. (1992a). Epistemic communities and international policy coordination. *International Organization*, *46*(1), 1–35. https://doi.org/DOI: 10.1017/S0020818300001442
[96] Haas, P. (2008). Epistemic Communities. In *The Oxford Handbook of International Environmental Law*. https://doi.org/10.1093/oxfordhb/9780199552153.013.0034
[97] There are several other conditions that describe contexts in which epistemic communities matter, including the ability for said epistemic communities to access decision makers, the coherence of the policy field, and the stage of the policy debate in the process of overall decision making. See: Cross, M. K. D. (2013). Rethinking epistemic communities twenty years later. *Review of International Studies*, *39*(1), 137–160. https://doi.org/10.1017/S0260210512000034
[98] Haas, P. M. (1992b). Introduction: Epistemic Communities and International Policy Coordination. *International Organization*, *46*(1), 1–35.
[99] Morisse-Schilbach, M. (2015). "Changing the world": epistemic communities, and the democratizing power of science. *Innovation: The European Journal of Social Science Research*, *28*(1), 18–26. https://doi.org/10.1080/13511610.2014.943163

arms control negotiations in which the role of individuals and groups of scientists in shaping state strategies has been well documented[100].

Since its introduction into IR literature, the concept of epistemic communities has largely not evolved; its study has been limited to a range of specific and narrow case studies of state policy influence by scientists[101]. This has left much unaddressed under the umbrella of understanding how a collection of actors with recognized expertise, shared policy goals, and a willingness to act can be politically influential in today's world. Critics have particularly emphasized the need for epistemic communities to be understood as actors with personal strategic interests that are not simply a reflection of their professional expertise; this thus calls for the politicization of epistemic communities in order to understand why and how they could be influential[102].

One promising extension of the concept has been in the direction of broadening the scope of those susceptible to epistemic community influence to include non-state actors. As the global governance literature began to broaden out to include the role of non-state actors (section 1.1.1), the concept of epistemic communities bled into the concept of transnational communities and private arenas of governance. Transnational communities – including professional and epistemic communities – were described as gaining in salience given the

---

[100] Adler, E. (1992). The emergence of cooperation: national epistemic communities and the international evolution of the idea of nuclear arms control. *International Organization*, *46*(1), 101–145. https://doi.org/DOI: 10.1017/S0020818300001466; Barth, K.-H. (2003). The Politics of Seismology: Nuclear Testing, Arms Control, and the Transformation of a Discipline. *Social Studies of Science*, *33*(5), 743–781. https://doi.org/10.1177/0306312703335005; Greene, B. P. (2015). "Captive of a Scientific-Technological Elite": Eisenhower and the Nuclear Test Ban. *Presidential Studies Quarterly*, *45*(1), 29–45. https://doi.org/10.1111/psq.12169; Hecht, D. (2016). Scientists at War: The Ethics of Cold War Weapons Research. *Journal of American History*, *102*(4), 1255.2-1256. https://doi.org/10.1093/jahist/jav717; Hymans, J. E. C. (2012). Achieving nuclear ambitions: scientists, politicians and proliferation. Cambridge: Cambridge University Press.; Ouagrham-Gormley, S. B. (2014). *Barriers to Bioweapons: The Challenges of Expertise and Organization for Weapons Development*. Cornell University Press.

[101] Löblová, O. (2018). When Epistemic Communities Fail: Exploring the Mechanism of Policy Influence. *Policy Studies Journal*, *46*(1), 160–189. https://doi.org/10.1111/psj.12213

[102] Dunlop, C. (2000). Epistemic Communities: A Reply to Toke. *Politics*, *20*(3), 137–144. https://doi.org/10.1111/1467-9256.00123; Krebs, R. R. (2001). The Limits of Alliance: Conflict, Cooperation, and Collective Identity. In A. Lake & D. A. Ochmanek (Eds.), *The real and the ideal : essays on international relations in honor of Richard H. Ullman*. Lanham, Md.: Rowman & Littlefield Publishers.

globalization of economics and governance[103]. Consequently, epistemic communities were described as increasingly influential on non-state actors in shaping governance more broadly, rather than specific government policies[104]. In the arena of global business, for example, epistemic communities such as the International Telecommunication Union (ITU) shaped international standards and laws propagated by international bodies, which were ultimately imposed on member states[105].

1.1.3.2 Professional networks

The concept of professionalization is closely related to that of epistemic communities, where professionalization of a network of experts enables them to exercise influence in a specific domain[106]. Critically, the difference between professional networks and epistemic communities is that the former does not share principled beliefs nor a common policy enterprise[107]. Rather, professional networks typically express a narrower set of concerns related to professional objectives such as economic security and labour rights.

The mechanisms of influence that professionals exercise include, among others: using their expertise and legitimacy to challenge incumbent orders; introducing new rules and standards to redefine the boundaries of the field; and using their social capital to introduce new ideas or create new institutions in the field[108]. Several empirical case studies document these mechanisms playing out in practice, including: the influence of German unions in the twentieth century on negotiating pay and working conditions[109]; the organization of museum

---

[103] Djelic, M.-L., & Quack, S. (2010). *Transnational communities : shaping global economic governance*. Cambridge: Cambridge University Press.
[104] Graz, J.-C., & Nölke, A. (2008). *Transnational private governance and its limits*. London: Routledge.
[105] Braithwaite, J. (2000). *Global business regulation*. Cambridge: Cambridge University Press.
[106] For an overview of the concept of professionalization, see Macdonald, K. M. (1995). *The sociology of the professions*. London: Sage.
[107] (P. M. Haas, 1992a)
[108] Suddaby, R., & Viale, T. (2011). Professionals and field-level change: Institutional work and the professional project. *Current Sociology*, *59*(4), 423–442. https://doi.org/10.1177/0011392111402586
[109] Schmitter, P. C., & Streeck, W. (1985). *Private interest government : beyond market and state*. London: Sage.

staff in advocating for specific policies[110]; and the strategic professionalization within a large international law firm to push for internal policy changes[111].

1.1.3.3 Researchers in a technology ecosystem

The concepts of epistemic communities and professional networks contributes partially but incompletely to describing the role that researchers could and do play in a technology ecosystem. In such an ecosystem, researchers combine the societally-oriented policy interests of epistemic communities with the private economic interests of professionals. Further, researchers simultaneously negotiate their relationship with firms as employees alongside their relationship with the state as funders and regulators of their research institutions and activities.

A case study of Silicon Valley in the 1990s captures some of these complexities[112]. By examining the institutions in and around Silicon Valley computer companies, the study reveals the motivations, coherence, and organizational capacities of the scientists and engineers, and consequently the impact that this group has had on the evolution of companies, industries, and communities in the region. The author, Saxenian, recounts the habit of informal cooperation among Silicon Valley engineers which encouraged a strong sense of community and common commitment to 'the cause of advancing technology' which superseded commitment to individual companies or industries. 'Even under relentless competitive pressures', Saxenian reflects, 'an underlying loyalty and shared commitment to technological excellence unified members of this industrial economy'.

---

[110] DiMaggio, P. J., & Powell, W. W. (1983). The Iron Cage Revisited: Institutional Isomorphism and Collective Rationality in Organizational Fields. *American Sociological Review*, *48*(2), 147–160. https://doi.org/10.2307/2095101

[111] Empson, L., Cleaver, I., & Allen, J. (2013). Managing Partners and Management Professionals: Institutional Work Dyads in Professional Partnerships. *Journal of Management Studies*, *50*(5), 808–844. https://doi.org/10.1111/joms.12025

[112] Saxenian, A. (1994). Regional advantage : culture and competition in Silicon Valley and Route 128. Cambridge, Mass: Harvard University Press.

In a study of the biotechnology industry, Vallas & Kleinman also add texture to the conception of researcher communities in a technology ecosystem with both academic and corporate influences[113]. Beginning in the 1980s, they recount the shift in the public expectation of publicly funded academic research towards generating economic value and enabling capital accumulation[114]. This triggered faculties and university administrators to look towards market-based sources of support and legitimacy. Ultimately, this led many to critique the erosion of traditional academic norms in the face of growing university-industry relationships; this was particularly salient in biotechnology research[115]. In the process of tracing the increasing blurring between academic and corporate research cultures in biotechnology, Vallas & Kleinman conclude that the logics of science and industry are by no means as incompatible as these critiques would suggest[116]. Rather, as market pressures and entrepreneurial practices have pervaded academia, university-like codes and practices have increasingly been adopted by science-intensive firms.

1.1.4 Summary

The political environment surrounding the development of a strategic GPT creates specific conditions that magnify and warp the nature of the actors engaged in these politics. Multinational technology firms have become a focal point of power by virtue of their capacity to innovate at the leading edge of technological development. As their clout increases, however, so does their interdependence on elements of the global governance and domestic

---

[113] Vallas, S. P., & Kleinman, D. L. (2008). Contradiction, convergence and the knowledge economy: the confluence of academic and commercial biotechnology. *Socio-Economic Review*, *6*(2), 283–311. https://doi.org/10.1093/ser/mwl035

[114] Powell, W. W., & Owen-Smith, J. (1998). Universities and the Market for Intellectual Property in the Life Sciences. *Journal of Policy Analysis and Management*, *17*(2), 253–277. Retrieved from JSTOR.; Slaughter, S., & Leslie, L. L. (1997). *Academic capitalism : politics, policies, and the entrepreneurial university*. Baltimore: Johns Hopkins University Press.; Slaughter, S., & Rhoades, G. (2004). *Academic capitalism and the new economy : markets, state, and higher education*. Baltimore: Johns Hopkins University Press.

[115] Blumenthal, D., Gluck, M., Louis, K. S., Stoto, M. A., & Wise, D. (1986). University-Industry Research Relationships in Biotechnology: Implications for the University. *Science*, *232*(4756), 1361–1366. Retrieved from JSTOR.

[116] Brint, S. G. (2002). The future of the city of intellect : the changing American university. Stanford, Calif.: Stanford University Press.

political systems. The literature conceptualizing the rise of private actors as political agents in the international system goes some way towards capturing these interdependencies. However, it falls short of specifically examining today's high technology multinational companies which are engaging in the development of strategic technologies and thus are of unique political salience. The bounds of their power, particularly vis a vis the state, remain contested topics in IR scholarship.

The state, conversely, becomes more dependent on these firms for access to the technologies required to maintain and strengthen national defense and security capabilities. Simultaneously, the state has a stronger impetus to exercise control over commercial firms given their relevance to national strategic interests. The literature to date captures the evolution of the U.S. government towards this state of dependence, documenting the pushes and pulls at play which forced the state's hand at various points across recent decades. In assessing the current capacities of the state, however, there is little to point to which analyses what the state is and can be capable of, and what they have and would be willing to do, in order to address their diminishing control over the development of critical technologies.

Finally, researchers and research communities are rarely addressed in IR literature. Where they have been acknowledged, it is often in the framing of crudely narrow interests – whether that be clear-eyed truth-seeking policy advocacy from epistemic communities, or private economic interests from professional networks. In high technology domains for which fundamental research is particularly important for progress, it is critical that researchers are conceptualized as both economic and social actors with strategic interests and political influence. Indeed, in these settings researchers often possess more influence than is often conveyed in case studies from other industries.

1.2 Research design

Let us bring this back to the case at hand – the global competition for leadership in AI, and the fraught politics at a national level that ensues. In this pursuit, actors find themselves braced for conflict as they negotiate for control and influence over the trajectory of AI development and deployment. States are pursuing AI as a matter of national interest, namely global economic dominance and military power. Private firms are chasing the profit that AI promises, driving for rapid commercialization and global proliferation of the technology, often with little regard for matters of national security and civil liberties. Researchers are pursuing AI, often as employees of firms but also as members of a transnational academic community underpinned by norms of openness and exchange; these can run counter to the goals of national security and proprietary profit held by states and firms, respectively.

The emerging case of AI provides insufficient evidence for meaningful analysis. This thesis aims to generalize this case in a way that enables the use of historical case studies to inform our analysis of AI. In the following section, I describe how this history will be dissected to find common drivers, trends and outcomes that describe the general trajectory of this type of technology pursuit.

1.2.1 Research objectives

The central claim that motivates this research is as follows:

> The development and deployment of a strategic general purpose technology follows a distinct pattern of politics. Specifically, a generalizable set of synergies and conflicts emerges between the state, firms and researchers across the technology life cycle. By modelling this pattern of politics for the general case of a strategic general purpose technology, we can make predictions about how the politics of artificial intelligence will unfold.

This breaks down into three sequential research objectives:

(1) *Develop a general model* for the development and deployment of a strategic GPT in terms of the synergies and conflicts that emerge between states, firms and researchers;

(2) *Validate and strengthen the model* by drawing on historical case studies of strategic GPTs that possess similar properties to AI;

(3) *Benchmark AI as a case study* by using the model as a framework and assessing the trajectory of development and deployment of AI to date in the U.S.

1.2.2 Methodology

1.2.2.1 Defining a strategic general purpose technology

A strategic GPT is defined as follows[117]:

> A general purpose technology which has the potential to deliver vast economic value and substantially affect national security, and is consequently of central political interest to states, firms, and researchers.

AI is an emerging strategic GPT. Hence, the applicable reference class of historical case studies are strategic GPTs that have already been developed and deployed. The three characteristics which define strategic GPTs are: its economic value, security relevance, and general purpose nature.

1.2.2.1. Economic value

A strategic GPT has the potential to generate substantial economic value. Critically, this economic value should be able to be directly captured by the developers of the

[117] A sincere thank you to Allan Dafoe and Pepper Culpepper, with whom I developed and refined the concept of a strategic GPT over the course of my Confirmation of Status examination.

technologies[118]. The capacity to gain proprietary wealth means that actors such as firms have strong incentives to pursue the development of a strategic GPT for private gain.

Such substantial economic value naturally arises from the general purpose nature of the technology – that is, its applicability across a wide range of domains and economic sectors. Its many valuable applications mean that the technology is rapidly and broadly proliferated across the economy, resulting in ample opportunity for profiting from its development and deployment.

1.2.2.1. Security relevance

The security relevance of a strategic GPT has two dimensions. Firstly, strategic GPTs can have *military value* – the potential for the technology to transform the competencies of a given military force. Secondly, strategic GPTs can pose *security risks* – the potential for the deployment of the technology to cause harm to the public and/or to the state. The security relevance of the technology guarantees the involvement of the state. Indeed, only one of these dimensions of security relevance need apply in order for a technology to capture the interest and resources of the state.

The *military value* of a technology manifests in a number of ways. A technology can introduce new capabilities which alter important strategic parameters in warfare such as the offense defense balance and the asymmetry of information[119]. It may enable expansion into an entirely new domain of activity; aerospace technologies, for example, revolutionised warfare by extending the bounds of the battleground to the air and then to outer space.

---

[118] The emphasis on direct economic value is intended to exclude technologies for which the economic value is indirect, and thus private actors would not face incentives to develop the technology without state intervention. An example of indirect economic value would be when a technology causes a general increase in the country's gross domestic product (GDP) in the long-run, but in the short-run has the characteristics of a public good (e.g. transportation infrastructure).

[119] Glaser, C. L., & Kaufmann, C. (1998). What is the Offense-Defense Balance and Can We Measure it? *International Security*, 22(4), 44–82. https://doi.org/10.2307/2539240. For an example of how emerging technologies can change the offense-defense balance, see: Zilinskas, R. A. (2000). *Biological warfare: modern offense and defense*. Lynne Rienner Publishers.

Transformative military technologies may also substantially augment existing capabilities, thereby strengthening one's strategic advantage. The use of satellite technology to augment reconnaissance and surveillance activities during the Cold War[120] and the integration of information technologies into command and control systems[121] are two salient examples of this.

Strategic GPTs may pose *security risks* by causing substantial harm to the public and/or to the state. Harm may arise from malicious use of the technology, the occurrence of accidents involving the technology, or the emergence of structural risks as a consequence of development and deployment[122]:

- The risk of *malicious use* arises when an actor wields the technology with the intention of causing harm. Malicious actors include non-state actors such as terrorist groups, criminal networks and rogue individuals. From the perspective of a state, a malicious actor may also be an adversarial state perceived to have hostile intentions[123].
- The risk of *accidents* implies unintentional harm arising from the development and/or deployment of the technology. Accidents typically arise as a result of technology systems behaving in ways that run counter to the intentions of the builder or the user

[120] For a detailed recount of the United States' efforts at developing satellite technology for the purposes of intelligence, surveillance and reconnaissance (ISR) on the Soviet Union, see: Arnold, D. C., & McCartney, F. S. (2005). *Spying from space: constructing America's satellite command and control systems (1st ed.*). College Station: Texas A&M University Press.

[121] The United States Department of Defense, for example, have as of 2000 announced their strategy for pursuing 'network centric warfare' which centres on leveraging information technologies to augment American military capabilities. See: Alberts, D. S., Garstka, J. J., & Stein, F. P. (2000). *Network Centric Warfare: Developing and Leveraging Information Superiority*. Washington, D.C.: United States Department of Defense. Retrieved from https://www.hsdl.org/?abstract&did=805186

[122] Zwetsloot, R., & Dafoe, A. (2019). Thinking About Risks From AI: Accidents, Misuse and Structure. *Lawfare*. Retrieved from https://www.lawfareblog.com/thinking-about-risks-ai-accidents-misuse-and-structure

[123] Note that the term 'malicious' as used here is a matter of perception. For example, from the perspective of state A, state B may be behaving maliciously if they are using a strategic GPT to strengthen their military offensive and defensive capabilities. However, for state B, this behaviour is consistent with them pursuing the technology for its military utility.

of the technology and can often be related to under investments in safety mechanisms.

- *Structural risks* emerge across a longer time period as a function of the strategic environment that actors find themselves within. Examples include the erosion of strategic stability, a collective avoidance of instituting standards of ethics and safety, and the steady elimination of an individual's access to employment or education. The driver of these risks lies in the tension between the strong incentives to pursue the development of the technology and the comparably weak incentives to coordinate to prevent the unintended consequences that result from this unchecked pursuit.

1.2.2.1. General purpose nature

As the name suggests, this category of technologies must be general purpose in nature. General purpose technologies (GPTs) are described as having an unusually broad and deep impact on the world, comparable to that of electricity, the internal combustion engine, and computers[124].

This is, firstly, an important characteristic for underlining the economic value of a strategic GPT. Over decades or more, GPTs alter the nature of economic productivity, causing substantial shifts in the growth trajectory of states and empires, as well as the broader trajectory of human civilisation across the centuries[125]. Electricity and modern information technology are canonical examples of GPTs that have penetrated deeply across society and have had transformative impacts on economic productivity and growth[126].

[124] General purpose technologies (GPT) is a label first couched by Timothy Bresnahan and Manual Trajtenberg in: Bresnahan, T. F., & Trajtenberg, M. (1992). General Purpose Technologies "Engines of Growth?" *National Bureau of Economic Research Working Paper Series*, *No. 4148*. https://doi.org/10.3386/w4148.
[125] Jovanovic, B., & Rousseau, P. L. (2005). General purpose technologies. In P. Aghion & S. Durlauf (Eds.), *Handbook of Economic Growth* (pp. 1182–1224). Elsevier.
[126] David, P. A., & Wright, G. (1999). *General purpose technologies and surges in productivity: historical reflections on the future of the ICT revolution*. Oxford: University of Oxford.

Secondly, the general purpose nature guarantees the extended involvement of researchers in the development and deployment of technology products and applications. GPTs are defined by their broad and fundamental nature. This means that complementary innovations and new market opportunities are continually being made possible, hence the continued relevance of early stage R&D.

Finally, the general purpose nature of the technology lends it to being a dual-use technology. Dual-use is defined as the simultaneous applicability of the technology to both commercial and defense domains[127]. It can apply to both research and knowledge as well as products and applications[128]. The convergence of commercial and military applications is important, as this is the premise by which both firms and the state have a stake in the technology. Dual-use can also be taken to more broadly refer to technologies that are both beneficial and harmful, depending on how they are used. A technology can be dual-use, for example, if it was designed to be used for civilian purposes, but its development and deployment raises the risk of unintended harm via accidents or negative externalities[129]. A dual-use technology may also have been designed to be used for civilian purposes, but the same technology may be used by malicious actors to cause harm[130]. This ultimately brings the economic interests of firms into tension with the state's concern for mitigating security risks.

1.2.2.2 Case study selection

In addition to the requirement of the technology being a strategic GPT, it is also important that the case study takes place in an analogous national and international political setting to

[127] Forge, J. (2010). A Note on the Definition of "Dual Use." *Science and Engineering Ethics*, *16*(1), 111–118. https://doi.org/10.1007/s11948-009-9159-9
[128] Harris, E. D. (2016). *Governance of Dual-Use Technologies: Theory and Practice*. Cambridge, MA: American Academy of Arts and Sciences.; Rappert, B., & Selgelid, M. J. (2013). *On the dual uses of science and ethics: principles, practices, and prospects*. Canberra: ANU E Press.; Tucker, J. B. (2012). *Innovation, dual use, and security: managing the risks of emerging biological and chemical technologies*. Cambridge, Mass.: MIT Press.
[129] Tucker, J. B. (2012). *Innovation, dual use, and security: managing the risks of emerging biological and chemical technologies*. Cambridge, Mass.: MIT Press.
[130] Forge, J. (2010). A Note on the Definition of "Dual Use." *Science and Engineering Ethics*, *16*(1), 111–118. https://doi.org/10.1007/s11948-009-9159-9

the one that we find ourselves in for AI. This means that the state should be considered a leading technology power in the context of the Westphalian world order. History must also have sufficiently run its course such that the technology has progressed through the life cycle of fundamental research through to commercial application, industry growth and consolidation, and technology maturation.

The case studies that fulfil these properties are limited in number – by definition, history features very few truly transformative GPTs that have been strategically critical for economic growth and military leadership. The candidate strategic GPTs identified are listed in Table 1.2-1. The three case studies ultimately selected for analysis are aerospace technology, biotechnology and cryptography due to ranking highest in aggregate across the properties.

Table 1.2-1: Candidate strategic general purpose technologies

Technology	*Property*		
	Economic value	*Security relevance*	*General purpose*
Aerospace technology	High	High	Moderate
Biotechnology	High	High	High
Cryptography	High	High	High
Nanotechnology	Unclear	Unclear	High
Laser technology	Moderate	Low	Moderate
Microprocessors	High	Low	High
Nuclear technology	High	High	Low

For all three case studies, the United States was selected as the national context of interest. This is motivated by the fact that across much of the 20th century the U.S. was the leading nation across a range of critical technology industries which have, by and large, had enough time to reach technological maturity. They thus offer enough empirical evidence for this research to draw upon.

1.2.2.3 Case study methodology

The historical case studies – aerospace technology, biotechnology and cryptography – and the contemporary case study of artificial intelligence are each assessed qualitatively. The assessment focuses on analysing the following components (further detail on each of these components is provided in chapter 2).

- *The actors:* how are the state, firms, and researchers engaged in the development and deployment of the strategic GPT?
    - What are their goals in relation to pursuit of the technology?
    - What resources do they have available to them to pursue their goals?
    - What constraints do they face in pursuing their goals?
- T*he actor relationships:* between pairs of actors (i.e. between the state and firms, the state and researchers, and firms and researchers) how does the relationship evolve between them as the technology matures?
    - What synergies emerge between the actors? How does this manifest?
    - What conflicts emerge between the actors? How does this manifest?
- *The technology:* what are the relevant properties of the technology and how are they changing with time?
    - How does the economic value, security relevance, and general purpose nature of the technology manifest? How does the salience of these properties change with time?
    - How is the technology evolving as it matures? (e.g. increasing/decreasing costs, novel applications, convergence with other technological trends)
    - How does the evolving nature of the technology affect the goals, resources and constraints of the actors?

    - How does the evolving nature of the technology affect the synergies and conflicts that emerge between the actors?
- *The strategic environment:* how is the environment in which the actors are operating changing?
    - What exogenous events/trends directly related to the technology occur throughout the development and deployment life cycle? (e.g. technological accidents, malicious use attacks)
    - What exogenous events/trends not directly related to the technology occur throughout the development and deployment life cycle? (e.g. shifts in the international security environment, macro-economic trends)
    - How do these events/trends affect the goals, resources and constraints of the actors?
    - How do these events/trends affect the synergies and conflicts that emerge between the actors?

A range of sources are drawn upon in conducting these case studies, namely:

- *Primary sources* e.g. pieces of legislation and regulation; presidential, executive and national security decision directives; text of speeches; statements and annual reports from firms;
- *Secondary sources* e.g. reports produced by the likes of the National Academy of Sciences and the National Academies Press; academic articles and reports by researchers at independent research institutions; analyses and commentary from independent authors and journalists.

1.2.3 Contribution to literature

This research enriches existing literature on private firms as political actors (section 1.1.1), on the evolution of the role of the U.S. government in strategic technology pursuit (section 1.1.2), and on the political influence of researchers and research communities (section 1.1.3). It does so by emphasizing an actor-centric approach in the model and focusing on strategic GPTs as a reference class of case studies.

Several international relations and global governance scholars have called for an actor-centric approach[131]. This responds to the tradition of focusing on macro-level drivers such as globalization, disembodied forces such as markets, and abstract concepts such as international stability. By focusing on the role of actors and their relationships with one another, the hypothesis is that the analysis will gain from a more nuanced understanding of how actors and actor relationships drive the observed outcomes – in this case, the way a strategic GPT is developed and deployed. As Mikler posits: 'studying the reality of powerful corporations interacting with powerful states means rejecting the notion that market-focused firms are in one corner of the ring while national interest-focused governments are in the other'[132]. Rather than an oversimplified battle between sides – national security versus economic growth, public versus private control – an actor-centric approach positions us to understand where states, firms and researchers find points of converging interests, and where diverging interests result in observable conflicts.

[131] The case for an actor-centric approach to governance has been made by the likes of: Avant, D. D., Finnemore, M., & Sell, S. K. (2010). *Who governs the globe?* New York: Cambridge University Press.; Barnett, M., & Duvall, R. (2005). Power in International Politics. *International Organization,* 59(1), 39–75. https://doi.org/DOI:10.1017/S0020818305050010; Mikler, J. (2018). The political power of global corporations. Cambridge, UK: Polity Press.

[132] Mikler, J. (2011). The Illusion of the "Power of Markets." *The Journal of Australian Political Economy*, (68), 41–61.

More broadly, the actor-centric model is underpinned by a strategic choice approach[133]. The strategic choice approach analyses actors according to actor-specific properties – namely, their preferences, and the beliefs that they hold about the preferences of others – as well as the strategic environment in which they are acting – specifically, the actions available to these actors, and the information available to them and other actors. This then informs the study of strategic interactions between actors, enabling one to derive insights into how the character of actors and actor relationships translates into observed outcomes.

Further, by contextualising this research specifically to cases of strategic GPTs as developed and deployed in the U.S., this enhances the model's applicability to the case of AI as it is unfolding today. For one, focusing on the specific national context of the U.S. provides a layer of useful granularity to how we understand the relationship between the U.S. government, firms, and research community. The evolution of dependencies between American defense agencies and technology firms (section 1.1.2) is an example of an element of the domestic political economy that uniquely informs this research. Additionally, by focusing on a reference class of case studies underpinned by technologies with similar characteristics to AI, this strengthens the explanatory power of the model. In a similar vein, several scholars have called for a more fine-grained taxonomy of different types of global governance problems in order to inform our analysis of governance responses most suitable to that type of problem[134]. We do so in this research by grounding the analysis in the specific context of the development and deployment of a strategic GPT in the United States.

---

[133] Lake, D. A., & Powell, R. (1999). *Strategic choice and international relations*. Princeton, N.J.: Princeton University Press.

[134] For example, Cutler et al. propose three attributes which affects the suitability of different constellations of public and private actor governance (Cutler, Haufler, & Porter, 1999b), and Drezner proposes a taxonomy of cooperative arrangements which respond to the demands for formality and participation from various actors (Drezner, 2004b).

2 Modelling the politics of strategic general purpose technologies

Technologies are tools of politics. The development and deployment of a technology can thus be analysed as a set of strategic interactions between actors. Each actor pursues the technology for their own ends, and each is differentially positioned to influence the manner in which the technology emerges and matures.

A strategic GPT is a specific type of technology with distinctive characteristics that lend to a particular pattern of politics between three actors – the state, firms, and researchers. When a strategic GPT is at stake, the strategies that these actors pursue to achieve their desired ends lead to relationships between them that can be both synergistic and conflictual.

This model describes this pattern of politics, illustrating how these synergies and conflicts emerge. It follows a life cycle of the development and deployment of a strategic GPT, moving through three phases – *Phase 1: emergence and promise, Phase 2: commercialization and proliferation,* and *Phase 3: consolidation and contestation.* Each phase (and the transitions between them) is defined by the state of the technology – for example, the extent to which fundamental research has been transformed into commercial products and applications; the accessibility of production capacity and knowledge; and the observed consequences of the technology being developed and deployed in society.

As we move through these phases, the model focuses on three actors – the state, firms, and researchers. Each actor is defined by their goals, resources, and constraints in relation to their role in shaping the development and deployment of a strategic GPT. Thus, each actor evolves with the technology life cycle. The model then extends the analysis to the relationships between these actors – specifically, the synergies and conflicts that emerge between them as their goals, resources, and constraints interact.

Section 2.1 characterises the actors. Then, section 2.2 charts the phases of the technology life cycle which form the strategic environment in which the actors interact. Finally, section 2.3 lays out how the relationships between the actors evolves across the technology life cycle.

A brief note on the basis for this model: the process through which it was developed drew on a combination of building upon existing literature on the nature of the actors and actor relationships (as discussed in Chapter 1) and general intuition. The historical case studies then provided empirical evidence that corroborated the model, and to a certain extent prompted further iterations and refinements. In this chapter, the model will be described in the abstract to provide a bird's eye view of how all of these components piece together; in subsequent chapters, the model will be grounded in the details of specific actors and relationships in history.

2.1 Defining the actors

States, firms, and researchers each have a unique stake and interest in how a strategic GPT is developed and deployed. Their unique nature can be captured by characterising each actor according to their *goals, resources* and *constraints*. An actor's *goals* describe their primary motivations for engaging with the technology – what are they seeking to gain, and what do they fear losing, as the technology matures and proliferates? In turn, an actor's *resources* describe what absolute advantage they have over the other actors – what resources, tangible and intangible, do they have access to and control over which can be used to shape the technology life cycle? Finally, each actor faces a set of *constraints* – what factors bound the scope of their behaviour, and how does the need to be sensitive to these factors constrain their ability to influence the technology life cycle? The following sections step through actor-specific goals (section 2.1.1), and their respective resources and constraints (section 2.1.2).

2.1.1 Actor goals

The *state* refers to the national government of a country. The core goals for the state are threefold. Firstly, the state wants to reap economic gains from the technology to boost national economic productivity and growth. They thus support the build-up of national technological capabilities such that they can capture the rents of domestic firms being at the frontier of a globally lucrative market.

Secondly, the state seeks to strengthen the nation's defense and security capabilities by capitalising on the military value of the technology. This manifests both as pursuing strategies to integrate commercial technologies into the military technology base, as well as increasing their capacity to develop such technologies in-house.

Thirdly, the state seeks to mitigate the security risks posed by the technology. An important part of the national security agenda is ensuring that these technologies are not used

maliciously against the state. More generally, mitigating the risk of unintended harm – particularly from accidents and structural risks – can be considered a public good which the state is expected to provide to its citizens.

Firms are private companies involved in developing and deploying the technology. The core goal for firms is to maximise profit. With respect to strategic GPTs, firms are thus most invested in maximising the economic value that they can reap from its development and deployment. Secondarily, firms are also interested in the military value of the technology insofar as this constitutes a market opportunity.

In the age of multinational corporations, the pursuit of profit maximization has often been reframed in terms of the intermediary goal of seeking to control increasingly large parts of the global market, particularly in sectors that are dominated by a handful of actors who benefit from sectoral consolidation and thus have been freed from the 'restraints of classical competition'[1]. This includes 'actively seeking to structure its environment to serve its needs' of autonomy, discretion and control[2] as demonstrated by their engagement in shaping the scope of international legal regimes in prominent areas such as trade and commerce, often

[1] Chandler, A. D. (1977). *The visible hand: the managerial revolution in American business*. Cambridge, Mass.: Belknap Press.; Harrod, J. (2006). The Century of the Corporation. In C. May (Ed.), *Global corporate power*. Boulder, Colorado: Lynne Rienner Publishers. Retrieved from http://www.loc.gov/catdir/toc/ecip061/2005029752.html

[2] Dallas, L. L. (1988). Two models of corporate governance: Beyond Berle and Means. *U. Mich. JL Reform*, *22*, 19.; May, C. (2015). Who's in charge? Corporations as institutions of global governance. *Palgrave Communications*, *1*, 15042.; Harrod, J. (2006). The Century of the Corporation. In C. May (Ed.), *Global corporate power*. Boulder, Colorado: Lynne Rienner Publishers. Retrieved from http://www.loc.gov/catdir/toc/ecip061/2005029752.html

at the invitation of states[3]. Thus, while firms are fundamentally economically motivated, they are more aptly characterized as political actors with economic motivations[4].

Researchers refer to individuals conducting research in this technology domain in academic and not-for-profit institutions. These researchers make up a research community which can be characterised as a combination of an epistemic community and a professional network (Chapter 1). Their core goal is to pursue research, both fundamental and applied. The ultimate drivers of this vary across research cultures but are a blend of the pursuit of academic prestige, personal profit (via research commercialisation), and the desire to discover truths and generate knowledge for humanity. Researchers are often bound together by a common set of fundamental principles and expectations, such as the capacity to pursue research in a truth-seeking and open manner[5].

[3] Illustrative examples include:

- James Enyart, former Director of International Affairs for Monsanto, stating: 'the rules of international commerce are far too important to leave up to government bureaucrats': Sell, S. K. (2003). *Private power, public law: the globalization of intellectual property rights*. Cambridge: Cambridge University Press. Retrieved from http://www.loc.gov/catdir/toc/cam031/2002035020.html
- The former Director General of the World Trade Organization, Pascal Lamy, calling for corporate leaders to assist in maintaining and crafting future rules for international trade and investment: WTO. (2011). As trade changes rapidly, you must help guide WTO, Lamy tells global business. *WTO News: Speeches - DG Pascal Lamy*. Retrieved from https://www.wto.org/english/news_e/sppl_e/sppl192_e.htm

[4] This framing of a firm is usefully articulated by Fuchs through the lens of 'business power'. The claim is that corporations can effectively exert political power in the name of their business interests in three different ways:

- *Instrumental power:* e.g. lobbying, corporate outreach, other direct forms of influence;
- *Structuralist power:* e.g. through private rule and standard setting, other forms of shaping institutions explicitly;
- *Discursive power:* e.g. through advertising and public relations, other forms of building ideational legitimacy and authority.

See: Fuchs, D. (2013). Theorizing the Power of Global Companies. In J. Mikler (Ed.), *The Handbook of Global Companies*. Chichester: John Wiley & Sons Inc.

[5] On the principles of openness – in recent years, and particularly in light of emerging catastrophic risks from some types of scientific research, scientists have become more cognizant of their professional reputation and standing among their peers, aware that their scientific freedom is evermore contingent on acting in a responsible, socially acceptable manner. See: Marchant, G. E., & Pope, L. L. (2009). The Problems with Forbidding Science. *Science and Engineering Ethics*, *15*(3), 375–394. https://doi.org/10.1007/s11948-009-9130-9

2.1.2 Actor resources and constraints

This model identifies four common resources and constraints that are relevant to these three actors: research and development (R&D) funding; innovation capacity; the legislative environment; and public concern.

R&D funding refers to the capital invested in carrying out both fundamental and applied research as well as translating this research into products and applications. Both the state and firms possess R&D funding as a resource – the former via federal funding for R&D, and the latter via private investment and within-firm R&D expenditure. Researchers, conversely, are constrained by R&D funding insofar as this funding comes with strings attached. If they rely on state funds, for example, this can often be constrained by laws that apply to federal grants, or expectations for what federal funding can be used for. Private funds, on the other hand, tend to constrain the extent to which basic research can be conducted and whether research results can be published openly.

Innovation capacity is the ability of an actor to push the frontier of technology development and deployment. Firms and researchers both have innovation capacity as a core resource. For researchers, their innovation capacity is particularly valuable in the early stages of R&D where their deep expertise is well-placed to generate novel insights and breakthroughs. For firms, their innovation capacity stems from their relative advantage in translating fundamental research insights into innovative technology products that serve user demands[6]. The state may also develop innovation capacity within government labs or agencies. For example, the Defense Advanced Research Projects Agency (DARPA) was set-up for the primary purpose of establishing innovation capacity within the government apparatus for the

[6] There are distinct exceptions to this, where firms have established substantial in-house research capabilities in fundamental research. Notable examples in history include Bell Labs, IBM's Watson's Lab, and AT&T. Modern examples include the likes of Microsoft Research and Google's fundamental science units.

incubation and production of cutting-edge emerging technologies. However, increasingly so, the innovation capacity of the government apparatus is falling behind relative to firms and researchers [7].

The *legislative environment* describes the operating conditions for the technology life cycle – namely, what hard and soft rules are in place that bound the ways in which the technology can be developed and deployed. The ability to shape this legislative environment is one of the state's core resources; indeed, the state is the only actor with the authority to implement or change national legislation and regulations to which other actors can be constrained by rule of law. Conversely, firms and researchers are constrained by the legislative environment as it affects the costs and benefits of their R&D activities and constrains what they are capable of doing, at least within the given national jurisdiction.

Public concern shapes the social and political environment in which these actors operate. Specifically, how strong the public concern is, and what the concerns are targeted at, constrains what is deemed acceptable behaviour by the actors. For the state, this constraint often takes the form of an expectation for the government to be responsive to the sentiments of the public and to act in line with the expressed interests of their citizens. For firms, public concern matters insofar as the public constitutes their employees as well as their consumers; thus, the firm's profitability and sustainability can be affected by the perception of the firm among the public. Researchers can often channel public concern as a resource, given their loose representation of the public's interests in pursuing knowledge and research in the name of the common good.

[7] Weinburger, S. (2017). *The Imagineers of War, The Untold Story of DARPA, the Pentagon Agency that Changed the World*, Alfred A. New York: Knopf.

Table 2.1-1: Summary of actor goals, resources and constraints

		State	*Firms*	*Researchers*
Goals		Economic growth Military leadership Risk mitigation	Maximise profit	Pursue research
Resources and constraints	*R&D funding*	Resource	Resource	Constraint
	Innovation capacity	Resource	Resource	Resource
	Legislative environment	Resource	Constraint	Constraint
	Public concern	Constraint	Constraint	Resource

2.2 The technology life cycle

This model traces the life cycle of a strategic GPT. The general progression is from fundamental scientific breakthroughs through to concrete applications and products in the market, and eventually to the growth of complementary innovations. The life cycle can be broken down into three distinct phases. Each phase is characterised both by the maturity of the technology as well as the activities of the actors with respect to the technology. The transitions from one phase to the next are marked by indicators of the technology reaching a new level of maturity, or events that cause exogenous shifts in the strategic environment.

2.2.1 Phase 1: Emergence and promise

Phase 1 – *emergence and promise* – is the period during which the research foundations are laid that underpin the strategic GPT. The point at which phase 1 begins is often difficult to define – the fundamental breakthroughs that propel the technology forward are often spread across various disciplines and some of these breakthroughs may have occurred decades earlier. It is also rarely one standalone discovery that is sufficient to ignite interest in a new strategic GPT; typically, it is a convergence of a series of discoveries, closely following each other or occurring in parallel.

In culmination, the effect of these fundamental breakthroughs is to highlight a new, unexplored area of research that has suddenly become tractable and could lead to vast opportunities for innovation. At this stage, it is unclear what the potential of this emerging technology is, but the scale of its transformative potential is sufficiently compelling to attract research funding and talent into the space. Early stage R&D efforts are largely funded by the government and carried out by academic institutions and government labs; the uncertainty around the technology is still too high for the likes of private sector investors.

2.2.2 Phase 2: Commercialisation and proliferation

The transition from phase 1 into phase 2 – *commercialisation and proliferation* – is marked by events signalling that the economic value of the technology has become evident enough to attract commercial interests. Such signals include the establishment of the first private firms, an increase in the number of patents being filed by researchers, and the growth of private capital being invested in R&D.

Phase 2 begins with the emergence of tangible commercial applications of the early stage research in the form of technology products and services. New markets are created; old industries are rejuvenated. Start-ups rapidly emerge to seize these opportunities. They grow into small-to-medium enterprises or are acquired by larger firms moving into this space in response to the growing market opportunity. The number of customers and users of the technology grows; early funders of the technology begin to see returns on their investments.

With the growth of the number of organisations engaged across the R&D pipeline, many become more specialised. Barriers to entry for these new actors decrease due to falling costs of technology production, the creation of supporting infrastructure, and the proliferation of common technology standards. The market for the technology becomes increasingly global, demanding the building up of global supply chains, distribution channels, and joint ventures between firms.

The research community also grows and becomes more transnational. This can take the form of increasing numbers of international research collaborations and partnerships, as well as more convenings via conferences and online communities to exchange knowledge and synchronise on best practice. It is during this phase that researchers transition from identifying as members of their academic or government institutions to being members of a transnational research community with common norms and beliefs.

As the economic value of the technology becomes more evident, so does its military value. During phase 2 there is an increase in attempts to integrate the emerging technology into the military technology base, often triggered by demonstrations of the technology being used successfully in combat. This spurs the state's interest in pursuing the technology with an eye towards strengthening their defense and security capabilities. This also drives more states to invest in the technology. By the end of phase 2 a number of moderate and emerging states have also developed their own technology capabilities, joining the original superpowers in a global competition for technology leadership. This means that the nation at the forefront of technological development – namely the U.S. – sees a decline in their technological prowess, losing ground in relative terms to other states and firms vying for global market share.

Phase 2 is also marked by an emerging fear of malicious use of the technology. Risks from technology proliferation becomes more of a focal point in the realm of national security and defense. In the public discourse, concerns about the negative repercussions of the technology being deployed enter more into mainstream discussions. Civil society groups and media organisations become more engaged on matters relating to technology risks.

2.2.3 Phase 3: Consolidation and contestation

Phase 3 is marked by two parallel and significant trends – *consolidation and contestation.*

Consolidation refers to the streamlining of firm activity to a few dominant firms which act as nodes of commercial activity. They own stable and substantial portions of the market share and tend to agglomerate proprietary technology, talent and core infrastructure. The transition to market consolidation is indicated by a decrease in the number of new firms being established and an increase in merger and acquisition activity. The core industries that marked the first wave of innovation reach market saturation and start to see decreasing returns. Entrepreneurial activity thus shifts towards building applications layers on top of the

core infrastructure. This may yield novel breakthroughs in new, composite ways of linking applications and products together across different domains which could trigger a second wave of innovation.

Contestation refers to the escalation of tensions between the firms and the state, and to a lesser extent the research community. This intensifies across phase 2; the transition from phase 2 to 3 is typically (although not necessarily) marked by sudden event such as a high profile case of technology failure or misuse. This event triggers a spike in public fear of the technology, and consequently creates the momentum for significant regulatory activity by the state[8]. The subsequent effects are mostly context-specific but broadly can be described as an increase in friction between actors.

[8] This type of event can be described as having 'demonstration effects', creating the momentum for regulatory activity. See: Mattli, W., & Woods, N. (2009). *The politics of global regulation*. Princeton University Press.

2.3 Actor relationships

These phases of technology development and deployment describe the environment in which the actors are operating. In this environment, actors pursue strategies to achieve their goals. The strategies available to them are shaped by their environment, which is changing as the technology emerges and matures[9]. Here, we first describe how changes in the environment influence the individual actors (section 2.3.1). It is assumed that while the goals of the actors remain constant, their willingness to leverage their resources and their susceptibility to their constraints are influenced by changes in the environment. Then, based on these changes at an individual actor level, we describe how the relationships between the actors change (section 2.3.2). Summaries are provided in Tables 2.3-1, 2.3-2 and 2.3-3.

2.3.1 The evolution of the actors

Across all of the phases, the goals for each of the actors remain constant. That is, the state seeks to reap the economic and military value of the technology, as well as address risks posed by the technology. Firms seek to maximise profit from the development and deployment of the technology. Researchers seek to pursue fundamental and applied research.

As the technology progresses through its life cycle, the resources and constraints that apply to these actors evolve. The provision of *R&D funding* shifts away from the state and towards firms. This is in large part explained by the difference in the risk profiles of public versus private R&D funding sources. State R&D funds are typically more risk tolerant compared to

[9] The model is premised on the strategic choice approach in international relations which attempts to explain the choices or decisions of actors based on the interactions of four independent variables:

- Actors' beliefs
- Actors' preferences
- The strategies and actions available to actors
- The information available to actors

The strategic choice approach assumes an ability to separate actors form their environments. See: Lake, D. A., & Powell, R. (1999). *Strategic choice and international relations*. Princeton, N.J.: Princeton University Press.

private R&D funds[10]; as such, the state is often the primary funder of early-stage R&D when the technology is in such formative stages that the likelihood of the research translating into commercially viable products is highly uncertain. As soon as there is greater certainty about the economic value of research, private R&D funding follows. For researchers the constraint of R&D funding remains constant but as the source shifts from public to private institutions different constraints are introduced.

Innovation capacity as a resource becomes increasingly concentrated with firms as the technology matures and proliferates. Particularly as private sources of funding become more readily available to fund research, firms scale and accrue core assets such as infrastructure and proprietary technology which enables them to strengthen their innovation capacity. Comparably, the innovation capacity of researchers decreases in relevance as the focus shifts from research to product and application development, which is much more the forte of firms than researchers. The state's innovation capacity also wanes as the technology matures, given their slow-moving nature and limited capital resources compared to firms.

The capacity to shape the *legislative environment* becomes a more relevant resource for the state as it becomes possible to implement specific legislation that targets specific products or institutions as the technology sector matures. Consequently, the legislative environment becomes more constraining for firms and researchers. Finally, the role of *public concern* becomes a more important constraint on firms and the state as the technology matures and as the public becomes more engaged in the consequences and impacts of these technologies.

[10] (Mazzucato, 2011)

Table 2.3-1: Evolution of actor goals, resources and constraints as technology matures, by actor

		State	*Firms*	*Researchers*
Goals		Economic growth = Military leadership = Risk mitigation =	Maximise profit =	Pursue research =
Resources and constraints	*R&D funding*	Resource ↓	Resource ↑	Constraint =
	Innovation capacity	Resource ↓	Resource ↑	Resource ↓
	Legislative environment	Resource ↑	Constraint ↑	Constraint ↑
	Public concern	Constraint ↑	Constraint ↑	Resource =

Notes:
↑ means that the goal / resource / constraint becomes more advantageous / constraining as the technology matures
↓ means that the goal / resource/constraint becomes less advantageous / constraining as the technology matures
= means that the goal / resource / constraint remains constant as the technology matures

Table 2.3-2: Evolution of actor goals, resources and constraints as technology matures, by phase

		Phase 1 → Phase 2 → Phase 3
Goals		Goals remain constant for all actors
Resources and constraints	*R&D funding*	Resource shifts from State to Firms Constraint remains constant for Researchers
	Innovation capacity	Resource shifts from Researchers and State to Firms
	Legislative environment	Resource increases for the State Constraint increase for Firms and Researchers
	Public concern	Resource remains constant for Researchers Constraint increases for Firms and the State

2.3.2 The evolution of actor relationships

The relationship between two actors arises from the combined effects of each actor's goals, resources and constraints. As these change across the phases, so does the nature of the relationships between these actors.

Each relationship can be described in terms of two types of dynamics:

- A *synergy* arises when the goals of both actors are aligned, and their resources and/or constraints are complementary (e.g. one actor's resources eases the other actor's constraints);

- A *conflict* arises when the goals of both actors are misaligned and at least one actor possesses the resources to hinder the other actor from pursuing their goal.

Across the development and deployment of a strategic GPT, synergies and conflicts arise between the state and firms (section 2.3.2.1), the state and researchers (section 2.3.2.2) and researchers and firms (section 2.3.2.3). The synergies and conflicts are described in terms of whether they become stronger or weaker across the technology life cycle.

2.2.3.1 State <> Firms

The state and firms develop a *synergy* based on the state's need to access the cutting edge commercial technologies produced by firms.

- Their *goals* align. Firms want to pursue technology development in order to profit. This aligns with the state's goals of pursuing economic and military leadership, which require access to cutting edge technologies. Because of the dual-use nature of the technology, technologies developed by firms are applicable for civilian applications as well as military applications.
- Their *resources and constraints* are complementary insofar as the state's lack of innovation capacity is offset by the firm's strong innovation capacity.
- This synergy *strengthens* as the technology matures. Firms become more competent at producing leading commercial technologies, and states face increasing pressure from global competition to address their lack of in-house innovation capacity.

A *conflict* that can emerge as this synergy increases, however, is when the state seeks to use firm-developed technologies for military applications. Firms may fear public backlash by allowing their products to be used for such applications.

- Their *goals* are misaligned insofar as the *constraint* of public concern means that by firms selling their products and services to government agencies for military applications, they would be jeopardising their ability to make profit.
- This conflict only *strengthens* in a case where firms are increasingly subject to public scrutiny. In cases where firms do not face this constraint, this conflict does not emerge.

A further *conflict* occurs when the state perceives the proliferation of the technology as a risk. This can be based on national security concerns – namely, when the state becomes concerned that proliferation of the technology to other states or non-state actors could enable adversarial uses of these technologies against the state[11]. This could also be based on the concern that proliferation of the technology could increase the likelihood of accidents.

- Their *goals* are misaligned in that firms are interested in reaping the economic gains of global proliferation and expansion of their market share, whereas states are primarily interested in mitigating risks by putting limits on technology proliferation particularly beyond national borders.
- This conflict *strengthens* as the technology matures. As the willingness of the state to shape the legislative environment increases, firms face stronger constraints on their growth.

2.2.3.2 State <> Researchers

The state and researchers find *synergy* in the funding relationship that develops between researchers and the state in the early stages of R&D.

[11] Export controls have been the most obvious manifestation of this conflict between American firms and the state. For years, the Department of Defense held that the strongest possible barriers should be erected against the eastward leakage of U.S. technologies and proved willing to sacrifice the commercial interests of U.S. allies as well as U.S. export industries in order to enable this. See: Alic, J. A. (1994). The dual use of technology: Concepts and policies. *Technology in Society*, *16*(2), 155–172. https://doi.org/10.1016/0160-791X(94)90027-2

- Their *goals* are aligned in that the state seeks to reap the economic and military value of the technology and investing in early stage R&D directly contributes to this.
- Their *resources and constraints* are complementary. The state is in a position to deploy funds for early stage fundamental research yet do not have the in-house capacity to carry out this research on their own. Conversely, researchers are best placed to carry out this innovative work but are ultimately dependent on an external funding source.
- This synergy *weakens* as the technology matures and as the state's R&D funds become fungible for private R&D funds.

The state and researchers face a *conflict* as the technology matures and as the state increasingly perceives the proliferation of research knowledge and talent as a national security risk[12].

- Their *goals* are misaligned in that researchers are interested in pursuing research unhindered, whereas the state is interested in mitigating risks by putting limits on the proliferation of knowledge and research talent.
- This conflict *strengthens* as the technology matures and as the state's willingness to shape the legislative environment becomes more of a constraint on researchers.

2.2.3.3 Firms <> Researchers

Firms and researchers find *synergy* particularly as of phase 2 when firms become the primary source of R&D funding, and researchers are increasingly integrated into the commercialisation pipeline of the industry.

- Their *goals* are aligned in that firms see investing in early stage R&D as directly contributing to downstream profits from commercialising this research.

[12] Note that this assumes research laboratories are civilian. National laboratories are, by design and culture, more inclined to not face this conflict with the state. See: Hecker, S. (1994). Retargeting the weapons laboratories. *Issues in Science and Technology*, 10(3), 44.

- Their *resources and constraints* are complementary in that researchers remain dependent on an external source of funding, and firms are able to provide this funding.
- This synergy *strengthens* as the technology matures.

A *conflict* that can emerge between researchers and firms arises when researchers clash with firms on considerations of the ethical and societal consequences of these technologies.

- Their *goals* are misaligned insofar as firms are able to make a profit by engaging in activities that researchers may object to.
- This conflict *strengthens* as the technology matures, and as public concern channelled via researchers becomes more of a constraint on firm activities.

Table 2.3-3: Evolution of actor relationships as technology matures

	Synergies	*Conflicts*
State <> *Firms*	State depends on access to commercial technologies ↑	State prevents firms from proliferating technologies ↑ Firms face public backlash for selling technologies to the state ↑
State <> *Researchers*	State creates supportive R&D environment ↓	State prevents researchers from proliferating knowledge and talent ↑
Firms <> *Researchers*	Firms create supportive R&D environment ↑	Researchers clash with firms on issues of ethics and societal consequences ↑

Notes:
↑ means that the synergy / conflict becomes stronger as the technology matures
↓ means that the synergy / conflict becomes weaker as the technology matures

3 Aerospace technology

Today, it is difficult to imagine what life would be like without space technologies. Much of modern civilian life depends on the use of outer space; one estimate suggests that a single day without access to space would stifle approximately $1.5 trillion worth of financial market transactions and disrupt over 100,000 commercial flights. Modern militaries have also become dependent on space-based assets to serve a number of critical functions, including communications, reconnaissance, surveillance, and high-precision-targeting[1].

Satellite technology in particular has fundamentally transformed the nature of civilian life and economic activity; one could claim that many of the benefits of globalization and information technology have either directly or indirectly relied on the proliferation of satellites. For one, the global telecommunications system as we know it today is made up of a configuration of satellites that connects us to services that we use every day[2]. The Global Satellite Navigation Systems (GNSS) provides autonomous geo-positioning with global coverage; the system most widely in use today is the Global Positioning System (GPS)[3]. Further, the use of satellites for weather monitoring and reporting has become central to the science of meteorology[4].

Using space and space-based technologies has become a cornerstone to maintaining U.S. military strategic advantage since the dawn of the Space Age. Space provides a wide range of capabilities to the military, ranging from the passive – intelligence, surveillance, and reconnaissance (ISR), for example – to the active – such as communications for command

[1] Al-Rodhan, N. (2018c). Preventing Future Conflicts in Outer Space. Retrieved from https://isnblog.ethz.ch/security/preventing-future-conflicts-in-outer-space; Watts, B. (2013). *The Evolution of Precision Strike*. Washington, D.C.: Center for Strategic and Budgetary Assessments. Retrieved from https://csbaonline.org/research/publications/the-evolution-of-precision-strike
[2] Livingston, D. (2001). *Outer space commerce: Its history and prospects*. Golden Gate University.
[3] Bonnor, N. (2012). A Brief History of Global Navigation Satellite Systems. *Journal of Navigation*, *65*(1), 1–14. https://doi.org/10.1017/S0373463311000506
[4] Williamson, M. (1996). Space: Towards the Next Millennium. *The Aeronautical Journal 100*, *1000*, 426–443.

and control, and the use of precision-guided munitions and smart bombs[5]. Space weapons – encompassing both weapons placed in space and those on Earth capable of targeting space assets[6] – have been proven to be both technically feasible and of interest to a number of states[7]. In particular, the development of kinetic-physical weapons such as ASATs – often referred to as 'hit-to-kill' systems – have been the target of major investments by states pursuing space weaponization[8]. There is an inherent difficulty in differentiating aerospace technologies that pose economic and security opportunities from those that risk causing substantial harm. Indeed, approximately 95% of space technologies are considered dual-use technologies[9] and the four official space missions that the U.S. pursue blur the lines between what are considered legitimate versus escalatory pursuits of space capabilities[10]. Therein lies the challenge of governing aerospace technology as a strategic GPT.

Section 3.1 begins by outlining the key actors who have been critical in shaping the trajectory of the aerospace industry. Then, sections 3.2, 3.3 and 3.4 analyse the three phases of the technology's development and deployment. Finally, section 3.5 offers a summative analysis.

---

[5] Peebles, C. (1945). *High Frontier: The United States Air Force and the Military Space Program* (Vol. 1959). Washington, D.C.: Air Force History and Museums Program.
[6] Hebert, K. D. (2014). Regulation of Space Weapons: Ensuring Stability and Continued Use of Outer Space. *Astropolitics*, *12*(1), 1–26. https://doi.org/10.1080/14777622.2014.890487
[7] Al-Rodhan, N. (2018b). Weaponization and Outer Space Security. Retrieved from https://www.globalpolicyjournal.com/blog/12/03/2018/weaponization-and-outer-space-security
[8] Lewis, J. (2014). They Shoot Satellites, Don't They? *Foreign Policy*. Retrieved from https://foreignpolicy.com/2014/08/09/they-shoot-satellites-dont-they/; Lewis, P., & Livingstone, D. (2016). What to Know About Space Security. Retrieved September 25, 2018, from https://www.chathamhouse.org//node/25077
[9] Johnson-Freese, J. (2007). Space as a strategic asset. Columbia University Press.
[10] Joint Chiefs of Staff Department of Defense. (2002). *Joint Doctrine for Space Operations, Joint Publication 3-14*. Washington, D.C.: Department of Defense.

3.1 The actors

Aerospace technology has been primarily shaped by three actors in the U.S. – the state, the firms, and, to a lesser extent, aerospace researchers. In the following sections, each actor is described in the context of their engagement with the development and deployment of aerospace technology.

3.1.1 State

Within the U.S. government, there are dozens of agencies and units with an interest in and responsibility for space technology and space activities. Broadly, they can be divided into the civilian segment, represented by the National Aeronautics and Space Administration (NASA), and the military segment, represented by the Department of Defense (DOD), and more specifically the U.S. Air Force (USAF) who are the primary executive agent in charge of the military space sector, as well as the National Reconnaissance Office (NRO) who are the primary agency associated with intelligence applications in the space sector.

3.1.1.1 NASA

In the midst of the Cold War, on October 1, 1958, the *National Aeronautics and Space Act* created NASA to carry out core civilian space activities – namely, the expansion of human knowledge and the improvement of space technologies in order to serve the goal of preserving U.S. leadership in space science[11]. NASA replaced its predecessor, the National Advisory Committee for Aeronautics (NACA), thus inheriting 8,000 employees, an annual budget of $100 million, and three major research laboratories from its inception. It quickly absorbed other organisations, including the space science group of the Naval Research

[11] McDougall, W. A. (1997). *The heavens and the earth: a political history of the space age*. Baltimore: Johns Hopkins University Press.

Laboratory, the Jet Propulsion Laboratory managed by the California Institute of Technology, and the Army Ballistic Missile Agency[12].

NASA's strategic priorities have consistently been the pursuit and utilisation of knowledge and science to improve the quality of life on Earth. During its first twenty years NASA conducted several major programs, ranging from human spaceflight initiatives such as Project Gemini and Project Apollo, remote-sensing satellites for information gathering, the Space Shuttle for space transportation, and robotic missions to the Moon, Venus, and Mars for scientific research[13]. More recently, NASA has partnered with commercial actors with the goal of making space travel accessible to everyone.

3.1.1.2 DOD

Since the end of the Cold War, the primary goal of the DOD has been to achieve full spectrum dominance of the battlespace through what has been coined a 'military transformation'. This has placed an emphasis on leveraging network-enabled operations and the development of more easily deployable forces with greater precision over longer distances – capabilities which space technologies are well-placed to enable. The explicit goals of U.S. space dominance to achieve these ends were laid out in the 1997 U.S. Space Command Vision for 2020, with the objectives of 'dominating the space dimension of military operations to protect U.S. interests' and 'integrating Space Forces into warfighting capabilities across the full spectrum of conflict'[14].

Whilst these goals have been consistent, the means by which they are pursued have evolved. Specifically, there has been an increasing turn in military doctrine towards the assertion and

[12] NASA. (n.d.-a). A Brief History of NASA. Retrieved October 1, 2018, from https://history.nasa.gov/factsheet.htm
[13] (NASA, n.d.-a)
[14] (Johnson-Freese, 2007)

pursuit of space dominance[15]. Key pieces of rhetoric illustrate the progressive escalation from the passive maintenance of military assets in space to the active weaponization of them[16]. Most notably, the 2001 report of the *Commission to Assess United States National Security, Space Management and Organization* warned of the inevitability of space weaponization – 'We know from history that every medium – air, land, and sea – has seen conflict. Reality indicates that space will be no different' – implying that it would be remiss for the U.S. to not prepare[17]. This school of thought – that, whilst weaponization is not necessarily a desirable end goal unto itself, it is a necessary pre-emption of the inevitable – has underpinned more recent statements from members of the U.S. defense community. General Lance Lord, then-commander of the Air Force Space Command, said in 2006: 'We must prepare to face future threats today. My top priority is to ensure space superiority.'[18] Peter Teets, then-Undersecretary of the Air Force and Director of the NRO, asserts a more aggressive stance in 2004: 'The fact is, we need to reach for that goal [of space dominance]. It is the ultimate high-ground.'[19]

---

[15] (Johnson-Freese, 2007)

[16] There are broadly four schools of thought when it comes to a justification for space weaponization – see Hayes, P. (1996). *Space power interests*. Boulder, Colorado: Westview Press and Lupton, D. E. (1998). *On space warfare: a space power doctrine*. Maxwell AFB: Air University Press. In order of decreasing active weaponization:

- *High ground*: underpinned by the belief that the U.S. is reliant on space, complete space dominance is considered essential as it represents the ultimate high ground;
- *Weaponization is inevitable*: whilst not necessarily desirable as an end unto itself, given the inevitability of space weaponization by other states the U.S. should prepare through developing space weapons of its own;
- *Limited militarization*: whilst the importance of space is asserted, this school of thought preserves the status quo of limited militarization and passive space defense systems mediated through arms control agreements;
- *Space is a sanctuary*: demilitarization of space (largely considered an unrealistic school of thought)

[17] Commission to Assess United States National Security Space Management and Organization. (2001). *Report of the Commission to Assess United States National Security Space Management and Organization: Executive Summary*. Washington, D.C.: Committee on Armed Services of the U.S. House of Representatives. Retrieved from https://fas.org/spp/military/commission/executive_summary.pdf

[18] Lord, L. Hearings on FY 06 Defense Authorization Budget Request for Space Activities, § Senate Armed Services Committee, Strategic Forces Subcommittee (2005).

[19] Teets: America Must Reach for Space Dominance. (2004). *Defense-Aerospace*. Retrieved from http://www.defense-aerospace.com/articles-view/release/3/45448/america-must-dominate-space%3A-dod-%28sept.-16%29.html

Much of this rhetoric can be interpreted as in line with the goal of space control, which as articulated in the *National Defense Strategy* of 2005 'ensure[s] our access to and use of space' and 'den[ies] hostile exploitation of space to adversaries'[20]. This reflects a cold war notion of escalation dominance, whereby the dilemma of deterrence is resolved by building up a fully equipped force structure against which adversaries cannot hope to gain from any form of aggression[21]. In practice, however, it appears that the U.S. are on a slippery slope. Space control originated with a focus on developing ground and space-based sensors to enhance space situational awareness (SSA), driven by the rationale that by disseminating high fidelity SSA data and creating an ability to attribute all activity in space adversaries would be dissuaded from hostile activities. In more recent years, space control has inched closer to resembling offensive counterspace operations, defined by the U.S. Air Force doctrine as missions that would 'disrupt, deny, degrade or destroy space systems or the information they provide'[22]. This has driven investments into space control and force application programmes such as hypersonic vehicles (e.g. the National Aerospace Plane, the X-40 Space Manoeuvre vehicle, and the Dyna-Soar), hypervelocity rod bundles (tungsten rods dropped on targets from space, nicknamed 'Rods from God'), and experimental spacecraft systems (including manoeuvrable microsatellites which could be used to attack satellites)[23].

3.1.2 Firms

The U.S. aerospace industry is distinct in its dependence on the government, both as an initial investor and as a significant source of demand for aerospace technology products.

---

[20] Department of Defense. (2005). *National Defense Strategy of the United States of America*. Washington, D.C.: The White House. Retrieved from http://www.au.af.mil/au/awc/awcgate/nds/nds2005.pdf

[21] (Coletta, 2009)

[22] Air Force Doctrine Center. (2004). *Air Force Doctrine Document 2-2.1, Counterspace Operations*. Washington, D.C.: U.S. Air Force.

[23] Butrica, A. J. (2003). *Single stage to orbit: Politics, space technology, and the quest for reusable rocketry*. JHU Press.; Peoples, C. . The Securitization of Outer Space: Challenges for Arms Control. *Contemporary Security Policy*, 32(1), 76–98. https://doi.org/10.1080/13523260.2011.556846; Thompson, M. O. (2013). *At the edge of space: the X-15 flight program*. Smithsonian Institution.

Absent these two forms of government support, the aerospace industry is unlikely to be commercially viable or self-sustaining[24].

The aerospace industry was, for a long time, dominated by a handful of large aerospace companies such as the Boeing Company, Lockheed Martin Corporation and Northrop Grumman. These firms (and their predecessors prior to mergers) were the primary defense contractors throughout both of the World Wars, demonstrating the ability to retain a technological lead as the aerospace industry expanded from traditional aircraft to include jets, missiles, and space technologies. By 1959, of the sixteen companies that dominated the U.S. missile industry, eight – including the six largest – were traditional aircraft firms[25]. To this day, these large incumbent companies continue to dominate the aerospace industry[26].

The past two decades has seen the emergence of a different breed of aerospace company. These new space actors are distinct in being initially funded almost entirely by private capital, sourced from wealthy individuals and venture capitalists, and founded by high-profile technology entrepreneurs turned billionaires. The most well-known of these firms are Elon Musk's' Space Exploration Technologies Corp., or SpaceX, and Jeff Bezos' Blue Origin LLC. These new firms are also distinct in their stated missions of growing the private space tourism industry, beginning with access to space exploration for citizens and eventually aiming for human settlement in space[27]. The entrance of these firms into the aerospace industry has already posed a challenge to the incumbent aerospace firms in traditional aerospace market segments, as covered in section 3.4.

---

[24] The Boeing Company provides an illustrative case of the reliance of a firm's success on government – specifically military – demand for their products and services. For a detailed recount, see: Kirkendall, R. S. (1994). The Boeing Company and the Military-Metropolitan-Industrial Complex, 1945-1953. *The Pacific Northwest Quarterly*, 85(4), 137–149.

[25] (Weiss & Amir, 2018)

[26] Jammula, A. K. R. (2018). The world's biggest aerospace and defence companies in 2018. Retrieved October 3, 2018, from https://www.army-technology.com/features/worlds-biggest-aerospace-defence-companies-2018/

[27] Davenport, C. (2018). *The space barons: Jeff Bezos, Elon Musk, and the quest to colonize the cosmos* (1st ed.). New York: PublicAffairs.

Over time, aerospace firms have come together to form a variety of industry alliances and professional associations. One of the oldest of these is the Aerospace Industries Association, founded in 1919 to represent leading manufacturers and suppliers in the U.S. of civil, military and commercial space systems and components. The American Institute of Aeronautics and Astronautics, founded in 1963, is a well-established professional society for the field of aerospace engineering, acting as the U.S. representative on the International Astronautical Federation and the International Council of the Aeronautical Sciences. These entities serve a number of functions – namely, providing venues for exchange of technical information, pooling resources in order to vie for larger joint contracts, and advocating for legislation and policies that benefit the industry[28].

3.1.3 Researchers

Aerospace researchers primarily identify as part of the state or firm through which they are employed rather than as an independent academic community with a distinct identity. This reflects important characteristics of the field of aerospace engineering – firstly, that the foundations of the field were driven by state-funded missile and space programs; and secondly, that the incentives for both public and private investment in aerospace research are primarily geared toward national security and profit rather than scientific pursuit.

By way of illustration, the early researchers who laid the foundations of the field were almost exclusively supported by their respective governments and their work was in service to the nation's military and strategic goals. Robert Goddard, the American engineer credited as the father of modern rocketry, relied on military funding for the majority of his pioneering efforts in attempts to reach beyond the Earth's atmosphere with liquid-fuelled rockets[29]. Konstantin

[28] Vedda, J. A. (2010). Non-governmental Space Organizations. In E. Sadeh, *The Politics of Space: a survey*. Routledge.
[29] NASA Goddard Space Flight Center. (2001). Dr. Robert H. Goddard, American Rocketry Pioneer. NASA. Retrieved from https://www.nasa.gov/centers/goddard/about/history/dr_goddard.html

Tsiolkovsky developed the fundamental rocket equation that defined the relationship between rocket speed and mass, and later developed a theory of multi-stage rockets; his work seeded the founding of the Soviet Union's Central Bureau for the Study of the Problem of Rockets in 1924 to 'bring together all persons in the Soviet Union working on the problem' to engage in research on the military applications of rockets[30]. Werner Von Braun, the German rocket scientist who was chief designer of the Saturn V launch vehicle that would take Americans to the Moon, was initially funded by the German government and was later transferred into the custody of the U.S. Army[31].

Throughout the Cold War, cooperation between scientists and science academies was largely viewed through the lens of national security – the national scientific communities were seen as extensions of the state in communicating its intentions and capabilities, and their successes and failures were interpreted as such. The Committee on Space Research (COSPAR), founded in 1958, was a notable exception. COSPAR was founded with the explicit goal of seeking to stay above Cold War geopolitics in building cooperative efforts in space.

Since the end of the Cold War researchers have begun to convene as more of an international community independent of their countries of origin via the likes of the International Astronautical Federation and International Academy of Astronautics. Research communities from other disciplines with an interest in space issues have also established similar entities, such as the International Institute of Space Law and the American and British Interplanetary Societies[32].

[30] (Dawson, 2017; McDougall, 1997)
[31] von Braun, Wernher. (n.d.). Retrieved September 25, 2018, from https://www.nationalaviation.org/our-enshrinees/von-braun-wernher/
[32] (Sadeh, 2010)

3.2 Phase 1: Emergence and promise [1957 - 1991]

Phase 1 – *emergence and promise* – was predominantly defined by the pursuit of military dominance by the two superpowers, the United States and the Union of Soviet Socialist Republics (USSR, used interchangeably with the Soviet Union). Indeed, the Space Age was abruptly ushered in with the launch of the Sputnik 1 satellite by the Soviet Union on October 4, 1957 – a date that has gone down in history as the commencement of the Space Race between the U.S. and the USSR. The Space Race fuelled sudden and significant increases in U.S. and Soviet investments in their respective space programs, accelerating the development of core aerospace technologies.

This period of history was framed by the dynamics of the Cold War, embedding the space industry within a narrative of international rivalry between two superpowers, as described in section 3.2.1.1[33]. Alongside the race for technological superiority there was simultaneously the emergence of satellite communications as the first commercially viable space industry, described in section 3.2.1.2. The emergence of international space law marks the final event of this phase of space history, described in section 3.2.1.3. Section 3.2.2 proceeds to describe how the relationships between the state, firms, and researchers evolved across Phase 1.

3.2.1 Notable events

3.2.1.1 The Space Race

Prior to the launch of Sputnik 1, the U.S. had already been investing in space technologies, specifically missile defense systems and satellite technology. Under the Eisenhower Administration there were two priorities in space policy in the 1950s – to push forward the

[33] This section does not intend to provide a detailed recount of the Space Race, but rather highlights some of the most notable events and dynamics. For examples of excellent historical accounts and analyses of the Space Race see: McDougall, W. A. (1997). *The heavens and the earth: a political history of the space age*. Baltimore: Johns Hopkins University Press.; Moltz, J. C. (2011). *The politics of space security: strategic restraint and the pursuit of national interests* (2nd ed.). Stanford, Calif.: Stanford University Press.

development of American missile technology, and to invest in space technologies such that the U.S. could penetrate the Soviet Union's Iron Curtain[34]. By 1955, the National Security Council had begun to suspect that the Soviet Union would launch a military satellite within the next few years, and therein would threaten the perception of U.S. dominance as a technological leader worldwide. In a *Draft Statement of Policy on U.S. Scientific Satellite Program,* its members made the case for seeking to beat the Soviet Union with an open, American satellite program[35].

The International Geophysical Year (IGY) was launched on July 1, 1957 – the goal of the year was to further scientific knowledge about the Earth's geophysical environment via a worldwide exchange of results from 67 national programs involving some 30,000 scientists. As a high-profile event with a strong focus on civilian scientific pursuit, the IGY came to be the perfect cover for both the U.S. and the USSR to pursue militaristic space activities in the name of science. In October 1954 the Soviet Union announced plans to orbit an IGY satellite; Eisenhower followed with an announcement on July 28, 1957 that the U.S. would do the same. The motivations articulated by both sides was to contribute to the pursuit of human progress, 'turn[ing] even the most daring of mankind's dreams into reality'. However, it was clear that both political leaders recognised the significance of being the first country to put an artificial satellite into orbit. The unspoken priority was beating the other country in missile development; participation in the IGY was a convenient political mechanism to signal dominance, and a cover for investing heavily in military aerospace technologies[36].

On August 21, 1957 the Soviets succeeded at launching the world's first intercontinental ballistic missile (ICBM). On October 4, 1957 the same R-7 rocket was used to launch Sputnik

---

[34] (McDougall, 1997)
[35] NSC 5520, found in: Logsdon, J. M., Lear, L. J., Williamson, R. A., & Day, D. A. (1995). *Exploring the unknown: Selected documents in the history of the US Civil Space Program. Volume 1; Organizing for exploration*. Washington, D.C.: NASA.
[36] Manno, J. (1984). *Arming the heavens: The hidden military agenda for space, 1945-1995*. Dodd Mead.; York, H. F. (1970). *Race to oblivion: A participant's view of the arms race*. Simon and Schuster New York.

1 – the world's first artificial Earth satellite, a landmark event that came simply to be known as 'Sputnik'. The world was shocked, and the U.S. was humiliated. Following Sputnik, public opinion polls in Western Europe showed that by a large margin, the French, Italian, German and British populations had become convinced that the Soviet Union were superior to the U.S. in scientific development and military power[37]. In the U.S., the media and the public were plunged into a crisis of identity. Sputnik challenged the notion that the U.S. was the world's superpower, interpreted as an undermining of the free, democratic system for which the U.S. was the bastion. In the weeks and months that followed, Premier Khrushchev and various spokesmen from the USSR fuelled the panic by framing Sputnik as proof of the inevitability of the Soviet Union's technological leadership and the inherent superiority of communism.

Sputnik marked a distinct shift in the U.S. approach to science and technology towards more overt technocracy across all domains of civilian, commercial and military pursuit. The U.S. embarked on a swift consolidation and expansion of aerospace programmes including those centred on the development of missiles, reconnaissance satellites, and artificial earth satellites[38]. The *Defense Reorganization Act* was promptly passed in 1958, establishing the Advanced Research Projects Agency (ARPA) as well as the position of the Director of Defense Research and Engineering. In Congress, a series of special committees were convened in response to Sputnik, leading to the creation of the House Science and Astronautics Committee and similar Senate committees all targeted at addressing 'the space problem'. The *National Aeronautics and Space Act* was signed on July 29, 1958, creating NASA.

Sputnik II was launched by the USSR on November 3, 1957. This satellite was heavier, and contained geophysical equipment, life support systems, and a live dog named Laika. The first

[37] (Moltz, 2011)
[38] (Sheehan, 2007)

American response to Sputnik was successfully pulled off in January 1958 with the launching of Explorer 1; this was followed by the launching of Vanguard 1, the first solar-powered satellite by the U.S. Navy. In subsequent years, the U.S. and USSR would continue to race to achieve a number of 'firsts' in space. From 1957 through to 1990, the U.S. and USSR were responsible for 93% of the satellites launched into space[39].

The most celebrated of these in U.S. history is the Apollo programme and the mission to land the first man on the moon. When the Soviet Union put the first human in orbit on April 12, 1961 President Kennedy felt he had to respond. On May 25, 1961 he announced to the nation: 'I believe that this nation should commit itself to achieving the goal, before the decade is out, of landing a man on the moon and returning him safely to Earth.'[40] The decision to go to the moon was supported by the defense and security communities. In a joint report by then-NASA Administrator James E. Webb and then-Secretary of Defense Robert S. McNamara, the importance of 'non-military, non-commercial, non-scientific, but civilian' projects were considered critical to turn the tide in 'the battle along the fluid front of the Cold War'. On July 20, 1969 the Apollo 11 crew successfully landed on the moon[41].

The Space Race was, fundamentally, an issue of national security and military dominance. Whilst prestige played a huge role in shaping the political discourse, the gravity of the importance of space policy and investment was firmly grounded in the rationale of strategic conflict[42]. Lieutenant General Ellen Pawlikowski (Air Force Space Command), Douglas Loverro (Defense Intelligence Senior Executive Service) and Colonel Thomas Cristler (U.S.

---

[39] (Harrison, Johnson, & Roberts, 2017)
[40] (Moltz, 2011)
[41] Pawlikowski, E., Loverro, D., & Cristler, T. (2012). Space: Disruptive Challenges, New Opportunities, and New Strategies. *Strategic Studies Quarterly*. Retrieved from https://www.airuniversity.af.mil/Portals/10/SSQ/documents/Volume-06_Issue-1/Pawlikowski.pdf
[42] Gotlieb, A. E., & Dalfen, C. M. (1970). International Relations and Outer Space: The Politics of Co-operation. *International Journal*, *25*(4), 685–703. https://doi.org/10.2307/40200950; Sadeh, E. (2002). *Space politics and policy: an evolutionary perspective* (Vol. 2). Springer Science & Business Media.; Sheehan, M. (2007). *The international politics of space*. Routledge London.

Air Force) reflect that 'most space systems were focused on strategic conflict' and that the large price tags for the programmes 'was regarded in contrast to its larger strategic purpose rather than as an element of discretionary military spending'[43]. Indeed, a closer examination of the U.S. space programmes show that they were aimed at a few primary ends: pre-conflict intelligence (i.e. reconnaissance), nuclear attack warning and response, continuity of nuclear command and control, and missile development. For example, the CIA succeeded in August 1960 in conducting the first U.S. film-return reconnaissance mission over the Soviet Union under the civilian cover of the Discoverer-14 mission; this spurred the creation of the highly classified NRO to coordinate U.S. intelligence gathering in space. The U.S. Air Force invested in an early-warning satellite programme known as the Missile Detection Alarm System (MIDAS) and a reconnaissance satellite programme known as the Satellite and Missile Observation System (SAMOS). Approximately 70% of the satellites launched during the Space Race were military satellites[44].

The Space Race also saw the first counterspace weapons being built and tested. In 1959 the U.S. conducted its first ASAT test with the launch of a Bold Orion missile from a B-47 aircraft. In 1962 the notorious Starfish Prime nuclear test was carried out, detonating a 1.4 megaton nuclear weapon to prove that nuclear weapons could be used to destroy satellites. According to some estimates as many as one third of all satellites in orbit at the time were destroyed. In 1963 the Soviet Union began developing a co-orbital ASAT system capable of destroying satellites in LEO; in parallel, the U.S. pursued a similar system via the likes of the Satellite Inspector (SAINT) program. Under the Reagan Administration in the 1980s, overt aggression in space peaked with the development of the Strategic Defense Initiative (SDI) which came to be known as the 'Star Wars' programme; the capabilities that were to be developed would be a clear rejection of the norm of collective military restraint in outer

[43] (Pawlikowski et al., 2012)
[44] (Harrison et al., 2017)

space. Simultaneously, the Air-Launched Miniature Vehicle (ALMV) programme was also launched; ALMV was a direct ascent ASAT weapon designed to be launched from an airborne platform and was tested once before being disbanded by Congress in December 1985 as part of a broader ban on ASAT tests[45].

3.2.1.2 Establishment of the satellite communications industry

The use of satellites for telecommunications was the first commercially viable space industry to develop and remains a substantial proportion of the space industry to this day. Its emergence and development as an industry is tightly coupled with the dynamics of the Space Race, and more broadly the growth of interest and investment in space technologies for military applications.

The pioneering vision for a global satellite communications system is accredited to Sir Arthur C. Clarke who predicted its emergence in a 1945 proposal for geostationary satellite communications, published in the Wireless World magazine. In parallel, classified DOD research under the remit of Project Rand had begun to explore the potential commercial use of synchronous communications satellites. In the commercial world, John Pierce of Bell Labs also articulated the idea of communications satellites independently in 1954. As the ideas gained traction, several private companies began to translate them into reality. Hughes Aircraft Company invested in demonstrating the feasibility of a design for synchronous satellites between 1959 to 1961, eventually convincing NASA and DOD to fund the remainder of the project. AT&T and Bell Labs similarly invested heavily in research and development on communications satellites, as did several other private companies such as RCA and Lockheed Martin Corporation[46].

---

[45] (Harrison et al., 2017)

[46] Evans, B. G., Thompson, P. T., Corazza, G. E., Vanelli-Coralli, A., & Candreva, E. A. (2011). 1945–2010: 65 Years of Satellite History From Early Visions to Latest Missions. *Proceedings of the IEEE*, *99*(11), 1840–1857. https://doi.org/10.1109/JPROC.2011.2159467

Sputnik created the impetus for an acceleration of investment into developing communications satellite systems. Escalating Cold War concerns stimulated interest from military and national security circles for new forms of secure and reliable long-distance communications. Further, strong participation in the development of a global communications satellite system was seen as a Cold War tool for connecting non-Western or non-aligned countries to the U.S. The post-Sputnik growth in the U.S. space programme also gave private companies – AT&T and Hughes Aircraft specifically – the boost that they needed to pursue commercial development of communications satellites with government backing[47]. By the early 1960s, the Kennedy Administration had set the establishment of an open, global satellite communications system, driven by U.S. companies and featuring all-American technology, as a national priority[48].

On July 26, 1963, the Hughes Aircraft Company launched the first geosynchronous communications satellite, Syncom 2, with the support of NASA. This was closely followed by the launch of Syncom 3 on August 19, 1964 which included expanded capabilities sufficient to carry out the first satellite television broadcast of the 1964 Tokyo Olympic Games[49]. As the technology and industry progressed, Congress mobilised to channel government support for the development of the industry by passing the *Communications Satellite Act* of 1962. This established the Communications Satellite Corporation (COMSAT), a telecommunications company with a mix of private and public control. COMSAT effectively operated as a government mandated monopoly, created with the hope of enabling swift movement in establishing an international satellite communications market that

[47] Slotten, H. R. (2002). Satellite Communications, Globalization, and the Cold War. *Technology and Culture*, *43*(2), 315–350.
[48] Chen, D. D., & MacAuley, M. K. (2010). Commercial Space Actors. In E. Sadeh, *The Politics of Space: a survey*. Routledge.
[49] (Livingston, 2001)

asserted the leadership of U.S. telecommunications companies, and therein U.S. leadership in space technologies[50].

After COMSAT was created, a number of other global and regional communications satellite organisations followed. To enable coordination, the U.S. created the International Telecommunications Satellite Consortium (INTELSAT) in 1964 as a consortium of states to establish, own and operate the space segment of a single global telecommunications system. Each state was to designate a public or private entity to represent them; for the U.S., this was COMSAT. By 1970, over 60 countries belonged to INTELSAT with 28 members operating 50 ground stations and achieving worldwide coverage in serving the Pacific, Atlantic, and Indian Ocean basins[51].

Throughout the 1970s to 1990s, the introduction of broadcast and mobile technology increased demand for telecommunications services from individuals and companies. Across the 1990s an average of twenty communications satellites were being launched annually at an average cost of $100 million each; in 1998, INTELSAT's membership had grown to 143 countries[52]. To this day, the global communications satellite industry has continued to grow as a commercially sustainable segment of the space industry.

3.2.1.3 The emergence of international space law

The sudden expansion of space activities at the emergence of the Space Age spurred prompt and rapid development of a number of multilateral treaties that would become the foundations for international space law. The pace at which a number of international norms and agreements were established with regards to space activities is striking; indeed,

[50] McLucas, J. L. (1991). *Space commerce*. Cambridge MA: Harvard University Press.; Whalen, D. J. (1997). Billion Dollar Technology: A Short Historical Overview of the Origins of Communications Satellite Technology, 1945—1965. In A. J. Butrica, *Beyond the Ionosphere: Fifty Years of Satellite Communication*. Washington, D.C.: NASA History Office.
[51] (Evans et al., 2011; Gotlieb & Dalfen, 1970; Livingston, 2001; Slotten, 2002)
[52] (Evans et al., 2011; Livingston, 2001)

international space law progressed farther than most other fields of international law between the 1960s and 1980s[53].

Within a year of Sputnik, the United Nations (UN) had commenced serious discussions in pursuit of securing the peaceful use of outer space. The first treaty to be adopted was the *Partial Test Ban Treaty* of 1963, in response to the Starfish Prime nuclear test; it called on all parties to prohibit, prevent, and to not carry out any nuclear weapons test explosions, or any other explosions, in areas under its control and including in outer space. Simultaneously, the U.S. and USSR were moving towards a declaratory ban on refraining from placing in orbit or stationing in space 'nuclear weapons or any other kinds of weapons of mass destruction'; this was formally adopted on October 17, 1963 via the UN General Assembly (UNGA) Resolution 1884, laying the basis for the arms control segment of subsequent outer space treaties[54].

Four years later, the first of the five core outer space treaties that make up the fabric of international space law was opened for signature – the *Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, including the Moon and Other Celestial Bodies* ('Outer Space Treaty'). The Outer Space Treaty establishes that the moon and other celestial bodies should be used exclusively for peaceful purposes, prohibiting parties from placing weapons of mass destruction in outer space and establishing military bases or installations for weapons testing or any other kinds of military manoeuvres. The Outer Space Treaty was opened for signature on January 27, 1967; it entered into force on October 10, 1967.

---

[53] Danilenko, G. M. (2016). International law-making for outer space. Tribute to Frances Brown from Jill Stuart, *Space Policy* Current Editor-in-Chief, 37, 179–183. https://doi.org/10.1016/j.spacepol.2016.12.002; Gorove, S., Finch, E. R., Sanders, B., Small, D., & Vogt, D. A. (1982). Arms Control in Outer Space. *Proceedings of the Annual Meeting (American Society of International Law)*, 76, 284–297.; O'Donnell, D. J. (1996). Commercialization by evolution in the jurisdiction of outer space. *Presented at the IAF, International Astronautical Congress*, *47th,* Beijing, China.

[54] Garthoff, R. L. (1980). Banning the Bomb in Outer Space. *International Security*, *5*(3), 25–40. https://doi.org/10.2307/2538418

Following this, the *Agreement on the Rescue of Astronauts, the Return of Astronauts and the Return of Objects Launched into Outer Space* ('Rescue Agreement') was established to set forth the rights and obligations of states to rescue persons in space; it was opened for signature on April 22, 1968 and entered into force on December 3, 1968. The *Convention on International Liability for Damage Caused by Space Objects* ('Liability Convention') shortly followed, expanding on the liability rules created in the Outer Space Treaty; it was opened for signature on March 29, 1972 and entered into force September 1, 1972. The *Convention on Registration of Objects Launched into Outer Space* ('Registration Convention') was then established to create a common registry of space objects; it was opened for signature on November 12, 1974 and entered into force September 15, 1976. Finally, the *Agreement Governing the Activities of States on the Moon and Other Celestial Bodies* ('Moon Treaty') attempted to establish a regime for the use of the Moon and other celestial bodies for the benefit of all states and all peoples of the international community. The Moon Treaty was particularly contentious – despite crossing the threshold for ratification and entering into force on July 11, 1984 it remains a weakly supported agreement. Notably, the U.S., Russia and China – who were considered the space superpowers then and now – are not parties to the treaty.

3.2.2 Relationships

3.2.2.1 Firms <> State

Since the beginning of the space age the U.S. government has been consistently supportive of the commercial space industry. This has been demonstrated through the passing of a number of industry-friendly bills and heavy government investment in kickstarting the commercial satellite industry, as described in section 3.2.1.2.

In part, this was due to the indispensability of firms when it came to research and development (R&D) for aerospace technologies. Rather than the usual exclusive

underwriting of early-stage R&D by the government, private firms were significant investors in the fundamental research that seeded the American space industry. Corporations such as the AT&T, Hughes Aircraft Company and RCA were heavily influential in satellite and electronics R&D; in fact, in 1959 major telecommunications companies invested more in space technology R&D than NASA[55]. Using their own revenue, these firms were uniquely positioned to finance early-stage research in satellite technology, resulting in major breakthroughs that seeded the field[56]. As a result of the R&D fuelled by these firms, all the technologies required for satellite communications had been invented by the time Sputnik I was placed into orbit[57].

The activities of private companies received the support and encouragement of federal government. A Congressional hearing on satellite communications in March 1959 featured representatives from AT&T, Bell Labs and other major private corporations; the proceedings convinced Congress members that private companies were not only able to invest in satellite communications on their own, but they already had a head start on government programmes[58]. President Eisenhower's response to this was to explicitly support leadership from private firms; he released a public statement concerning national policy for satellite communications in December 1960 endorsing an approach of 'aggressively encouraging private enterprises in the establishment and operation of satellite relays for revenue-producing purposes'[59]. The government also intervened to ensure that AT&T would not

---

[55] Glover, D. R. (1997). NASA Experimental Communication Satellites, 1958-1995. In A. J. Butrica, *Beyond the Ionosphere: Fifty Years of Satellite Communication*. Washington, D.C.: NASA History Office.
[56] For example, a high-gain linear amplifier known as the traveling-wave tube was invented by AT&T researchers which came to be used by satellites for transmission; RCA developed a significant amount of the radio and television technology that enabled communications applications in the satellite industry. Hughes invested its own capital in developing a prototype of the Syncom satellite; similarly, AT&T and ITT invested their own money into satellite R&D, and other companies developed complementary ground station technology using their own revenues. See: Whalen, D. J. (1997). Billion Dollar Technology: A Short Historical Overview of the Origins of Communications Satellite Technology, 1945—1965. In A. J. Butrica, *Beyond the Ionosphere: Fifty Years of Satellite Communication*. Washington, D.C.: NASA History Office.
[57] (Livingston, 2001)
[58] (Livingston, 2001)
[59] (Slotten, 2002)

form a satellite monopoly and thus prevent competition and technological advancements in the industry. The result was an anti-trust lawsuit against AT&T in 1979 by the Department of Justice[60].

In 1962 the *Communications Satellites Corporation Act* was passed, establishing a joint public and private commercial communications satellite company to participate with satellite systems of other countries in creating a global communications network[61]. The company was called COMSAT; its structure represented a compromise between public and private control as a for-profit U.S. corporation that was required to submit to presidential supervision, obtain guidance form the State Department, and issue shares to both public and private shareholders. The de facto monopoly that COMSAT was guaranteed enabled it to move swiftly in establishing an international satellite communications market with the full backing of NASA in providing at-cost satellite launches and the full support of the U.S. State Department in negotiating on international treaties and regulatory forums[62]. INTELSAT was then created by two multilateral agreements – *The Agreement Relating to the International Telecommunications Satellite Organization* and *The Operating Agreement Relating to the International Telecommunications Satellite Organization;* both opened for signature in 1971 and entered into force in 1972[63]. INTELSAT was subsequently created in 1964, representing a balancing act of commercial and U.S. foreign policy interests to bring into existence a global telecommunications service.

---

[60] (Livingston, 2001; Slotten, 2002; Whalen, 1997)

[61] The final version of the bill that was passed represented a compromise between three bills that were initially proposed in the first few months of 1962. Two of the three bills represented opposite positions with regards to private ownership of the communications satellite systems – the Kerr bill called for ownership by a group of existing telecommunications companies, whereas the Kefauver bill called for total state ownership. The Administration bill took the middle ground of placing responsibility for the communications satellite system in the hands of a private company, whilst regulation, negotiation with foreign countries, R&D and launch services would be provided by the government. This was the version of the bill that passed.

[62] (Livingston, 2001; McLucas, 1991; Sadeh, 2002)

[63] Weeks, E. (2007). *The politics of space law in a post-Cold War era: Understanding regime change*. Northern Arizona University.

Overt support from the government towards the development of the commercial satellite communications industry was ultimately in the interest of the state. Specifically, both DOD and NASA sought to gain by supporting private firms in developing and deploying satellite technology given the convergence of civilian and military satellite communications systems from 1960 to 1980[64]. Conversely, the success of the satellite industry also relied heavily on available military technologies such as military ballistic missiles for satellite launching services and insights from DOD's defense communication satellite programmes of the 1960s[65].

During this period, fledgling commercial space industries were being encouraged by pro-industry legislation. For example, the *Commercial Space Launch Act* of 1984 promoted private investment and entrepreneurial activity in space; it was subsequently amended in 1988 to require that launch companies obtain insurance and use cross-waivers in order to minimise liability in the case of accidents and failures, further incentivising commercial activity. The *Land Remote Sensing Commercialization Act* of 1984 also encouraged the privatization of the market for collecting and selling remote sensing data that had been obtained by government-owned Landsat satellites.

3.2.2.2 Researchers <> State

Interactions between researchers and the state during phase 1 took two forms. Firstly, government-funded researchers were central to the development of space technology and policy. Secondly, researchers were used as political tools of the state particularly in signalling cooperative intentions.

[64] (Evans et al., 2011; Slotten, 2002)
[65] (Evans et al., 2011)

3.2.2.2. Researchers as developers of space technology and policy

The missile and rocketry research that formed the foundations of the American space industry was carried out largely by academics and technical universities funded directly by the government. Some of the earliest government-funded research programmes include the Guggenheim Aeronautical Laboratory based at the California Institute of Technology (Caltech) which was a site of jet propulsion research and early prototypes of rocket-assisted take-off devices. In the early 1940s, Caltech received increasing amounts of funding from the National Defense Research Committee and the DOD's Office of Research and Development for extensive rocket programmes. George Washington University also received major university contracts from the U.S. Army, as did an army-affiliated research laboratory in Maryland. The U.S. Navy partnered with the Applied Physics Laboratory at John Hopkins University[66].

Simultaneously, researchers at RAND Corporation became heavily influential in shaping the state's actions with respect to investment in military space programmes. In May 1946, RAND released a report that was notable in its foresight; the report concluded: 'Satellites would undoubtedly prove to be of great military value', emphasizing both its potent potential as a scientific tool for the study of cosmic rays and gravitation as well as its symbolic importance as an achievement that 'would inflame the imagination of mankind and would probably produce repercussions in the world comparable to the explosion of the atomic bomb'. Another report from RAND in February 1954 concluded that ICBMs were technically feasible sooner than had been predicted, and that the U.S. was losing to the Soviets in the ICBM race. The U.S. Air Force subsequently commissioned RAND to continue studying the military utility of satellites; on October 4, 1950 RAND thus released a report that delved into the political and military implications of earth satellites. This landmark report heavily shaped

[66] (Moltz, 2011)

the origins of American space policy, and directly triggered the circulation of U.S. Air Force General Operations Requirement #90 on March 16, 1955 announcing the parameters of Project WS-117L on the establishment of the first American strategic satellite system[67]. Thus, RAND poses an example of how researchers were not only relevant in shaping the technology itself but were also influential in shaping the strategic policy that underpinned its development.

3.2.2.2. Cooperation in research as a political tool

In a period defined by Cold War tensions between the U.S. and the USSR, cooperation in space science became one of a number of political tools exercised by the two rivalrous states, and in some instances, reflected genuine cooperative intentions. The orbital flight of Yuri Gagarin on April 12, 1961 triggered an uptick in the political rhetoric of space science cooperation. Premier Khrushchev stated in a letter to President Kennedy: 'If our countries pooled their efforts…to master the universe, this would be very beneficial for the advance of science and would be joyfully acclaimed by all peoples.'[68] Kennedy responded in kind: 'Let's both sides seek to invoke the wonders of science instead of its terrors. Together let us explore the stars.'[69] The Kennedy Administration seemingly had genuine intentions of following through, proposing a number of bilateral projects including joint efforts in weather satellites, tracking services, and satellite communications. Kennedy even proposed turning the Apollo programme into a joint U.S.-Soviet effort, stating: 'Why should man's first flight to the Moon be a matter of national competition?'. Unfortunately, Kennedy's assassination put a halt to these projects before they could be realised[70].

[67] (McDougall, 1997; Moltz, 2011)
[68] Ezell, E. C., & Ezell, L. N. (1978). *The Partnership: A History of the Apollo-Soyuz Test Project*. NASA Special Publication-4209.
[69] Shackelford, S. J. (2014). Governing the Final Frontier: A Polycentric Approach to Managing Space Weaponization and Debris. *American Business Law Journal*, *51*(2), 429–513.
[70] (Shackelford, 2014)

Empowered by this strand of political rhetoric, the nations' scientific communities made multiple attempts at establishing bilateral cooperative efforts in space research, to varying degrees of success. In late 1959 and 1960, NASA initiated a new round of bilateral space science proposals. This began with a meeting of the American Rocket Society in November 1959 during which NASA's then-Deputy Administrator Hugh Dryden escorted visiting Soviet academicians Leonid I. Sedov (then-President of the Soviet Commission for Interplanetary Communications) and Anatoliy A. Blagonravov (then-Vice President of the USSR Academy of Sciences) through NASA facilities. NASA Administrator T. Keith Glennan subsequently offered the Soviet Academy of Sciences use of the U.S. space tracking network to address the 'blind' periods where communications from Soviet spacecraft could not reach Soviet receiving stations because of the curvature of the Earth[71]. On both occasions, the Soviets failed to reciprocate or follow up – Soviet scientists had comparatively less power to signal cooperative intentions on behalf of the USSR[72].

A second round of attempts commenced in March 1962 with negotiations in New York between NASA's Dryden and the Soviet academician A. A. Blagonravov, with follow-up negotiations in Geneva in May. The two scientists reached an agreement – which came to be known as the Dryden-Blagonravov agreement – providing for three areas of cooperation: space communications, space meteorology and geomagnetic surveys. In October, the agreements were formalized by the American and Soviet governments. The official Soviet news agency, Tass, summarized the significance of the event: 'There is no doubt that this agreement will make a great contribution to the conquest of the universe and to the further advance of international cooperation between scientists.'[73]

---

[71] Schauer, W. H. (1976). *The politics of space. A comparison of the Soviet and American space programs*. New York: Holmes and Meier.
[72] (Moltz, 2011)
[73] NASA. (n.d.-b). The First Dryden-Blagonravov Agreement - 1962. Retrieved October 6, 2018, from https://www.hq.nasa.gov/pao/History/SP-4209/ch2-3.htm

Even as U.S.-Soviet relations deteriorated politically under the Ford and Carter administrations, cooperation in pursuit of science and knowledge continued, albeit often at a halting pace due to lack of political buy-in from the respective governments. In 1979 an agreement was established to form COSPAS (the Russian acronym for 'Space System for the Search of Vessels in Distress') and SARSAT (the U.S. 'Search and Rescue Satellite-Aided Tracking'). This joint rescue system would involve the use of transmitters aboard ships and aircraft linked to a joint satellite network to receive and locate distress signals worldwide. A number of biomedical research projects and data-sharing initiatives were also driven forward by both government scientists and commercial scientists[74].

The space research community were in a unique position to improve relations between the U.S. and the USSR given the strong sense of internationalism among the community of scientists and technologists. However, among scientists at the time, the salience of their national identity and the underlying patriotism that motivated much of scientific pursuit during the Space Race meant that researcher-led cooperation hit its limits without political support. Arnold Frutkin, the NASA Deputy Director for international affairs during the Space Race, reflects[75]:

> The evidence appears to be overwhelming that scientists confronted with the exigencies of national need have reacted much as other patriotic citizens, professional and nonprofessional…International ties [between scientists], real or fancied, have not weighed in the balance in any significant way…When we say that science is international we mean that it is international where scientific matters of essentially professional

[74] (Gotlieb & Dalfen, 1970; Moltz, 2011)
[75] Frutkin, A. W. (1965). International cooperation in space. NASA.

character are concerned, and not really where political matters are concerned.

Indeed, some scholars have reflected that space cooperation during the Cold War was in fact motivated by the antagonistic competitive dynamics between the two superpowers. They argue that the value of declaring space to be an arena of common human pursuit was of prudent, selfish interest to both states in order to hinder domination of outer space by the other[76]. Thus, how much one can separate scientific cooperation from political competition during this period is unclear.

[76] Dolman, E. C. (2002). *Astropolitik : classical geopolitics in the space age*. London: Frank Cass.; Meijer, H. L. E. (2009). Reflections on Politics, Strategy and Norms in Outer Space. *Defense & Security Analysis*, *25*(1), 89–98. https://doi.org/10.1080/14751790902749942

3.3 Phase 2: Commercialisation and proliferation [1992 - 2000]

The end of the Cold War and the dissolution of the Soviet Union in 1991 shifted the tectonic plates of the global geopolitical environment. Phase 2 – *commercialisation and proliferation* – thus commenced with dramatic changes in the military and economic balance of power across the world, and with that, dramatic changes in the state of the aerospace industry.

In the U.S., the end of the Cold War marked a sobering of national interest in space – there was no longer an overt race with another superpower, and the post-Soviet space policies were more open and less adversarial. The government decreased funding for space activities, and the aerospace industry responded to the narrowing business opportunities by seeking mergers as a way to integrate strengths, combine resources, and reduce costs by eliminating redundancies[77].

American market dominance in the worldwide aerospace industry took a downturn as of 1998. The U.S. percentage of the world launch vehicle market dropped from 50% in the year 2000 to 20% in 2002, and the percentage of the world satellite market dropped from 65% between 1997 and 1999 to 40% in 2001 and 2002[78]. Simultaneously, an increasing number of state and non-state actors emerged as viable competitors in the global aerospace market. Indeed, by the turn of the century, a number of countries had positioned themselves as viable space actors alongside the U.S. and Russia and had captured substantial proportions of the space launch services and satellite markets[79]. From 1991 to 2016, for example, 43% of new satellites and 39% of space launches were from nations other than the U.S. and Russia, most prominently China, Japan, Europe and India[80].

Towards the end of the 1980s the trend in U.S. domestic law increasingly favoured the expansion of the private sector in new space industries, creating incentives for commercial enterprises to

[77] (Weiss & Amir, 2018)
[78] (Johnson-Freese, 2007)
[79] For an up-to-date overview of the capabilities of spacefaring nations, see: Dawson, L. (2017). *The Politics and Perils of Space Exploration : Who Will Compete, Who Will Dominate?* Cham: Springer International Publishing : Imprint: Springer.
[80] (Harrison et al., 2017)

pursue emerging areas such as remote sensing, data imagery, and commercial space launch and transportation services[81]. Section 3.3.1.1 provides an overview of the emergence of commercial and military application of aerospace technologies given this firm-friendly legislative environment. Separately, section 3.3.1.2 describes the emergence of China as a potential space power and the consequent deterioration of U.S.-China relations. Section 3.3.2 proceeds to describe how the relationships between the state, firms, and researchers evolved across Phase 2.

3.3.1 Notable events

3.3.1.1 The emergence of commercial and military applications

The private sector component of the aerospace industry had up until the late 1980s primarily consisted of contractors for government programmes. As the end of the Cold War loomed and as the cost of aerospace technologies decreased, companies began to turn their attention towards new applications and business models for operating in space. Aerospace, and specifically outer space technologies, thus transitioned from being fuelled by inter-state competition for prestige and military prowess to inter-firm competition for market dominance and profit[82]. The commercialisation of space was encouraged and accelerated by a host of U.S. laws and policies designed to promote the privatization of space[83].

Space transportation in particular became of interest to a number of companies[84]. The first commercial launch service provider was established in 1980 as Arianespace, and the U.S. opened the door for private launch service providers in 1984. In the satellite industry, private companies began to compete with INTELSAT and its sister intergovernmental organisation, the International

[81] (Weeks, 2007)
[82] Aldrin, A. J. (1998). Technology Control Regimes and the Globalization of Space Industry. *Space Policy*, *14*(2), 115–122.
[83] Bromberg, J. L. (2000). *NASA and the Space Industry*. Baltimore MD: JHU Press.; McLucas, J. L. (1991). *Space commerce*. Cambridge MA: Harvard University Press.
[84] (Weeks, 2007)

Maritime Satellite Organisation (INMARSAT); both companies were thus pushed into privatization in 2001 and 1998, respectively[85].

Private companies also began to expand the types of activities that could be conducted in space. In 1984 SPACEHAB Inc. was incorporated as one of the earliest private companies to provide space habitat micro-gravity experimentation equipment and services to NASA[86]. SPACEHAB's experimental science and research laboratory, known as the 'Research Module', doubled the amount of working and living space available to astronauts and was one of the first facilities to enable companies to conduct privately funded research alongside public research[87]. The first commercial satellite to capture images in colour was SeaStar which was launched into orbit on August 1, 1997 by commercial launch service company Orbital Sciences Corporation on Pegasus, the first privately developed space launch vehicle. The SeaStar program continues to provide daily ocean colour imagery and data to NASA and private businesses across the world[88]. We even saw the establishment of a space funeral company, Celestis Inc., in 1994; to date, Celestis has launched into space the cremated human remains of notable figures such as Star Trek's creator Gene Roddenberry and the iconic American psychologist Timothy Leary.

As of 1996 commercial revenues from space exceeded government revenues for the first time at 53% and 47%, respectively. The two dominant commercial space activities at the time were infrastructure at 61% (which includes the likes of launch facility operations and satellite and launch vehicle manufacturing) and telecommunications at 30% (which includes services such as international telephone services, direct-to-home television and radio broadcasting). Emerging applications such as remote sensing, geographic information systems (GIS) and micro-gravity

[85] von der Dunk, F. G. (2018). Billion-dollar questions? Legal aspects of commercial space activities. *Uniform Law Review*, *23*(2), 418–446. https://doi.org/10.1093/ulr/uny022
[86] Since 2009 SPACEHAB Inc. has operated under the name Astrotech Inc.
[87] Astrotech. (n.d.). Astrotech | About Us. Retrieved October 7, 2018, from http://www.astrotechcorp.com/about-us; Livingston, D. (2001). *Outer space commerce: Its history and prospects*. Golden Gate University.
[88] The SeaStar program has been renamed the ORVIEW 2 program.

R&D sat at 5%. The space industry employed 835,900 employees and worldwide revenues totalled $77 billion[89].

On the military front, the first 'space war' – that is, the first time space-based capabilities played a critical role in conventional military operations – was Operation Desert Storm of 1991[90]. This demonstration of the utility of space technologies for conventional warfare spurred General Chuck Horner, commander of the aerial forces for Operation Desert Storm and former Commander of the Air Force Space Command, to state: 'What we have to do is change our [space] emphasis from strategic war to theatre war'.

In the subsequent ten years, Horner advocated successfully for the integration of space into conventional combat theatre tactics and direct combat support. Space capabilities quickly became critical in enabling the DOD to deploy smaller and more mobile force structures. GPS became central to how U.S. forces located and destroyed targets, planned operations, controlled war-fighting assets, and synchronized ground troops and remotely piloted aircraft. Satellite imaging augmented target location and identification, missile warning and defense, and route planning[91].

3.3.1.2 The deterioration of U.S.-China relations

In the evolving relationship between the U.S. and China, space was but one of many facets where there was escalating tension and a deterioration in diplomacy during this phase. In response to fears of Chinese espionage, in November 1989 Congress prohibited approval of any export license applications for the launch of U.S. satellites aboard Chinese rockets. The President was given the authority to waive these sanctions if China made progress in political and human rights reforms.

[89] KPMG Peat Marwick. (1997). *1997 Outlook: State of the Space Industry*. KPMG Peat Marwick, SpaceVest, Space Publications, and Center for Wireless Telecommunications.
[90] (Couvault, 1991)
[91] (Pawlikowski et al., 2012)

Existing sanctions were expanded in 1990 with the passing of the *Foreign Relations Authorization Act* which suspended licenses given to any U.S. satellites to be flown on a Chinese rocket.

Then, in 1996, these controls were relaxed somewhat with the shifting of the export licensing authority for commercial satellite technology from the State Department to the Department of Commerce. This made it easier for U.S. satellite companies to cooperate with Chinese companies. However, this was abruptly turned around with the Loral-Hughes satellite scandal of 1998. In April 1998 it was reported that the Department of Justice was investigating U.S. firms Loral Space Communications and Hughes Electronics Corporation for violation of export control laws[92]. The *Select Committee on U.S. National Security and Military/Commercial Concerns with the People's Republic of China* (referred to as the Cox Committee after its Chairman Representative Christopher Cox) was established to investigate the issue further. In a classified report released on December 30, 1998 the committee concluded that China's technology acquisitions over the past twenty years have harmed U.S. national security and that steps should be taken to tighten export controls on satellite technology[93]. In the fall of 1998 Congress passed the *FY1999 Strom Thurmond National Defense Authorization Act* that transferred the licensing authority for commercial satellite technology back to the State Department as a sensitive military technology[94]. The State Department was also provided increased means of preventing the spread of sensitive technologies and declared

[92] The firms had shared findings with their Chinese counterparts from an investigation into the cause of a Chinese rocket explosion in February 1996, which was carrying a U.S. satellite. It was claimed that by sharing this information the firms had provided expertise to China that could be used to improve the accuracy and reliability of its future ballistic missiles. At least three classified studies reportedly found that U.S. national security was harmed as a result of this technical assistance. For further detail on the case, see: Kan, S. A. (2001). *China: Possible Missile Technology Transfers from U.S. Satellite Export Policy – Actions and Chronology* (CRS Report for Congress). Washington, D.C.: Congressional Research Service. Retrieved from https://fas.org/sgp/crs/nuke/98-485.pdf

[93] Select Committee on US National Security and Military/Commercial Concerns with the Peoples' Republic of China. (1999). *US National Security and Military/Commercial Concerns with the Peoples' Republic of China*. Washington, D.C.: The White House. Retrieved from https://www.gpo.gov/fdsys/pkg/GPO-CRPT-105hrpt851/pdf/GPO-CRPT-105hrpt851.pdf

[94] For a detailed overview of both the Cox Committee report as well as how this was subsequently translated into the reforms of the U.S. export control system in 1998-1999, see: Johnson-Freese, J. (2000). Alice in Licenseland: us satellite export controls since 1990. *Space Policy*, 16(3), 195–204.; Johnson-Freese, J. (2001). Becoming Chinese: Or, How U.S. Satellite Export Policy Threatens National Security. *Space Times*.

fundamental research and academic intellectual information related to satellite technology as munitions[95].

Further, a Senate task force was established on May 20, 1998 to review U.S. export control policies on launches of U.S. built satellites on Chinese launch vehicles. On May 7, 1999 the task force released a report that recommended strengthening control over satellite exports including giving the Defense Threat Reduction Agency the authority to suspend launch-related activities. On October 5, 1999 the President signed into law *FY2000 National Defense Authorization Act* in which export controls relating to missile technology and satellites were further tightened[96].

Whilst satellite export controls became the lightning rod issue, it is important to bear in mind the broader context of a deteriorating U.S.-China relationship. The Tiananmen Square protests of 1989 had soured the political climate between the two countries, as had the issue of military and diplomatic support for Taiwan[97]. Indeed, within Washington a group who called themselves the 'Blue Team' began meeting in the mid-1990s, unified by their strong anti-China views and support for confrontational foreign policy towards China. The Blue Team became a consistent lobbying force within the U.S. government across this period, including in advocating for harsher satellite export control rule[98].

[95] Specifically, the Strom Thurmond National Defense Authorization Act provided for the following:
- Enabling the State Department to reserve the right to apply the controls to everyday transactions even with allies;
- Requiring that export licenses were required to return hardware to its country of origin;
- Directing the President to implement measures such as mandatory licensing for U.S. persons involved for the investigation of the failure of a launch in a foreign country of a satellite of U.S. origin;
- Restricting the President's authority to issue waivers by mandating notification of the U.S. Congress of the approval of a license for all exports of a U.S. satellite;
- Mandating review by the intelligence community of all export license applications and technical assistance agreements.

[96] (Kan, 2001)

[97] Reddy, V. S. (2017). U.S.-China Space Cooperation: Balancing Act between the U.S. Congress and President. *Astropolitics*, *15*(3), 235–250. https://doi.org/10.1080/14777622.2017.1378962

[98] (Johnson-Freese, 2007)

3.3.2 Relationships

3.3.2.1 Firms <> State

The relationship between firms and the state can be segmented into two distinct dynamics. The first is a reliance on commercial technologies to support the U.S. military industrial base, creating a synergistic dependence between firms and the state. The second is a conflictual dynamic centred around satellite export control reform.

3.3.2.1. Increasing reliance on commercial technologies

The U.S. government, and specifically the DOD, became ever more reliant on firms to provide them with space technologies as the prominence of state-funded and state-led space programmes decreased. The demand for satellite communications, for example, increasingly outpaced the capacity of military systems; the DOD have thus had to turn to leasing capacity from commercial satellite operators and indeed have benefitted from the relatively low cost compared to maintaining systems of their own[99].

In commercial space transportation, the winding down of the Space Shuttle programme rendered it necessary to partner with commercial firms in order to ensure U.S. access to space. Initially, the Space Shuttle was designated by law as the 'sole provider of American civilian launch services'; private companies who were producing ELVs at the time had to phase out their operations as a result[100]. However, the Space Shuttle Challenger loss in January 1986 and the two vehicle failures later that year grounded the Space Shuttle fleet. Regan thus signed *National Security Decision Directive 254* on December 27, 1986 overturning the Space Shuttle's monopoly of the launch market and welcoming commercial launchers into the market.

[99] (Harrison et al., 2017; Hays, 2010)
[100] Fought, B. E. (1988). Legal Aspects of the Commercialization of Space Transportation Systems. *High Technology Law Journal*, *3*, 99.

The convergence of the technology base for commercial and military systems was not painless, however. An in-depth analysis by former U.S. Air Force officials cites a number of challenges, both structural and cultural, which impeded the integration of commercial technologies into the technology base that underpinned U.S. space capabilities. In doing so, they conclude that whilst leveraging the competitive commercial satellite bus market and hosting payloads on commercial platforms are desirable goals, significant reformation is still required to realise these benefits[101].

3.3.2.1. Friction over export controls

Across the 1980s and 1990s, export restrictions on satellite technology had been progressively loosened by the Reagan, Bush and Clinton administrations in recognition of the importance of keeping the American space industry competitive in the global market. Throughout this period, firms were active and relatively successful in lobbying for their interests. For example, in August 1993 the Clinton Administration announced new sanctions against China in response to evidence that China had transferred missile-related technology to Pakistan. These sanctions halted a number of large contracts aerospace companies such Martin Marietta and Hughes Aircraft were engaged in with Chinese launch services, spurring intensive industry lobbying. By January 1994 the Clinton Administration had yielded to a number of exemptions for the affected companies. By October 1994 the sanctions had been lifted, and in December 1994 President Clinton had named Michael Armstrong, CEO of Hughes Aircraft as leader of the Export Council[102]. Then, in 1996, the transferring of commercial satellites from the United States Munitions List (USML) to the Commerce Control List (CCL) marked a temporary 'win' by the commercial satellite industry.

[101] (Pawlikowski et al., 2012)
[102] Kan, S. A. (2001). *China: Possible Missile Technology Transfers from U.S. Satellite Export Policy – Actions and Chronology* (CRS Report for Congress). Washington, D.C.: Congressional Research Service. Retrieved from https://fas.org/sgp/crs/nuke/98-485.pdf; Lamb, R. D. (2005). *Satellites, Security, and Scandal: Understanding the Politics of Export Control* (CISSM Working Paper). Center for International & Security Studies at Maryland. Retrieved from http://www.cissm.umd.edu/publications/satellites-security-and-scandal-understanding-politics-export-control-0

This was abruptly reversed by the Strom Thurmond Act of 1999, which declared that communications satellites and all of their associated components and research were munitions in the eyes of the state, irrespective of its intended use and intended recipient. This had a chilling and conclusively negative effect on the commercial satellite industry[103]. In 1995, U.S. companies held 90% of the market share of the satellite components market worldwide; in 1999 this dropped to 56%. International projects such as INTELSAT were affected, with the new export control rules delaying shipments of benign components such as screws[104]. In response, INTELSAT threatened to move its headquarters outside the U.S. due to the 'unfriendly' environment created by the export control rules[105]. Foreign companies began to sever ties with U.S. companies due to complaints about their dependability. Germany's DaimlerChrysler Aerospace decided to divest itself of U.S. subcontractors; Telesat Canada decided in 2003 to purchase their satellites from a French company rather than risk licensing issues with their longstanding U.S. partners[106]. German officials reportedly considered appealing the export control rules to the World Trade Organisation[107].

Within the U.S. government, some had quickly realised the detrimental effects of the export control reforms. James Sensenbrenner, then-Chairman of the House Science Committee, stated in an address in May 1999: 'Members of Congress are clearly growing concerned about the potential damage to the U.S. satellite industry and some are blaming overzealous government bureaucrats for the slowdown of export license decisions.'[108] Others raised concerns that by weakening domestic manufacturing capacity of satellite components and subsystems, this weakened the

[103] Lewis, J. A. (2003). *Preserving America's Strength in Satellite Technology* (CSIS Satellite Commission). Center for Strategic and International Studies (CSIS). Retrieved from https://www.csis.org/analysis/preserving-americas-strength-satellite-technology
[104] Lawrence, S. V. (1999). Clipping Their Wings. *Far Eastern Economic Review*.
[105] SpaceNews. (1999). Intelsat Might Move Out of US. *SpaceNews*.
[106] Chang, L. (1999). US Firms Rue Negative Effects of Cox Report – Stricter Scrutiny of Ties to China May Threaten Lucrative Contracts. *Asian Wall Street Journal*.
[107] deSeldin, P. B. (1999). US Export Rules Frustrate Germans. *SpaceNews*.
[108] Anselmo, J. (1999). Congress Seeks Fix to Export Quagmire. *Aviation Week & Space Technology*.

domestic industrial base and thus forced the U.S. military to increase their dependence on foreign suppliers, undermining national security[109].

The outcome of the cases against Loral and Hughes sent an ominous signal to firms in their battle against the state on export controls. Despite both investigations not yielding conclusive evidence to prove the government's case, both companies ended up paying fines to the State Department to preserve their capacity to gain licenses in the future[110]. Loral settled in January 2000 for $20 million, and Hughes (which had been acquired by Boeing in 2000) settled in December 2002 for $32 million. Loral filed for bankruptcy in July 2003 due to falling demand for their products.

[109] Johnson, D. J., Pace, S., & Gabbard, B. C. (1998). *Space: Emerging Options for National power*. RAND Corporation. Retrieved from https://www.rand.org/pubs/monograph_reports/MR517.html; Smith, D. D. (2001). A double-edged sword: Controlling the proliferation of dual-use satellite systems. *National Security Studies Quarterly*, 7(2), 31–68.
[110] (Johnson-Freese, 2007)

3.4 Phase 3: Consolidation and contestation [2001 – Present]

Phase 3 – *consolidation and contestation* – marks a New Space Age, an era in which the reaping of the economic and military value of space technologies become prominent national goals for the U.S. as well as China. This restokes rivalrous dynamics between two superpowers, mirroring the political patterns observed in phase 1. Once again, the goals of the state become a predominant driver of the dynamics that emerge between actors in the aerospace industry on both the political and commercial fronts.

On the political front, the U.S. national posture in space took on a flavour of overt military aggression under President Bush's leadership, set against a backdrop of the September 11 attacks of 2001 and the U.S. withdrawal from the Anti-Ballistic Missile Treaty in 2002; this is described in section 3.4.1.1. The central target of this aggression was China whose actions in space have sparked what some are calling a U.S.-China Space Race, as described in section 3.4.1.2.

On the commercial front, a set of new space actors emerged onto the scene, beginning in 2000 with Jeff Bezos' Blue Operation LLC (the pre-cursor to the Blue Origin aerospace company) and in 2002 with Elon Musk's Space Exploration Technologies (SpaceX). Their entry into the market was symptomatic of the ever lucrative commercial opportunities in space as complementary information technologies became more available, demand from end users for data-driven products and services increased, and space technologies and its components became cheaper to manufacture. This technology-entrepreneur-led wave of space commercialization is described in section 3.4.1.3.

Phase 3 also saw the gradual fizzling out of international cooperation in space, particularly in the progression of international space law[111]. With the exception of orbital debris management,

[111] (Shackelford, 2014)

establishing multilateral consensus on the norms and constraints on space activities has become more difficult with the emergence of multiple capable state and non-state actors.

3.4.1 Notable events

3.4.1.1 The doctrine of space control

The doctrine of space control – to ensure freedom of action in space for the United States and its allies and deny an adversary freedom of action in space[112] - has been the strategic foundation of space policy since the early 2000s. Its interpretation, however, has progressively shifted towards the development of offensive capabilities in space as a means of assurance of control. This was certainly the case during the Bush Administration, and after a brief hiatus during the Obama Administration, the Trump Administration has signalled a continuation of this trend towards space weaponization.

3.4.1.1. The Bush Administration

President George W. Bush's campaign rhetoric portrayed space as an arena primarily for military defense, citing a perceived rise of missile threats to the U.S. and what he perceived as the increasing irrelevance of international arms control agreements[113]. Once in office, President Bush appeared intent on following through with these sentiments. Post the September 11 attacks of 2001, military space programmes – particularly those for missile defense – saw huge increases in military spending. The U.S. withdrew from the Anti-Ballistic Missile Treaty in 2002, marking the first time that the U.S. had withdrawn from a major international arms treaty and dealing a significant blow to international arms control. Shortly afterwards, the Missile Defense Agency was established, responsible for developing ground, sea and space-based defense systems against ballistic missiles. The Missile Defense Agency proceeded to invest in a number of space systems, including space-

[112] Joint Chiefs of Staff Department of Defense. (2002). *Joint Doctrine for Space Operations, Joint Publication 3-14*. Washington, D.C.: Department of Defense.
[113] (Moltz, 2011)

based ballistic missile interceptors that would attack ballistic missiles in boost phase. Given the technological similarities between ballistic missiles and space launchers, many considered an investment in missile defense programmes a step towards space weaponization[114].

The Bush Administration's space policy was heavily influenced by the Space Commission. Senator Bob Smith, a vigorous advocate for space weaponization, was a critical figure in the mid-1990s in pushing for the creation of a Space Commission to evaluate the need for reform of U.S. military space organisation and capabilities. Thus, the *Commission to Assess United States National Security, Space Management and Organization* ('Space Commission') was established with former Secretary of Defense Donald Rumsfeld as its chair. Rumsfeld was subsequently nominated to serve as the Secretary of Defense under President Bush, uniquely enabling Rumsfeld to ensure that the Space Commission's recommendations were implemented. In its final report, the Space Commission called for the development of physically destructive anti-satellite capabilities and the development of 'live firing ranges' in space to tests these systems on a regular basis. It also recommended that the U.S. take the approach of ignoring the alleged legal impediment to the use of weapons in space, asserting that the U.S. had the legitimate right of self-defence including 'anticipatory' self-defence[115]. Despite reaffirming the American commitment to the peaceful use of space, the Commission's report overwhelmingly invoked a sense that the U.S. were facing a potential existential threat if it did not adequately prepare for a 'Space Pearl Harbour' event[116].

This framing took hold within the White House. The 2002 *U.S. National Security Strategy* stated the goal to 'dominate the space dimension of military operations' as being necessary to maintain technological supremacy via 'the ability to defend the homeland, conduct information operations, ensure U.S. access to distant theatres, and protect critical U.S. infrastructure and assets in outer

[114] Meijer, H. L. E. (2009). Reflections on Politics, Strategy and Norms in Outer Space. *Defense & Security Analysis*, *25*(1), 89–98. https://doi.org/10.1080/14751790902749942
[115] (Commission to Assess United States National Security Space Management and Organization, 2001)
[116] Peoples, C. (2011). The Securitization of Outer Space: Challenges for Arms Control. *Contemporary Security Policy*, *32*(1), 76–98. https://doi.org/10.1080/13523260.2011.556846

space'[117]. The *National Space Policy* of 2006 echoed the perceived irrelevance of international space law, stating that 'the United States will oppose the development of new legal regimes or other restrictions that seek to prohibit or limit U.S. access to or use of space'[118]. The U.S. Air Force Doctrine Document entitled 'Counterspace Operations', released in August 2004, alluded to the development of offensive space weapons and their pre-emptive use as being necessary to achieve their strategic ambitions in space[119]. This was followed by an Air Force request for the administration's approval to 'move the United States closer to fielding offensive and defensive space weapons' in May 2005[120]. Later that year, the U.S. became the only country to vote 'no' against a total of 160 'yes' votes on a UN resolution calling for negotiations on a treaty to ban space weaponization[121]. By contrast, the Bush Administration's attempts at a civilian space programme, launched in 2004 under the banner of the *New Vision for Space Exploration,* received no presidential follow-up and faced a number of threats to budget cuts in Congress[122].

3.4.1.1. The Obama Administration

Under the Obama Administration, U.S. space policy temporarily pivoted towards overtures of cooperation and civilian space applications. In the 2010 *National Security Strategy* the U.S. dependence on space capabilities was framed as a reason to pursue cooperation rather than as grounds for unilateralism: 'Across the globe, we must work in concert with allies and partners to optimize the use of shared sea, air, and space domains'. The administration also gave strong indications that it would support a global ban on weapons that interfere with commercial and

---

[117] The White House. (2002). *The National Security Strategy of the United States of America*. Washington, D.C.: The White House. Retrieved from https://www.state.gov/documents/organization/63562.pdf
[118] The White House. (2006). *U.S. National Space Policy*. Washington, D.C.: The White House. Retrieved from https://obamawhitehouse.archives.gov/sites/default/files/microsites/ostp/national-space-policy-2006.pdf
[119] (Joint Chiefs of Staff Department of Defense, 2002)
[120] Weiner, T. (2006). Air Force Seeks Bush's Approval for Space Weapons Programs. *The New York Times*. Retrieved from https://www.nytimes.com/2005/05/18/business/air-force-seeks-bushs-approval-for-space-weapons-programs.html
[121] (Reddy, 2017)
[122] Rose, A. (2005). Bush's Space Vision. *National Review*.

military satellites[123]. Similar sentiments were echoed in the 2010 *National Space Policy* in which the civilian, commercial and scientific pillars of space activity were emphasized as the central components of American space policy[124].

To some extent, the Obama Administration was successful in making progress towards international cooperation in space. In 2013, the U.S. participated in a UN governmental expert meeting for confidence building and transparency measures in outer space[125]. In 2014, the U.S. also adopted a UN compendium of space debris mitigation standards[126]; in the same year, the U.S. expressed support for an EU proposal on governing the use of conventional weapons in orbit[127]. The U.S. and China even initiated discussions on space cooperation in May 2016, with a follow up meeting in late 2016[128]. However, space was never a high priority issue for the Obama Administration; thus, any groundwork that was laid for a more cooperative approach to space from the U.S. proved easily overturned by the subsequent change in administration.

Meanwhile, it had become clear that Russia and China were developing the capacity to destroy U.S. satellites in response to the persistence of the U.S. military in pursuing counterspace operations[129]. In 2016 Russian Deputy Foreign minister Sergey Ryabkov voiced concerns about the possibility of weapons being deployed in space[130]. This statement was prompted by the U.S. Prompt Global Strike Program which had been developing hypersonic glide vehicles since the

---

123 The White House. (2010a). *National Security Strategy of the United States of America*. Washington, D.C.: The White House. Retrieved from https://www.hsdl.org/?abstract&did=24251

124 The White House. (2010b). *National Space Policy of the United States of America*. Washington, D.C.: The White House. Retrieved from https://www.nasa.gov/sites/default/files/national_space_policy_6-28-10.pdf

125 Johnson, C. (2014). *The UN Group of Governmental Experts on Space TCBMs: A Secure World Foundation Fact Sheet*. Secure World Foundation. Retrieved from https://swfound.org/media/109311/swf_gge_on_space_tcbms_fact_sheet_april_2014.pdf

126 United Nations Office for Outer Space Affairs. (2014). Compendium of space debris mitigation standards adopted by States and international organizations. Retrieved September 25, 2018, from http://www.unoosa.org/oosa/en/ourwork/topics/space-debris/compendium.html

127 Roberts, T. G. (2017). Why We Should Be Worried about a War in Space. *The Atlantic*. Retrieved from https://www.theatlantic.com/science/archive/2017/12/why-we-should-be-worried-about-a-war-in-space/548507/

128 Gruss, M. (2016). U.S., China will meet this year to talk space debris. *SpaceNews.Com*. Retrieved from https://spacenews.com/u-s-china-will-meet-this-year-to-talk-space-debris/

129 (Al-Rodhan, 2018b)

130 Gazeta, R. (2016). Moscow worried over possibility of deployment of attack weapons in space. *Russia Beyond*. Retrieved from https://www.rbth.com/news/2016/02/08/moscow-worried-over-possibility-of-deployment-of-attack-weapons-in-space_565825

mid-2000s[131]. Russian military journals reportedly featured articles presenting American hypersonic weapons as an existential threat to Russia, and in 2015 the Russians replaced its air force with a new Aerospace Forces branch specifically aimed at defending against the Prompt Global Strike Program[132]. Similar responses from the Chinese government and the People's Liberation Army are described in section 3.4.1.2. Despite the Obama Administration's attempt at reshaping the international discourse on space, the escalation in space militarisation and weaponization had effectively continued unabated.

3.4.1.1. The Trump Administration

The Trump Administration has thus far signalled a renewed interest in space. On June 30, 2017 President Trump resurrected the National Space Council with an executive order[133]. Further, the White House has announced a national priority of returning to the moon in the 2020s and venturing to Mars by the 2030s[134].

On defense, the Trump Administration appears to have picked up where the Bush Administration left off with regards to building up U.S. military space capabilities and technological prowess[135]. At a 2017 conference U.S. Navy Vice Admiral Charles A. Richard, Deputy Commander of the U.S. Strategic Command, stated: "I submit [that] the best way to prevent war is to be prepared for war, and we're going to make sure that everyone knows we're going to be prepared to fight and win wars in all domains, including space."[136] U.S. Air Force Chief of Staff General David Goldfein told

---

131 Beckhusen, R. (2015). Russia Is Concerned About America's Far-Off Space Weapons. *Motherboard*. Retrieved from https://motherboard.vice.com/en_us/article/d73az7/russia-is-concerned-about-americas-far-off-space-weapons

132 RT. (2015). Russia boosts air defense in face of US Prompt Global Strike capacity. *RT International*. Retrieved from https://www.rt.com/news/246869-global-strike-missile-defense/

133 Malik, T. (2017). Resurrected National Space Council Will Hold 1st Meeting Oct. 5. *Space.Com*. Retrieved from https://www.space.com/38300-national-space-council-first-meeting-date.html; SpaceNews. (2017). President Trump Re-Establishes National Space Council. *Space.Com*. Retrieved from https://www.space.com/37363-president-trump-national-space-council.html

134 (Al-Rodhan, 2018d)

135 (Al-Rodhan, 2018c)

136 Wall, M. (2017). Star Wars: US Must Prep for Space Battles, Commander Says. *Space.Com*. Retrieved from http://www.space.com/36246-united-states-prepare-space-war.html

the *Washington Post* that they were working towards 'space superiority'[137]; articles by national security experts warn of the need to respond in the face of the risk that North Korea could kill 90% of Americans using a satellite weapon to send an electromagnetic pulse over the U.S. 'triggering widespread blackouts and societal collapse'[138].The 2017 *National Defense Authorisation Act* (NDAA) proposed the creation of a Space Corps, a new military service for space. In facing much opposition, notably from the Air Force Secretary Heather Wilson and the Chief of Staff David Goldfein, the final version of the bill does not create a Space Corps but does make a number of significant changes that give the Air Force Space Command additional authorities, laying the groundwork for the potential creation of the Space Corps in the future[139].

3.4.1.2 A U.S.-China Space Race?

The emergence of China as a space power has been uniquely rapid. From the launch of its first satellite in 1970, China became the third nation to put a man in space a mere 33 years later. Today, China boasts a record of successful crewed space flights, operates two space stations, and landed their *Jade Rabbit* rover on the moon in 2013, representing the first time that a robot had landed on the moon's surface in nearly half a century[140]. China operates its own navigation satellite system – BeiDou – and became the first country to begin testing a quantum-enabled satellite in 2016[141].

The Chinese government have certainly not been coy about the scale of their ambitions in space. In 2016 the State Council of the People's Republic of China (PRC) published a white paper on its space activities, stating that the country's vision was to 'build China into a space power in all

---

[137] Ignatius, D. (2017). War in space is becoming a real threat. *Washington Post*. Retrieved from https://www.washingtonpost.com/opinions/war-in-space-is-becoming-a-real-threat/2017/03/16/af3c35ac-0a8f-11e7-a15f-a58d4a988474_story.html

[138] Takala, R. (2017). How North Korea could kill 90 percent of Americans. *The Hill*. Retrieved from https://thehill.com/blogs/pundits-blog/defense/326094-how-north-korea-could-kill-up-to-90-percent-of-americans-at-any

[139] Harrison, T. (2017). Is Congress Creating a Military Space Corps? Retrieved September 25, 2018, from https://www.csis.org/analysis/congress-creating-military-space-corps

[140] Al-Rodhan, N. (2018a). China Aims for the Moon – and Beyond. Retrieved October 8, 2018, from https://thediplomat.com/2018/02/china-aims-for-the-moon-and-beyond/

[141] Wong, E. (2016). China Launches Quantum Satellite in Bid to Pioneer Secure Communications. *The New York Times*. Retrieved from https://www.nytimes.com/2016/08/17/world/asia/china-quantum-satellite-mozi.html

respects'[142]. In turn, they have significantly increased their spending in pursuit of this goal; in 2017 China was the country with the second highest expenditure in space at $11 billion[143].

On the military front, China's strategy is nominally one of active defense; according to their military strategy as of 2015, the PRC acknowledge that 'outer space and cyber space have become new commanding heights in strategic competition among all parties'[144]. The People's Liberation Army (PLA) have subsequently created a new organisation dedicated to both space and cyber space, known as the Strategic Support Force – its mission includes 'coordinating and executing electronic warfare, space/counter-space and cyber warfare activities[145]. In 2007, the PRC tested a kinetic-kill ASAT weapon targeted at a malfunctioning Chinese weather satellite, breaking an informal moratorium on destructive ASAT tests that had until then been upheld since the last such test by the U.S. in 1985[146]. Despite the international condemnation, in 2013 China launched another rocket ostensibly for a science mission but which was perceived as a practice run for future anti-satellite weapons[147].

The U.S. government's response has ranged from caution through to raised alarms of an impending arms race between the U.S. and China in outer space[148]. The launch of Shenzhou V on October 15, 2003 signalled China's entry into the space superpower club as the third country capable of manned spaceflight; whilst Russia and Europe welcomed China's success, the U.S. remained silent[149]. In the 2015 *U.S.-China Economic and Security Review Commission* report to Congress,

---

[142] The Information Office of the State Council. (2016). *China's Space Activities in 2016 (Published by Xinhua, translated by Global Times)*. The State Council Information Office of the People's Republic of China. Retrieved from http://www.globaltimes.cn/content/1025893.shtml

[143] (Harrison, Johnson, & Roberts, 2018)

[144] The Information Office of the State Council. (2015). *China's Military Strategy in 2015 (translated by USC US-China Institute)*. The State Council Information Office of the People's Republic of China. Retrieved from https://china.usc.edu/prc-state-council-chinas-military-strategy-2015-may-26-2015

[145] (Harrison et al., 2018)

[146] (Harrison et al., 2017)

[147] Paoletta, R. (2017). Military Officials Say We Need to Prepare for Space War. *Gizmodo*. Retrieved from https://gizmodo.com/military-officials-say-we-need-to-prepare-for-space-war-1793774231

[148] Johnson-Freese, J. Hearing on China's Space and Counterspace Programs, § U.S.-China Economic and Security Review Commission (2015).

[149] (Johnson-Freese, 2007)

it is noted that China's aspirations in space are driven by its judgement that space power enables the country's military modernization, enabling it to challenge U.S. information superiority during a conflict. It describes China's space and counterspace programs as being designed to negate American capabilities in space and warns that as China's developmental counterspace capabilities becomes operational 'China will be able to hold at risk U.S. national security satellites in every orbital regime'. Civilian space projects led by China were viewed as being directly supported by the PLA, and thus 'U.S. cooperation with China on space issues could mean supporting the PLA's space and counterspace capabilities'[150].

In Congress, the anti-Chinese rhetoric has reared its head on a number of occasions. In a 2007 House Appropriations Subcommittee review of NASA's budget, former House Majority leader Tom Delay declared that the U.S. was engaged in a 'space race' with China; representative Frank Wolf declared that 'if China beats us [to the moon], we will have lost the space program… they are basically, fundamentally in competition with us'[151]. The 2007 Chinese ASAT test was described as 'the first real escalation on the weaponization of space that we've seen in 20 years'[152]. Investments by Tencent Holdings (a Chinese technology company) in U.S.-based space start-ups such as Planetary Resources and World View Enterprises have been framed as tools of economic espionage by the PRC[153]. Consequently, Congress passed legislation in 2011 prohibiting NASA and the Office of Science and Technology Policy (OSTP) in the White House from initiating any bilateral cooperative activities with China or Chinese-owned companies[154]. The lack of transparency in China's military space programs and its release of technical information, compared

[150] David, L. (2015). Report Flags China's Space Prowess; Challenges Decades of U.S. Dominance in Space. Retrieved September 25, 2018, from http://www.LeonardDavid.com/report-flags-chinas-space-prowess-challenges-decades-of-u-s-dominance-in-space/
[151] Foust, J. (2006). The Space Review: China, competition, and cooperation. *The Space Review*. Retrieved from http://www.thespacereview.com/article/599/1
[152] Broad, W. J., & Sanger, D. E. (2007). China Tests Anti-Satellite Weapon, Unnerving U.S. *The New York Times*. Retrieved from https://www.nytimes.com/2007/01/18/world/asia/18cnd-china.html?_r=2&mtrref=undefined
[153] (Harrison et al., 2018)
[154] (Reddy, 2017)

to NASA and the ESA, fuels the mistrust between the U.S. and China with respect to its intentions in outer space[155].

3.4.1.3 A new wave of space commercialization

The commercial space industry has continued to grow, in large part driven by the rapidly decreasing cost of space technologies. Today, building a satellite is a far less costly and complicated endeavour, lowering the barrier to entry for new actors in the space industry. More powerful and energy efficient computing hardware has made it easier to construct a viable satellite at a far lower weight. The streamlining of satellite payload manufacturing has been made possible by additive manufacturing techniques such as 3D printing and laser sintering, as well as the sheer increase in demand for satellites enabling economies of scale in the manufacturing process[156]. The emergence of lighter satellites – from mini (500 kilograms) through to femto (10 and 100 grams) satellites – are all in development, opening up a range of potential applications in communications, signals intelligence, environmental monitoring, and geo-positioning[157].

The market for remote sensing data has boomed – its applications range from facilitating the peaceful settlement of border disputes and the verification of arms control agreements to detecting heat signatures using infrared imagery over a warzone[158]. From what used to be the exclusive domain of the government for the collection of classified imagery, today companies such as GeoEye, DigitalGlobe and Google offer civilians access to custom images in real-time.

The recent upsurge in enthusiasm for the commercial space industry is in no small part due to the entrance of a unique set of space companies. Founded and funded by celebrity technology entrepreneurs such as Elon Musk (of Tesla), Jeff Bezos (of Amazon), Richard Branson (of the

---

155 (Al-Rodhan, 2018a)
156 (Baiocchi & Welser, 2015)
157 (Davenport, 2018)
158 Baker, J. C., O'Connell, K. M., & Williamson, R. (2001). *Commercial Observation Satellites: At the Leading Edge of Global Transparency*. Santa Monica, California: RAND Corporation. Retrieved from https://www.rand.org/pubs/monograph_reports/MR1229.html

Virgin Group) and Paul Allen (of Microsoft), these new entrants have caused significant stir among incumbent space actors and hype among the public. The Ansari X Prize was a landmark event in welcoming this new type of commercial space actor. Established with the goal of triggering a commercial space movement and ending a government-dominated space era, the $100 million prize was awarded to Spaceship 1, built by a small private company called Scaled Composites and funded by Paul Allen. In recent years, these companies – specifically Musk's company SpaceX and Bezos' company Blue Origin – have gone on to achieve a number of firsts for privately funded space companies.

On the surface, the entrance of the new space companies was cause for friction with the large incumbent aerospace companies who had, to date, dominated the industry. In 2004, for example, SpaceX protested to the U.S. Government Accountability Office (GAO) that a sole-source award from NASA to Kistler Aerospace Corporation was not fair competition. NASA rescinded Kistler's $234 million contract after the GAO warned them that it would likely rule in favour of SpaceX. In October 2005 SpaceX filed suit against the United Launch Alliance LLC – a joint venture between Boeing and Lockheed Martin – alleging that the companies had used strong arm tactics to force the Pentagon to approve the merger and thus secure exclusive launch contracts. SpaceX successfully sued the Pentagon in this case, and their rocket Falcon 9 was certified to conduct launches thereafter[159].

However, a closer look at the dynamic between the emergent and incumbent space companies reveals more cooperation than conflict. Blue Origin, for example, has consistently partnered with the United Launch Alliance, most recently to provide engines for its Vulcan rocket[160]. In 2006 all of the major industry entrepreneurs gathered together in SpaceX's headquarter to form the

[159] (Davenport, 2018)
[160] Pasztor, A., & Cameron, D. (2018). Jeff Bezos' Space Startup to Supply Engines for Boeing-Lockheed Rocket Venture. *Wall Street Journal*. Retrieved from https://www.wsj.com/articles/jeff-bezoss-space-startup-to-supply-engines-for-boeing-lockheed-rocket-venture-1538035079

Personal Space Flight Federation, motivated by a common agenda to avoid overly burdensome regulations. All of the actors expressed a commitment to 'resolving the regulatory legal, political and broad strategic challenges that the personal space flight industry faces moving forward' particularly as Congress and the Federal Aviation Administration (FAA) began to consider how to regulate the emerging industry[161]. It is thus increasingly clear that firms, for the most part, recognise the strategic benefits of forming alliances when facing state actions.

3.4.2 Relationships

3.4.2.1 Firms <> State

In continuation of the trend observed in phase 2, the state's dependence on commercial space technologies became more entrenched across phase 3. By the year 2000, the number of space vehicles launched in the commercial versus military space markets reached rough parity; by 2010 the commercial market launched 50% more than the military market[162].

The defense and security establishment appear to have embraced the integration of commercial technologies and indeed have set up a number of programmes with the view to partnering with private firms. In 2003 DARPA announced the Force Application and Launch from Continental U.S. (FALCON) programme to develop a means of delivering a substantial payload from within the U.S. to anywhere on Earth within two hours. To enable this capability, they needed affordable rockets that would cost less than $5 million per launch. The Falcon rocket, developed by SpaceX, was the most viable candidate technology; hence in 2004, DARPA agreed to invest in SpaceX and thus became the company's first external investors[163].

As of 2010, NASA's strategy took a turn towards establishing collaborations with commercial space entities, signifying a strategic bet that the private sector would be able to service a number

[161] (Davenport, 2018)
[162] (Pawlikowski et al., 2012)
[163] (Davenport, 2018)

of their routine operations at a lower cost[164]. With the end of the Space Shuttle programme a significant business opportunity arose to meet the demand for low cost transportation of cargo and humans to the ISS. NASA thus awarded over $8.2 billion under various contracts for different aspects of commercial crew development and transportation[165]. This included contracts to SpaceX and Orbital ATK for the resupplying of the ISS with cargo as part of NASA's Commercial Orbital Transportation (COTS) Programme. The COTS contract became critical for ensuring SpaceX's medium-term stability as a company[166]. NASA further awarded Orbital ATK and SpaceX with commercial resupply service contracts to deliver cargo to the orbiting laboratory[167]. In 2010 and 2011, NASA also experimented with providing stimulus packages to support fledgling space companies in developing technologies for space missions[168]. A further set of contracts were awarded in 2014 and 2016 under the remit of NASA's Commercial Crew Development Program.

There is speculation that even the ISS may transition to privately funded crews and missions. Indeed, the economic case works in favour of such a model – the ISS cost over $100 billion to develop, whilst the Bigelow Expandable Activity Module (BEAM) was developed for $17.8 million by technology company Bigelow Aerospace and can serve as a facility in which astronauts can operate in space[169]. As an alternative, Axiom Space, an American start-up founded in 2015, are reportedly seeking to establish the world's first private international commercial space station by 2020[170].

---

[164] (Dawson, 2017)
[165] Siceloff, S. (2014). Commercial Crew Program - The Essentials [Text]. Retrieved September 25, 2018, from http://www.nasa.gov/content/commercial-crew-program-the-essentials
[166] NASA. (2014). *Commercial Orbital Transportation Services: A New Era in Spaceflight*. NASA. Retrieved from https://www.nasa.gov/sites/default/files/files/SP-2014-617.pdf
[167] Yembrick, J., & Byerly, J. (2008).NASA Awards Space Station Commercial Resupply Services Contracts. Retrieved September 25, 2018, from https://www.nasa.gov/offices/c3po/home/CRS-Announcement-Dec-08.html
[168] Chang, K. (2011). NASA Awards $269 Million for Private Projects. *The New York Times*. Retrieved from https://www.nytimes.com/2011/04/19/science/space/19nasa.html?mtrref=www.google.co.uk&gwh=37A572CC68E024B128FB470E058C7E76&gwt=pay; Clark, S. (2010). NASA selects winners of first commercial crew contest. *SpaceFlight Now*. Retrieved from https://spaceflightnow.com/news/n1002/02ccdev/
[169] (Al-Rodhan, 2018d)
[170] David, L. (2017). Private Space Station Coming Soon? Company Aiming for 2020 Launch. *Scientific American*. Retrieved from https://www.scientificamerican.com/article/private-space-station-coming-soon-company-aiming-for-2020-launch/

The rationale for relying on commercial technologies to deliver on government space capabilities, both civilian and military, has become increasingly clear. The government recognises that the private sector is already carrying out the leading R&D, and thus the more cost effective mechanism of acquiring these technological capabilities would be to focus on ensuring early access to these technologies via the likes of establishing the Dual-Use Science and Technology (DUST) program within the Pentagon rather than investing in internal R&D efforts[171]. To some extent, the commercial sector remains reliant on government demand for their technologies, creating a synergistic relationship. For example, Operation Iraqi Freedom generated a more than 560% increase in the use of commercial satellites for military communications[172]. The DOD remains the single largest customer for the commercial satellite industry with commercial satellites supplying approximately 80% of the U.S. military capabilities in both communications and imagery transmission.

3.4.2.2 Researchers <> State

In an echo of attempts made during the Space Race to forge bridges via research communities, similar efforts can be observed between the American and Chinese space research communities amidst the escalating hostility between the two countries. Researchers thus find themselves in passive synergy with the state as political tools for nominal cooperation.

During the Bush Administration, a Chinese delegation was allowed to attend a workshop on U.S. human space exploration initiatives during which then-NASA Administrator Sean O'Keefe met his counterpart from the China National Space Administration (CNSA) and struck an agreement to maintain regular informal communications. In 2006 CNSA's then-Vice Administrator visited the Goddard Space Flight Center, and NASA's then-Administrator Michael Griffin reciprocated by visiting China. In 2010, a similar visit was conducted by then-NASA administrator Charles

[171] (Johnson-Freese, 2007)
[172] Air Force, Assessment and Analysis Division. (2003). *Operation Iraqi Freedom – By the numbers*. Washington, D.C.: United States Air Force.

Bolden to Chinese human spaceflight facilities; Bolden visited again in August 2016 to discuss areas of space cooperation. On the international stage, U.S. and Chinese scientists and agencies have used fora such as the International Academy of Astronautics and the International Astronautical Congress to progress discussions of cooperation between their respective countries, share scientific achievements, and build bridges between the two space communities[173].

[173] (Reddy, 2017)

3.5 Analysis and discussion

The emergence of aerospace technology has been heavily shaped by the trajectory of international politics – specifically the Cold War during phase 1, and the evolving relationship between the U.S. and China in phase 3. Against this backdrop, the goals and actions of aerospace firms, researchers, and the U.S. government have been central to shaping how aerospace technology has been developed and deployed. Section 3.5.1 and Table 3.5-1 summarise how the actors evolved across the phases. Section 3.5.2 and Table 3.5-2 then summarise the evolution of the relationships that developed between them.

3.5.1 The evolution of actors

The state eclipsed the other actors in its influence on the development and deployment of aerospace technology. The Space Race during phase 1 put the goal of military leadership and national security at the forefront of the U.S. government's agenda. With the proliferation of space capabilities to other state actors, particularly China, the perceived threat to American security and the need for military strength in outer space sustained through to phase 3. Secondarily, the state was also intent on capturing the economic value of space technologies – from telecommunications and satellite technologies to more recent commercial opportunities such as space tourism.

Throughout the phases, the state's legislative capacity as a resource remained important, particularly in shaping the nature of commercial activity in the aerospace industry. However, the state's role as the funder of R&D in the aerospace industry became less relevant with time as more private funders enter the sector given the increasingly lucrative market for commercial space applications. As the industry began to distance itself from state funding, the state's lack of in-house innovation capacity drove NASA and the DOD to establish programs for integrating commercial technologies into the military technology base.

Firms consistently pursued the commercialisation of space as a goal. The innovation capacity of the private sector was boosted by the emergence of novel space companies, funded by private investors, in phase 3. Aerospace firms remained constrained by the legislative environment throughout the phases given the centrality of the industry to national interests.

Finally, researchers by and large remained nationally bound throughout the phases. As such, researchers were consistently driven by the agenda of either the state or the firm that employs them or funds their research, thus were tightly constrained by their legislative environment and their dependence on external funding.

3.5.2 The evolution of actor relationships

Across all three phases, the dynamics of the relationships between the state, firms and researchers have remained relatively stable, indicating strong synergies and limited conflicts between these actors. The majority of the conflict remained at an inter-state level – aerospace was (and is) primarily viewed by the U.S. as a political arena in which it is important for them to portray dominance and strength relative to other countries. Firms and researchers have, for the most part, fallen in line with the pursuit of this as a national goal; this is indicative of a dependence on the government for commercial viability and support, as well as a general ambivalence on their part towards the manner in which the technologies being developed are used in practice.

Between the state and firms, two elements of their relationship have been consistent across the phases. Firstly, the state has generally been supportive of the development of the commercial space sector, and thus supportive in rhetoric and in action of the development of aerospace firms. Across all three phases of the technology's development, political leaders and bureaucrats across the political spectrum affirmed the importance of a healthy private sector in ensuring military strength and technological dominance. These have been consistent national priorities for the U.S., particularly during phases 1 and 3 where there has been a specific foreign power to compete against

(the Soviet Union and China, respectively) – hence, the strength of aerospace firms has been framed as a necessary condition for achieving these national priorities.

Secondly, the state has also been consistently supportive of the integration of commercial technologies into the state's core infrastructure – specifically, the defense industrial base – in recognition of the calibre of private sector innovation compared to in-house R&D. In phase 1 this was led by the defense and security communities who, since the emergence of the Space Age, have enthusiastically partnered with firms to deliver on their programmes. In more recent times, NASA has also turned to the private sector to carry out what were considered to be central NASA activities such as crew and cargo transportation.

From the perspective of firms, the consistently cooperative stance of government has been welcome. Consequently, there has been little demonstration of push back from the private sector in the form of industrial lobbying. The one exception was the contestation that arose between firms and the state with regards to the export of commercial satellites during phase 2. This period of tension was unique in marking a significant divergence between the state's dual goals of preserving national security and supporting the commercial sector. The quiet submission of Loral and Hughes indicate that, in this case, the state won against industry interests. Critical to this relationship is also the recognition that since the emergence of the Space Age, the government has been a significant customer for aerospace firms – indeed, a number of space industries would not have been commercially viable if it were not for the demand for space technologies from the government. As such, firms have, and continue to be, dependent on the state given the nature of their business models and the market for space technologies.

Researchers played a minor role across the development of aerospace technology. During phase 1, this was in large part because their central agenda – the pursuit of science and knowledge – was aligned with how the U.S. government sought to portray their national priorities, and also provided a convenient cover for the state to pursue militaristic goals in space. Thus, the state was naturally

supportive of the scientific community, and the scientific community were content to be supported. This remained true across phases 2 and 3 despite a decrease in state R&D funding.

Table 3.5-1: Summary of evolution of actors

		State	*Firms*	*Researchers*
Goals		Economic growth = Military leadership = Risk mitigation =	Maximise profit =	Pursue research =
Resources and constraints	*R&D funding*	Resource ↓	Resource ↑	Constraint =
	Innovation capacity	Resource ↓	Resource ↑	(Resource)
	Legislative environment	Resource =	Constraint =	Constraint =
	Public concern	(Constraint)	(Constraint)	(Resource)

Notes:
↑ means that the goal / resource / constraint becomes more important as the technology matures
↓ means that the goal / resource/constraint becomes less important as the technology matures
= means that the goal / resource / constraint remains constant as the technology matures
() indicates that the goal / resource / constraint is not relevant in this case

Table 3.5-2: Summary of evolution of relationships

	Synergies	*Conflicts*
State <> *Firms*	State depends on access to commercial technologies ↑	State prevent firms from proliferating technologies ↑ (Firms face public backlash for selling technologies to the state)
State <> *Researchers*	State creates supportive R&D environment ↓	(State prevent researchers from proliferating knowledge and talent)
Firms <> *Researchers*	Firms creates supportive R&D environment ↑	(Researchers clash with firms on issues of ethics and societal consequences)

Notes:
↑ means that the synergy / conflict becomes stronger as the technology matures
↓ means that the synergy / conflict becomes weaker as the technology matures
= means that the synergy / conflict remains constant as the technology matures
() indicates that the synergy / conflict is not relevant in this case

4 Biotechnology

Biotechnology is the science and industry of harnessing cellular and biomolecular processes to develop technologies and products[1]. From the development of recombinant DNA techniques to genome engineering and synthetic biology[2], advances in biotechnology have equipped humanity with nothing short of the power to understand, manipulate and create the fundamental building blocks of biological life[3].

The biotechnology industry has generated huge economic value, enabling innovative products that have application across a wide range of sectors and provide solutions to a breadth of social and environmental problems. The challenge of transitioning towards renewable energy and materials is being addressed by the synthesis of biofuels, bioenergy crops, and bio-based chemicals. The need for more effective healthcare interventions motivate advances in gene therapy and genomic medicine. The prevention of disease drives innovation in vaccine design and genomic sequencing[4]. Looking ahead, future biotechnology

[1] Biotechnology Innovation Organisation (BIO). (n.d.). What is Biotechnology? Retrieved July 25, 2018, from https://www.bio.org/what-biotechnology; Institute of Medicine, & National Research Council. (2006). *Globalization, Biosecurity, and the Future of the Life Sciences*. Washington: National Academies Press.

[2] Biotechnology Innovation Organisation (BIO). (2018). Synthetic Biology Explained. Retrieved July 18, 2018, from https://www.bio.org/articles/synthetic-biology-explained; Cameron, D. E., Bashor, C. J., & Collins, J. J. (2014). A brief history of synthetic biology. *Nature Reviews Microbiology*, *12*(5), 381. https://doi.org/10.1038/nrmicro3239; Deplazes, A. (2009). Piecing together a puzzle. An exposition of synthetic biology. EMBO Reports, 10(5), 428–432.; European Commission. (2006). SYNBIOLOGY: An analysis of Synthetic Biology Research in Europe and North America (European Commission 6th Framework Programme NEST - New and Emerging Science and Technology).; Garfinkel, M. S., Endy, D., Epstein, G. L., & Friedman, R. M. (2007). Synthetic Genomics: Options for Governance. J. Craig Venter Institute; Center for Strategic and International Studies; MIT.; Pang, S., Lee, S. Y., & Seul, J. Y. (2017). Policy Challenges and Ethical Issues with the Breakthrough Technology: The Case of Synthetic Biology. *Science, Technology and Society*, *22*(3), 455–472. https://doi.org/10.1177/0971721817723388; Tucker, J. B., & Zilinskas, R. A. (2006). The Promises and Perils of Synthetic Biology. *The New Atlantis*. Retrieved from https://www.thenewatlantis.com/publications/the-promise-and-perils-of-synthetic-biology

[3] National Research Council. (National Research Council, 2004). *Biotechnology Research in an Age of Terrorism*. Washington, DC: The National Academies Press. https://doi.org/10.17226/10827; National Academies of Sciences, Engineering, & Medicine. (2017). *Preparing for Future Products of Biotechnology*. Washington, DC: The National Academies Press. https://doi.org/10.17226/24605; Rhodes, C. (2010). The History of the Biotechnology Revolution. In *International Governance of Biotechnology: Needs, Problems and Potential* (1st ed., pp. 8–21). London: Bloomsbury Academic. Retrieved from http://www.bloomsburycollections.com/book/international-governance-of-biotechnology-needs-problems-and-potential/ch2-the-history-of-the-biotechnology-revolution/

[4] (Garfinkel et al., 2007; Institute of Medicine & National Research Council, 2006)

products will demonstrate increased scope, scale and complexity, serving and creating new markets[5].

In parallel to the enthusiasm surrounding modern biotechnology, there is longstanding concern over the use of the very same technologies for harmful purposes[6]. Prominent scientists have raised concerns of the danger that biotechnology poses, with many pointing to the novel ease of acquisition and production of lethal microorganisms and toxins which could cause mass casualties due to biological attacks[7]. As modern biotechnology has progressed and proliferated, the spectrum of possible harm has expanded to include low-probability high-impact existential threats to humanity[8].

Biological weapons in particular have proved to be an attractive tool for resource-constrained states and non-state actors. Biological warfare refers to the intentional use of such weapons by state actors[9]; bioterrorism, on the other hand, refers to acts carried out by non-state actors

[5] (National Academies of Sciences & Medicine, 2017)

[6] For a recent overview of biotechnology as a global catastrophic risk, see the Special Issue of *Health Security* (Volume 15, Issue 4 – August 2017): https://www.liebertpub.com/toc/hs/15/4 specifically: Schoch-Spana, M., Cicero, A., Adalja, A., Gronvall, G., Kirk Sell, T., Meyer, D., … Inglesby, T. (2017). Global Catastrophic Biological Risks: Toward a Working Definition. *Health Security*, *15*(4), 323–328. https://doi.org/10.1089/hs.2017.0038

[7] Anderson, J. (1998). *Microbes and Mass Casualties: Defending America Against Bioterrorism*. The Heritage Foundation. Retrieved from /homeland-security/report/microbes-and-mass-casualties-defending-america-against-bioterrorism; Atlas, R. M. (1998). The medical threat of biological weapons. Critical Reviews in Microbiology, 24(3), 157–168.; Barnaby, W. (1997). Biological weapons: an increasing threat. Medicine, Conflict and Survival, 13(4), 301–313.; Hansen, J. E. (1999). Viruses, bacteria and toxins as biological warfare. Ugeskrift for Laeger, 161(6), 772–775.; Henderson, D. A. (1998). Bioterrorism as a public health threat. Emerging Infectious Diseases, 4(3), 488.; Henderson, D. A. (1999). The looming threat of bioterrorism. Science, 283(5406), 1279–1282.; Osterholm, M. T. (1997). The Silent Killers. *Newsweek*. Retrieved from https://www.highbeam.com/doc/1G1-19979945.html; Osterholm, M. T., & Schwartz, J. (2001). Living Terrors: What America Needs to Know to Survive the Coming Bioterrorist Catastrophe. New York: Delacorte Press.; Slater, M. S., & Trunkey, D. D. (1997). Terrorism in America: an evolving threat. Archives of Surgery, 132(10), 1059–1066.

[8] Inglesby, T. V., & Relman, D. A. (2016). How likely is it that biological agents will be used deliberately to cause widespread harm?: Policymakers and scientists need to take seriously the possibility that potential pandemic pathogens will be misused. *EMBO Reports*, *17*(2), 127–130. https://doi.org/10.15252/embr.201541674; Millett, P., & Snyder-Beattie, A. (2017). Existential Risk and Cost-Effective Biosecurity. *Health Security*, *15*(4), 373–383. https://doi.org/10.1089/hs.2017.0028

[9] (Institute of Medicine & National Research Council, 2006)

using biological weapons with the intent to cause harm[10]. The combined potency[11], low-cost[12] and military utility[13] of modern biological weapons make them particularly suitable as tools for causing harm to mass populations[14]. Fortunately, in practice there have been few recorded incidents of malicious use of biological weapons[15].

Absent an intent to cause harm, there remains the risk of harm caused by accidental release of hazardous biological materials. In the earliest days of biotechnology, the discovery of recombinant DNA techniques precipitated a discussion about accidental harm caused by biological agents and the importance of biosafety practices and policies. With the proliferation of biotechnology and the concomitant growth in the number of laboratories and researchers, the rate of accidents has increased. Indeed, hundreds of accidents and cases of poor biosafety practice have been recorded at public and private research facilities[16].

---

[10] (Institute of Medicine & National Research Council, 2006)

[11] A 1970 World Health Organisation (WHO) study found that fifty kilograms of anthrax could result in 200,000 casualties in a medium-sized city such as Boston. The U.S. Office of Technology Assessment has further estimated that an attack with less than 100 kilograms of aerosolised anthrax spores could cause up to 3 million casualties.

[12] The U.S. Office of Technology Assessment estimated that a simple fermentation plant suitable for the production of biological warfare agents would cost approximately $10 million. In 1999, the U.S. Defense Threat Reduction Agency (DTRA) built a small facility that could be used to produce biological warfare agents for $1.6 million.

[13] Biological weapons lend a number of unique advantages in warfare, including:

- Diversity of available agents and the range of their effects, providing military planners with a flexible weapon system capable of carrying out a range of missions on a broad set of targets;
- Penetrability of aerosol clouds in the face of fortifications and buildings;
- Applicability to targeting operational or theatre level warfare – e.g. attacking logistical networks, reinforcement, and command and control facilities – such as to induce operational paralysis.

[14] Koblentz, G. (2004). Pathogens as weapons: The international security implications of biological warfare. *International Security*, *28*(3), 84–122.

[15] For detailed sources for a record of biosecurity incidents since the year 1980, see:

- Ari, M. D. (2012). *CDC's Implementation of Dual-Use Research of Concern (DURC) Oversight*. Presented at the Council of Science Editors Annual Meeting, Seattle. Retrieved from http://www.resourcenter.net/images/cse/files/2012/annmtg/handouts/03_ari_3.pdf
- Berger, K., Stephan, R., Mauger, P., Venugopalan, G., & Casagrande, R. (2016). Biosecurity Risk Assessment of Acts Targeting a Laboratory. In Gryphon Scientific, *Risk and benefit Analysis of Gain of Function Research: Final Report*. Takoma Park: Gryphon Scientific. Retrieved from http://www.gryphonscientific.com/wp-content/uploads/2016/04/Risk-and-Benefit-Analysis-of-Gain-of-Function-Research-Final-Report.pdf;
- Carus, W. S. (2001). *Bioterrorism and Biocrimes: The Illicit Use of Biological Agents Since 1900*. Washington, D.C.: Center for Counterproliferation Research, National Defense University.

[16] Young, A., & Penzenstadler, N. (2015). Inside America's secretive biolabs. *USA TODAY*. Retrieved from https://www.usatoday.com/story/news/2015/05/28/biolabs-pathogens-location-incidents/26587505/

The transformative yet harmful potential of biotechnology culminates in what is perhaps its defining security challenge – the dual-use nature of biotechnology. On the one hand, breakthroughs in biotechnology enable vast improvements in healthcare, agriculture, and sustainable energy. On the other hand, there is a compelling need to contain the development of biological weapons and hazardous biological agents[17]. The U.S. defense community have cautioned that these two goals are in tension: 'Progress in biomedical science inevitably has a dark side and potentiates the development of an entirely new class of weapons of mass destruction'.[18] The 2016 Biodefense Report to the U.S. President surmised the challenge as follows[19]:

> The power of biotechnology has been growing at an exponential rate over the past several decades…While the ongoing growth of biotechnology is a great boom for society, it also holds serious potential for destructive use by both states and technically-competent individuals with access to modern laboratory facilities.

This case study analyses the politics surrounding the development and deployment of modern biotechnology in the United States. Section 4.1 describes the actors engaged throughout the technology life cycle. Then, sections 4.2 to 4.4 step through the three phases of biotechnology development, highlighting notable events and relationships. Section 4.5 offers a summative analysis.

---

[17] Atlas, R. M., & Dando, M. (2006). The Dual-Use Dilemma for the Life Sciences: Perspectives, Conundrums, and Global Solutions. *Biosecurity and Bioterrorism: Biodefense Strategy, Practice, and Science*, *4*(3), 276–286. https://doi.org/10.1089/bsp.2006.4.276; (Chyba, 2006); (Institute of Medicine & National Research Council, 2006)

[18] Block, S. M. (1999). Living nightmares: biological threats enabled by molecular biology. In S. D. Drell, A. D. Sofaer, & G. D. Wilson, *The new terror: Facing the threat of biological and chemical weapons* (pp. 39–75). Hoover Institution Press.; Directorate of Intelligence. (2003). *The Darker Bioweapons Future*. Central Intelligence Agency (CIA). Retrieved from https://fas.org/irp/cia/product/bw1103.pdf

[19] President's Council of Advisors on Science and Technology. (2016). *Biodefense Report 2016*. Washington, D.C.: Executive Office of the President. Retrieved from https://obamawhitehouse.archives.gov/sites/default/files/microsites/ostp/PCAST/pcast_biodefense_letter_report_final.pdf

4.1 The actors

The trajectory of modern biotechnology has been primarily shaped by three actors – the state, the firms, and the researchers. In the following sections, each actor is described in the context of their engagement with the development and deployment of biotechnology.

4.1.1 State

The U.S. government has three key touch points with the biotechnology industry: the regulation of biotechnology products; the establishment of biosafety and biosecurity capabilities; and the pursuit of biotechnology-enabled military capabilities.

The *regulation of biotechnology products* focuses on commercial and civilian products and applications. The U.S. government serves two distinct regulatory functions: consumer regulation – concerned with occupational safety regulations that protect consumers and users of biotechnology products; and environmental regulation – concerned with human and non-human health risks from environmental exposure to biotechnology products. The main regulatory agencies involved in delivering on these functions are the Environmental Protection Agency (EPA), the Food and Drug Administration (FDA), and the U.S. Department of Agriculture (USDA)[20]. A *Coordinated Framework for the Regulation of Biotechnology*, released in 2017 by the White House, lays out the responsibilities and interactions between the EPA, FDA and USDA as well as the major statues enforced by these agencies on the biotechnology industry[21].

The *biosecurity agenda* of the U.S. government aims to protect the state against biological warfare and terrorism. The core pillars of this agenda, as outlined in *Homeland Security*

[20] (National Academies of Sciences & Medicine, 2017)
[21] Executive Office of the President. (2017). *Modernizing the Regulatory System for Biotechnology Products: An Update to the Coordinated Framework for the Regulation of Biotechnology*. Washington, D.C.: The White House.

Presidential Directive 10, emphasize activities such as threat awareness, protection of critical infrastructure, surveillance and detection, and response planning[22]. Whilst the Department of Defense (DOD) plays a central role in executing on biosecurity activities, given the U.S. defense-only posture towards biological weapons the DOD does not take the primary leadership role. Instead, responsibility for delivering on biosecurity capabilities is dispersed among over two dozen committees which each have authority and oversight over specific activities yet lack a coherent framework within which to coordinate between themselves[23]. Among these are: the National Institutes of Health (NIH) who play a central role in funding bioterrorism and biodefense-related research[24]; the Centres for Disease Control and Proliferation (CDC) who jointly administer the Federal Select Agent Program for the restriction of shipments of dangerous biological agents[25]; and the DOD who provide core resources and expertise to both civilian and military biodefense programs[26]. Between 2001

[22] In further detail, the core pillars as outlined are as follows:
- *Threat awareness*: biological warfare related intelligence; assessments; anticipation of future threats;
- *Prevention and protection*: proactive prevention; critical infrastructure protection;
- *Surveillance and detection*: attack warning and attribution;
- *Response and recovery*: response planning; mass casualty care; risk communication; medical countermeasure development; decontamination.

[23] (Blue Ribbon Study Panel on Biodefense, 2015)

[24] The NIH saw a huge expansion in their biodefense expenditures post the September 11th and anthrax attacks, from $53 million in 2001 to $1.9 billion in 2007. This includes funding laboratories that can handle the most dangerous pathogens, and eight new regional centres of excellence for biodefense and emerging infectious disease research. See: National Research Council. (2007). *Science and Security in a Post 9/11 World: A Report Based on Regional Discussions Between the Science and Security Communities*. Washington, DC: The National Academies Press. Retrieved from https://www.nap.edu/catalog/12013/science-and-security-in-a-post-911-world-a-report

[25] The Federal Select Agent Program is jointly administered by the USDA Animal and Plant Health Inspection Service (USDA-APHIS) and the CDC. This, combined with the Department of Commerce's restrictions and the Department of Health and Human Services (DHHS) voluntary screening programs, make for the bulk of existing programs in place for restricting the shipments of biological agents.

[26] Civilian and military operators share many similar requirements for protection in biologically contaminated environments, making the DOD a natural source of resource and expertise in civilian contexts. The U.S. Northern Command has taken on a number of responsibilities for providing support to civilian authorities in executing on the likes of bio-surveillance and pandemic planning and has managed to foster civilian-military collaboration in areas of biodefense. The DOD has established doctrine for supporting civilian authorities in biodefense; see: Joint Chiefs of Staff. (2013). *Defense Support of Civil Authorities*. Washington, D.C.: U.S. Department of Defense.

and 2014 the U.S. government spent approximately $80 billion on biodefense activities[27] and are planning to spend approximately $3 billion on biodefense in the fiscal year 2018[28].

With respect to *pursuing military capabilities*, the Defense Advanced Research Project Agency (DARPA) has established 'harnessing biology as technology' as one of its main areas of focus for its strategic investments[29]. DARPA's director has emphasized this strategic focus on biotechnology, celebrating biology as 'nature's ultimate innovator' and claiming that 'any agency that hangs its hat on innovation would be foolish not to look to this master of networked complexity for inspiration and solutions.'[30] This led to the creation of a Biological Technologies Office in 2014 which has enabled a portfolio of bio-based programs across synthetic biology, neuro-technologies, and infectious disease research[31]. Of late, a substantial amount of federal funding in biotechnology research is directly attributed to the pursuit of military capabilities. DOD and DARPA account for two thirds of the $200 million invested in 2014 in synthetic biology research[32] and as of 2017 over $270 million was invested in biotechnology R&D from defense-related agencies[33]. Such R&D efforts are often a mix of biodefense and bio-capabilities research[34].

---

[27] Sell, T. K., & Watson, M. (2013). Federal Agency Biodefense Funding, FY2013-FY2014. *Biosecur Bioterror*, *11*(3), 196–216.
[28] Watson, C., Watson, M., & Kirk Sell, T. (2017). Federal Funding for Health Security in FY2018. *Health Security*, *15*(4), 351–372. https://doi.org/10.1089/hs.2017.0047
[29] Lentzos, F. (2018). How do we control dangerous biological research? *Bulletin of the Atomic Scientists*. Retrieved from https://thebulletin.org/2018/04/how-do-we-control-dangerous-biological-research/
[30] Prabhakar, A. Department of Defense (DOD) Fiscal Year 2016 Science and Technology Programs: Laying the Groundwork to Maintain Technological Superiority, § Subcommittee on Emerging Threats and Capabilities, Armed Services Committee (2015). Retrieved from https://www.darpa.mil/attachments/Prabhakar-A20150326.pdf
[31] DARPA. (n.d.). Our Research. Retrieved October 14, 2018, from https://www.darpa.mil/program/our-research/more
[32] (Lentzos, 2015b)
[33] The Office of Naval Research reported $32.9 million; the Defense Threat Reductions Agency (DTRA) reported $149.8 million; and the U.S. Army Research Lab reported approximately $88 million. See: (National Academies of Sciences & Medicine, 2017)
[34] For example, the Lawrence Livermore National Laboratory invest in high-performance computing power to advance life sciences for both biodefense efforts as well as fundamental research in genomic and proteomic arrays. The DTRA's Chemical and Biological Technologies Directorate similarly invest in new technologies that may be applied to civilian arenas as well as biodefense. See: Center for Biosecurity. (2011). *Preserving National Security: The Growing Role of the Life Sciences - Conference Report*. Washington, D.C.: Center for Biosecurity of UPMC.

4.1.2 Firms

Biotechnology firms can broadly be distinguished into two categories[35]:

- *Start-ups and small-to-medium enterprises* are companies focused on a specific application of biotechnology or specific core service lines in the commercial biotechnology sector. These companies are typically at the frontier of technological development. Their core business strategy is to develop proprietary technologies that make them an attractive acquisition opportunity for larger companies.
- *Multinationals* are large companies for which industrial biotechnology makes up a substantial proportion of their portfolio. These companies comprise the bulk of biotechnology revenues and R&D budgets in the industry. They maintain their innovative edge largely through acquisition of smaller companies, and/or licensing technologies from others.

As the biotechnology industry scaled, these two types of firms became naturally complementary. The increasing cost, scale and complexity of technological development became prohibitive for most start-ups and new entrant small-to-medium enterprises (SMEs). Smaller biotechnology firms thus turned to developing interfirm relationships with large corporations who could absorb the cost of R&D. The large corporations in turn sought to gain from the talent and novel intellectual property that tended to accompany the founding teams of smaller enterprises. International subcontracting also became more common, where larger firms would contract out the production of components, supplies and products. This was evermore the case as supply chains across a range of industries became globalized[36].

[35] Festel Capital. (2010). *Industry Structure and Business Models for Industrial Biotechnology*. Presented at the OECD Workshop on the Outlook on Industrial Biotechnology, Vienna. Retrieved from https://www.oecd.org/health/biotech/44776744.pdf

[36] (Hoyt & Brooks, 2003; Institute of Medicine & National Research Council, 2006)

Notably, both of these types of biotechnology firms are typically not very visible to the public. Smaller biotechnology companies are quick to be acquired before they build up a prominent public-facing brand. Larger multinationals are often already established multinational firms in large industries such as pharmaceuticals, agricultural technologies, biomedicine, and consumer products, which often do not brand themselves as biotechnology companies, per se, and thus garner limited public attention.

4.1.3 Researchers

The biotechnology research community draws from a large number of disciplines, including: biology, chemistry, medicine, engineering and the life sciences. Further, biotechnology researchers work for a range of employers and in a number of settings, from government agencies to universities to industry laboratories. It is thus difficult to precisely draw a boundary around what constitutes the biotechnology research community. With that said, there are three characteristics of this community that are notable – its transnational scale, its de-skilled nature, and its self-governance infrastructure.

A *transnational* research community is generally evidenced through the emergence of shared research infrastructure – whether that be standardization, open source resources, or convening events to build a shared knowledge base. Such infrastructure reduces the costs of international cooperation and introduces a sense of belonging to a research community that is not bound by national borders. For the biotechnology research community, this infrastructure emerged in earnest in the early 2000s. In 2003, the Registry of Standard Biological Parts (RSBP) was established, acting as a public repository that developed a digital catalogue and physical store of genetic parts in a standardized format[37]. The translation of these registries into a computational language, Synthetic Biology Open Language (SBOL),

[37] (iGEM, 2017)

furthered the development of common tools among synthetic biologists[38]. Similarly, the development of OpenWetWare, a public wiki originally developed at MIT, has grown to become a valuable resource for biotechnologists around the world, serving as a forum for sharing protocols and hosting laboratory websites[39].

Efforts to convene the biotechnology research community include the SyntheticBiology conferences, the first of which was held at MIT in 2004. This was widely lauded for the positive impact that it had on the then nascent field of synthetic biology. It created an identifiable community, and galvanized efforts to design and construct further transnational research infrastructure. The SyntheticBiology conferences have since been held all around the world, from Zurich to Hong Kong. In that same year, the first iGEM competition was held. The iGEM competition has since grown into a powerful international initiative that has become a defining cornerstone of the biotechnology research community, acknowledged primarily for its role in sustaining the norm of cooperation between researchers across different countries[40].

The establishment of this transnational infrastructure has in larger part contributed to the *de-skilling* of the biotechnology research community – the increasing ease by which a variety of actors with limited training can engage with biotechnology R&D. This trend has been bolstered by the falling costs of DNA sequencing, synthesis and editing[41], and the establishment of the likes of shared platforms for conducting experiments[42], incubator spaces

---

[38] SBOL. (2018). The Synthetic Biology Open Language (SBOL). Retrieved July 18, 2018, from http://sbolstandard.org/

[39] OpenWetWare. (2017). OpenWetWare. Retrieved July 18, 2018, from https://openwetware.org/wiki/Main_Page

[40] Ball, P. (2004). *Synthetic biology: starting from scratch*. Nature Publishing Group.; Ferber, D. (2004). Microbes made to order. *Science*, *303*(5655), 158.

[41] The cost of sequencing DNA dropped by seven orders of magnitude between 2002 and 2008; it has since dropped an additional order of magnitude between 2008 and 2015. See: (National Academies of Sciences & Medicine, 2017)

[42] Notable examples include: Benchling, a peer-to-peer sharing platform that provides software tools for experiment design and note-taking in molecular biology; Transcriptic and Emerald Cloud Lab, both cloud-based platforms which provide access to advanced instrumentation and automation for conducting experiments.

for biotechnology start-ups[43], and centralized bio foundries[44]. The de-skilling trend has encouraged growth of the likes of the Do-It-Yourself (DIY) Biology community, consisting of individuals and organisations who engage in biotechnology research beyond the bounds of traditional research institutions. As of 2013 the DIY Biology community was estimated to be between 3,000 and 4,000 people worldwide, with community laboratories operating across the U.S. and Europe[45].

Ever since the emergence of the field, the biotechnology research community has turned to researcher-led *self-governance* measures to manage biosafety and biosecurity risks. After the 9/11 attacks, for example, universities took it upon themselves to increase activities to educate students and faculty members about national security concerns and expended additional resources to improve the physical security of their laboratories. Researchers created peer review groups to implement new security and safety requirements related to the handling of select agents and were more responsive to requests from law enforcement and security agencies[46].

The synthetic and DIY biology communities are particularly sensitive to biosecurity and biosafety concerns and have taken an active role in pre-emptively defining and addressing governance issues. At the SyntheticBiology 1.0 and 2.0 conferences there were calls for community-derived codes of ethics and common declarations of appropriate practices in relation to the threat of bioterrorism[47]. DIY Biology labs have also actively promoted responsibility within the community[48]. Further, a number of researcher-led initiatives have

[43] QB3 and LabCentral are notable examples.
[44] Bio-foundries are centralized facilities designed to leverage software and automation to increase the number of organisms that can be engineered in parallel.
[45] (National Academies of Sciences & Medicine, 2017)
[46] (National Research Council, 2007)
[47] Frow, E. (2017). From "Experiments of Concern" to "Groups of Concern": Constructing and Containing Citizens in Synthetic Biology. *Science, Technology, & Human Values*, 0162243917735382. https://doi.org/10.1177/0162243917735382
[48] (Jefferson, Lentzos, & Marris, 2014)

emerged to promote validation and integrity of proprietary data sources used for risk assessment in biotechnology[49].

[49] Examples include:

- *Allergen Online by the University of Nebraska*: a peer-reviewed allergen list and database intended to identify proteins that may present a potential risk of allergenic cross-reactivity;
- *The International Life Sciences Institute's crop composition database*: summarising ranges in nutrient, toxicant, and anti-nutrient content of crops;
- *CIRPR Genome Analysis Tool by Iowa State University*: used for design and analysis of guide RNA to minimise off-target genome edits.

4.2 Phase 1: Emergence and promise [1953 – 1979]

The origins of modern biotechnology are often traced back to the birth of genetic engineering – or more specifically, the application of engineering principles and techniques to the field of genetics. The seminal discovery of the structure of DNA in 1953 by Watson and Crick laid the foundations for this approach[50]. Twenty years later, Cohen and Boyer performed the first successful recombinant DNA experiment, demonstrating for the first time how to manipulate genetic material to produce new biological entities[51].

A wave of fundamental breakthroughs throughout the 1970s and 1980s propelled biotechnology forward. In 1977, genetically engineered bacteria were used to synthesize a human growth protein, marking the first time a synthetic recombinant gene was used to clone a protein. The President of the National Academy of Sciences proclaimed this as a 'scientific triumph of the first order'[52]. The polymerase chain reaction (PCR) was invented in 1983; recognised as a watershed discovery in molecular biology, the PCR technique enabled the multiplying of DNA sequences and has since become an indispensable technique in medical and biochemical research. Restriction enzymes were also discovered in this period, underpinning a technique for cutting DNA into pieces that has become fundamental in modern genetic research[53].

Phase 1 also marked two significant events in the governance of modern biotechnology: the establishment of a strong international norm against the use of biological weapons, and the institution of a researcher-led self-governance regime for the management of risks from recombinant DNA technology. Both of these events are described in section 4.2.1. Critical

[50] Watson, J. D., & Crick, F. H. (1953). Molecular structure of nucleic acids. *Nature*, *171*(4356), 737–738.
[51] Cohen, S. N., Chang, A. C., Boyer, H. W., & Helling, R. B. (1973). Construction of biologically functional bacterial plasmids in vitro. Proceedings of the National Academy of Sciences, 70(11), 3240–3244.
[52] Itakura, K., Hirose, T., Crea, R., Riggs, A. D., Heyneker, H. L., Bolivar, F., & Boyer, H. W. (1977). Expression in Escherichia coli of a chemically synthesized gene for the hormone somatostatin. Science, 198(4321), 1056–1063.
[53] (Cameron et al., 2014)

relationships that shape the dynamics of phase 1 are then described in section 4.2.2 between researchers and the state, and researchers and biotechnology firms.

4.2.1 Notable events

4.2.1.1 The Biological Weapons Convention

The year 1969 marked an abrupt and remarkable change in the role of the U.S. in proliferating biological weapons. After nearly thirty years of pursuing the development, testing and production of biological weapons, President Nixon announced on November 25, 1969 that the U.S. would cease production of and destroy offensive biological weapon stockpiles, pledging that the U.S. would restrict their biological programmes to 'defensive purposes, strictly defined'. A string of similar renunciations followed from countries such as the Netherlands[54], Canada[55], the UK[56] and Sweden[57].

Alongside a renunciation of offensive biological weapons, Nixon also announced official U.S. support for a multilateral treaty banning the development, production and possession of biological weapons. This added to the already gathering momentum on the international stage to move towards a global norm against the use of chemical and biological weapons[58]. The United Kingdom first tabled a draft of such a convention on July 10, 1969; a parallel draft led by a coalition of countries, including the USSR, was submitted to the UN General

[54] On March 17, 1970, in a statement to the Conference of the Committee on Disarmament (CCD) Mr Eschauzier of the Netherlands affirmed that when they ratified the Geneva Protocol in 1930 this was understood as a unilateral renunciation of the use of bacteriological or biological weapons.
[55] On March 24, 1970, in a statement to the CCD, Canada stated that it does not possess now and has no intention in the future to develop, produce, acquire, stockpile or use biological or toxin weapons.
[56] On April 7, 1970, in a statement to the CCD, Lord Chalfont as then-UK Disarmament Minister restated the UK's position: 'We have never had any biological weapons, we have none now, and we have no intention of acquiring any.'
[57] On April 29, 1970, Swedish Ambassador Alva Myrdal informs the CCD on behalf of the Swedish Parliament: 'Sweden does not possess, nor does it intend to manufacture any biological or chemical means of warfare.'
[58] For a more detailed account of the timeline of events that led up to the establishment of the Biological Weapons Convention, see: Spelling, A., McLeish, C., & Balmer, B. (2015). *Where did the Biological Weapons Convention come from? Indicative timeline and key events, 1925 - 75*. University of Sussex Science Policy Research Unit (SPRU). Retrieved from https://www.ucl.ac.uk/sts/sites/sts/files/wherediddbwccomefrom.pdf

Assembly on September 19, 1969[59]. These proposals converged into a revised draft *Convention on the Prohibition of the Development, Production, and Stockpiling of Bacteriological (Biological) and Toxin Weapons and on their Destruction*, which was submitted to the UN General Assembly on September 28, 1971. The convention – which came to be known as the *Biological Weapons Convention* (BWC) – officially opened for signature on April 10, 1972. Within one year, 115 countries had signed the convention and began domestic ratification procedures. With the instruments of ratification signed, exchanged and deposited at ceremonies in London, Washington D.C. and Moscow, the BWC entered into force on March 26, 1975. This pivotal event in history marked the first major attempt by nations around the world to outlaw an entire class of weapons and establish a strong international norm for full disarmament of biological weapons[60].

4.2.1.2 The Asilomar Conference on Recombinant DNA

The seminal event that established this model of researcher-led self-governance was the Asilomar Conference on Recombinant DNA of 1975. The advent of recombinant DNA (rDNA) technology in the early 1970s had raised both enthusiasm for its prospects as well as concern at for its risks among the research community. At the Gordan Research Conference on Nucleic Acids in July 1973, conference participants decided to write a letter to the National Academy of Sciences requesting them to commission a study on the possible risks of rDNA technology. A subsequent letter in 1974 established a voluntary moratorium on rDNA research given its prospective hazards.

[59] The countries included: Bulgaria, Byelorussian SSR, Czechoslovakia, Hungary, Mongolia, Poland, Romania, Ukrainian SSR and the USSR.

[60] For a more detailed recount of the history of the BWC and its significance, see: Guillemin, J., Meselson, M., Robinson, J. P., & Sims, N. (2015). Witness Seminar: Origins of the Biological Weapons Convention. In *Biological Threats in the 21st Century* (Vols. 1–0, pp. 357–384). IMPERIAL COLLEGE PRESS. https://doi.org/10.1142/9781783269488_0021

This culminated in the convening of the Asilomar Conference on Recombinant DNA in 1975. The focus of the conference was to develop physical and biological containment guidelines for 'experiments of concern' involving recombinant DNA. The stated aims were the protection of researchers and public health; biosecurity issues were not on the agenda, nor were broader debates surrounding the ethics of rDNA technology. The established guidelines at the conclusion of the conference triggered a lifting of the moratorium on rDNA research.

To this day, the overarching structure established at the Asilomar Conference for the governance of recombinant DNA research remains intact. The National Institutes of Health (NIH) published and routinely revises their *Guidelines for Research Involving Recombinant DNA molecules* which was recently updated in 2013 in light of advances in synthetic biology. The synthetic biology research community have also based a lot of their proposals and initiatives for community self-governance mechanisms on the Asilomar model[61].

4.2.2 Relationships

4.2.2.1 Researchers <> State

From the earliest days of modern biotechnology, a dominant attitude among scientists engaged in the life sciences was a general distrust of the government's capacity to enact sensible policies, and a fear that poor policy would impose barriers to the pursuit of science and innovation[62]. In order to avoid the enactment of poor policy, the biotechnology research community has tended to push for self-governance measures that are designed, enacted and enforced by researchers themselves.

[61] Frow, E. (2017). From "Experiments of Concern" to "Groups of Concern": Constructing and Containing Citizens in Synthetic Biology. *Science, Technology, & Human Values*, 0162243917735382. https://doi.org/10.1177/0162243917735382

[62] (Harris, 2016; Institute of Medicine & National Research Council, 2006; National Research Council, 2009a)

The Asilomar Conference was a case in point of this tension between researchers and the state. Indeed, a sense of urgency was reported to have pervaded the 1975 meeting, in part because researchers were impatient to put the new technology to work yet understood that without addressing issues of safety there remained the danger of public or government retaliation. The researcher community hoped that the guidelines would persuade Congress that legislative restrictions were not needed. Despite their efforts, as the research progressed various levels of government became increasingly involved in attempts to regulate it. In 1976 the NIH released a set of guidelines which applied to NIH-funded rDNA research. In 1977 the City Council Ordinance of Cambridge proclaimed that all rDNA experiments carried out under their jurisdiction must adhere to the NIH guidelines, marking the first piece of legislation passed in the U.S. regulating rDNA research. In 1978, sixteen separate bills were introduced in Congress related to the regulation of rDNA research; none of them passed, in part due to lobbying by researchers. As part of this lobbying effort, researchers retracted statements about the risks of rDNA research, claiming that they had overstated them. Serendipitously for the scientific community, this period coincided with a broader era of deregulation in the U.S. during the 1980s, as well as the promotion of the biotechnology industry as an economic sector of national importance, quashing arguments for further regulation[63].

Nevertheless, the state also remained a supportive funder of early-stage biotechnology R&D. As the field began to gain traction and the fruits of the earliest breakthroughs became evident, the National Sciences Foundation (NSF) escalated the availability of funding for fundamental research fields related to biotechnology – namely, the life sciences, molecular biology, and

[63] Barinaga, M. (2000). Asilomar Revisited: Lessons for Today? *Science*, *287*(5458), 1584–1585.; Weiner, C. (1999). Is self-regulation enough today?: Evaluating the recombinant DNA controversy. *Health Matrix (Cleveland, Ohio : 1991)*, *9*(2), 289.; Weiner, C. (2001). Drawing the line in genetic engineering: self-regulation and public participation. *Perspectives in Biology and Medicine*, *44*(2), 208–220.

genetics[64]. The recent rise of synthetic biology as a subfield of biotechnology demonstrates how fundamental research benefitted from government funding[65]. Between 2008 and 2014, the cumulative amount invested in synthetic biology by U.S. federal agencies totalled to $820 million[66]. The creation of Synberc in 2006, funded by NSF's Engineering Research Centre, further marked a significant government investment in a multi-institutional research centre focused on foundational research and field building through training and education efforts[67].

4.2.2.2 Researchers <> Firms

While it would take some time for the biotechnology industry to get off the ground, the seeds of a burgeoning private sector emerged during this phase. Cetus Corporation was founded in 1971, establishing itself as one of the first biotechnology companies. A mere ten years later, Cetus raised $108 million in a record initial public offering (IPO) at the time. It was closely followed by the founding of Genentech in 1976 and Applied Molecular Genetics Inc. (AMGen) in 1980, both of which would grow to become some of the world's largest biotechnology companies.

The emergence of these early biotechnology companies was precipitated by researchers themselves. Cetus Corporation was founded by a biochemist, physician and physicist; Genentech was pioneered by Herbert Boyer; and AMGen's first CEO was a chemist and biologist. Surges in commercial activity were also coupled with research progress. Shortly after the milestone gene splicing breakthrough by Cohen and Boyer in 1973, the first wave of biotechnology start-ups began to emerge, closely followed by venture capital funding.

---

[64] Wright, S., & Wallace, D. A. (2000). Varieties of Secrets and Secret Varieties: The Case of Biotechnology. *Politics and the Life Sciences*, *19*(1), 45–57.
[65] (Pang et al., 2017)
[66] The Synthetic Biology Project. (2015). *U.S. Trends in Synthetic Biology Research Funding*. Woodrow Wilson International Center for Scholars. Retrieved from https://www.wilsoncenter.org/publication/us-trends-synthetic-biology-research-funding
[67] Si, T., & Zhao, H. (2016). A brief overview of synthetic biology research programs and roadmap studies in the United States. *Synthetic Biology in China, UK and US*, *1*(4), 258–264. https://doi.org/10.1016/j.synbio.2016.08.003

Similarly, the 1977 milestone of using genetically engineered bacteria to synthesize protein triggered a significant increase in the amount of private capital flowing into funding genetic engineering research; by 1980 equity investments in small genetic engineering firms had reached $600 million[68]. The synergistic relationship thus forming between researchers and early-stage firms in this phase bodes of the forthcoming shift in biotechnology toward private industry, and away from public funding.

[68] (Cameron et al., 2014)

4.3 Phase 2: Commercialisation and proliferation [1980 - 2000]

As the prospects of commercial exploitation of biotechnology became apparent, a surge of private sector activity in the early 1980s signalled the beginning of phase 2 – *commercialisation and proliferation*. This phase is characterised by the rapid commercialisation of research into technologies that found widespread application across the economy. The technologies became more mature and supporting technologies that led to their production became more cost-effective and standardized. The productivity of commercially available DNA synthesis services, for example, have been estimated to be increasing faster than Moore's law since 1985. The shortest time required to determine protein structures also decreased dramatically from 1 year in 1980 to 0.015 years in 2000[69].

Propelling this growth were biotechnology firms – namely, early stage start-ups who partnered with or were acquired by large pharmaceutical and agriculture companies. The number of firms engaged in biotechnology research rose from 1,863 in 1982 to 50,677 in 1993[70]. In the U.S. alone, the biotechnology industry had reached over 1,274 biotechnology firms and revenues of $31.5 million in aggregate by the year 1997[71]. Globally, the biotechnology industry more than doubled in size of revenue from $8 billion in 1993 to $20 billion in 1999[72]. With increasing private sector activity, the locus of influence in biotechnology shifted from the public to the private. Prior to the 1980s the federal government outspent the private sector by a factor of 2 in basic research; post

[69] (Robert Carlson, 2003)
[70] Banerjee, P., Gupta, B. M., & Garg, K. C. (2000). Patent Statistics as Indicators of Competition an Analysis of Patenting in Biotechnology. *Scientometrics*, *47*(1), 95–116. https://doi.org/10.1023/A:1005669810018
[71] Giesecke, S. (2000). The contrasting roles of government in the development of biotechnology industry in the US and Germany. *Research Policy*, *29*(2), 205–223. https://doi.org/10.1016/S0048-7333(99)00061-X
[72] Ernst & Young Economics Consulting and Quantitative Analysis. (2000). The Economic Contributions of the Biotechnology Industry. *Biotechnology Industry Organization*. Retrieved from https://www.bio.org/articles/economic-contributions-biotechnology-industry

the 1980s this transitioned into private sector funders outspending the government by a factor of three[73].

Collaboration between firms also increased, pushing the biotechnology industry towards internationalisation. The number of cooperation agreements between biotechnology firms grew from near zero in 1970 to almost 700 by 1989. Whilst the majority of these agreements were between U.S. based firms (34%), a number of firm-firm agreements were struck up between U.S. and Japanese companies (10%) and U.S. and Western European companies (19%). This proved to be an effective mechanism for scaling by allowing for knowledge, capital, and production facilities to be more efficiently distributed beyond the boundaries of individual biotechnology firm [74]. These global firms also began to form their own institutions at an international scale. In 1993, two smaller trade associations merged to form the Biotechnology Industry Organisation (BIO) which exists to this day as the world's largest advocacy group for the biotechnology industry. This foreshadows the increasing political influence of biotechnology firms in the next phase as the industry gains coherence and organising power of its own.

Two notable events occur in phase 2 – the *Diamond v. Chakrabarty* case, and the establishment of the Human Genome Project – which are described in turn in section 4.3.1. Each event has distinct and important flow-on effects vis a vis the synergies and conflicts that emerge between the researchers, the state, and firms, which are described further in section 4.3.2.

[73] Mervis, J. (2017). Data check: U.S. government share of basic research funding falls below 50%. *Science*. Retrieved from http://www.sciencemag.org/news/2017/03/data-check-us-government-share-basic-research-funding-falls-below-50

[74] Powell, W. W., Koput, K. W., & Smith-Doerr, L. (1996). Interorganizational Collaboration and the Locus of Innovation: Networks of Learning in Biotechnology. *Administrative Science Quarterly*, *41*(1), 116–145.

4.3.1 Notable events

4.3.1.1 Diamond v. Chakrabarty

A landmark Supreme Court case occurred in 1980 – *Diamond v. Chakrabarty* – in which it was ruled that a patent could be obtained for a laboratory-created genetically engineered bacterium. Genetic engineer Ananda Mohan Chakrabarty had filed for a patent for a genetically modified bacterium that could break down multiple components of crude oil; his application was initially rejected on the premise that living organisms were generally not considered patentable. The case was brought to litigation and escalated to the Supreme Court which, on June 16, 1980, ruled in favour of Chakrabarty. This ruling was pivotal for the biotechnology industry, establishing a precedent for companies and investors that the U.S. patent system would enable proprietary protection of modified naturally occurring subject matter. This encouraged industry-funded research into a range of application areas such as diagnostics, medical therapies and agricultural technologies[75].

The *Diamond v. Chakrabarty* case was closely followed by a number of rulings in favour of increasing the patentability of biotechnology innovations[76]. This, combined with the passing of the *Bayh-Dole Act* in 1980 providing universities the right to file for patents from federally funded research, precipitated an upswing in biotechnology patenting activity. Between 1982 and 1993 the total number of patents granted in biotechnology per year went from 1,831 to 4,864. There was a strong increase in the number of patents filed in the 1990s which has been attributed to universities being more inclined to commercialise their intellectual property[77]. The rate of growth of DNA-related

[75] Battaglia, G. (2016). Rapid Advances in Biotechnology Bring Questions about Patentability. *Bioradiations*. Retrieved from http://www.bioradiations.com/rapid-advances-in-biotechnology-bring-questions-about-patentability/
[76] Rao, R. R. (2012). *Patenting in Biotechnology - An Overview*. SSRN. Retrieved from http://dx.doi.org/10.2139/ssrn.1999541
[77] Friedrichs, S. (2018). *Report on statistics and indicators of biotechnology and nanotechnology* (OECD Science, Technology and Industry Working Papers). Paris: OECD. Retrieved from https://www.oecd-ilibrary.org/industry-and-services/report-on-statistics-and-indicators-of-biotechnology-and-nanotechnology_3c70afa7-en

patents in the U.S. is estimated to have been roughly 50% per annum during the 1990s[78]; the annual number of biotechnology patents peaked in 1998 with the issuing of 5,977 patents[79].

The increase in biotechnology patenting activity during this phase did not come without its challenges. The evolving landscape of commercial biotechnology interests resulted in inconsistent and under-specified practices applied by the U.S. Patent and Trademark Office. This was particularly the case when it came to patents that were broad in scope. Between 1982 and 1994, U.S. courts invalidated approximately one third of challenged patents, creating uncertainty for companies and inventors as to the value of the patents that they held[80].

4.3.1.2 The Human Genome Project

The Human Genome Project (HGP) was an international collaboration with a grand ambition: to determine, store, and make publicly available the entire human genome[81]. The seed of the idea came from Robert L. Sinsheimer of the University of California, Santa Cruz, who in 1985 proposed the possibility of a collaborative effort to sequence the human genome. This was echoed by Nobel laureate Renato Dulbecco in 1986. As the idea began to gain traction, a series of reports from the U.S. Department of Energy (DOE), the Congressional Office for Technology Assessment, and the National Research Council were published all recommending such a project. Soon thereafter, the NIH and the DOE signed a memorandum of understanding committing to 'provide for the formal coordination' of their activities 'to map and sequence the human genome'. In 1988, Congress provided funds to both the DOE and NIH to follow through on this commitment,

[78] Caulfield, T., Cook-Deegan, R. M., Kieff, F. S., & Walsh, J. P. (2006). Evidence and anecdotes: an analysis of human gene patenting controversies. *Nature Biotechnology*, *24*, 1091–1094. https://doi.org/10.1038/nbt0906-1091
[79] Jamison, M. (2015). Patent Harmonization in Biotechnology: Towards International Reconciliation of the Gene Patent Debate. *Chicago Journal of International Law*, *15*(2), 688–720.
[80] Gold, E. R. (2000). Finding common cause in the patent debate. *Nature Biotechnology*, *18*, 1217.
[81] For a detailed history of the Human Genome Project, see: Fridovich-Keil, J. L. (n.d.). Human Genome Project | History, Timeline, & Facts. Retrieved November 9, 2018, from https://www.britannica.com/event/Human-Genome-Project

formally launching the HGP[82]. The project progressed from a pilot to a full-scale systematic sequencing effort in 1999.

At around the same time, well-known biotechnologist Craig Venter and the DNA sequencing instrument manufacturer Applied Biosystems Inc. announced a joint venture to sequence the human genome using a different approach to that of the HGP – a whole-genome shotgun approach. The data would be held by the company Celera Inc. and released initially only to paying subscribers; patents would be sought for genes of interest. The emergence of a competing private project raised strong criticism from the scientific community concerned about the privatization of important genetic information.

Nevertheless, by June 26, 2000 both the international HGP and the private effort jointly announced that they had each succeeded at producing an initial draft of the human genome sequence. The HGP published a full and significantly more accurate human genome sequence in 2004; all of the data was deposited in a publicly available database that was available over the internet for free to any user.

The HGP marked a significant milestone in the establishment of open-source research databases to support biotechnology research worldwide. In 1996, the international group of scientists involved in the HGP unanimously passed the *Principles of International Strategy Meeting on Human Genome Sequencing* (commonly referred to as the Bermuda Rules), which stated the following[83]:

> All human genomic DNA sequence information, generated by centres funded for large-scale human sequencing, should be freely available in the public domain in order to encourage research and development and to maximise its benefit to society.

[82] National Academy of Sciences. (2005). *Reaping the Benefits of Genomic and Proteomic Research: Intellectual Property Rights, Innovation, and Public Health*. Washington, D.C.: National Academies Press.
[83] (National Academy of Sciences, 2005)

The Bermuda Rules have continued to underpin a principle of data sharing and release in the field of genetic science. This has critically enabled the development of shared infrastructure among the transnational research community to fuel more efficient and synchronous research efforts. For example, GenBank was established as a nucleic acid sequence database at the Los Alamos National Laboratory, funded by the National Institute of General Medical Sciences. In 1988 the NIH took over the management of GenBank; today GenBank belongs to an international collaboration of sequence databases which also includes the European Molecular Biological Laboratory and the DNA Data Bank of Japan. The Universal Protein Resource (UNIPROT) is another international consortium, established in 2002, which provides freely accessible protein sequence and functional information.

4.3.2 Relationships

4.3.2.1 Firms <> State

As firm activity took off in the biotechnology industry, the state adopted a supportive stance in encouraging the commercialisation of biotechnology research and accelerating the development of biotechnology products to market. Their main mechanism for doing so was in enabling the patenting of biotechnology research such as to incentivise researchers to pursue commercial applications via licensing to firms or starting up their own companies[84].

For example, the *Act to Promote United States Technological Innovation for the Achievement of National Economic, Environmental, and Social Goals, and for other purposes* of 1980, better known as the Stevenson-Wydler Technology Innovation Act, marked the first major U.S. technology transfer law requiring federal laboratories to actively participate in and budget for technology transfer activities. This enabled the NIH and other federal agencies to enter into licensing agreements with commercial entities, therein promoting the development of commercial technologies based on government-

[84] (National Academy of Sciences, 2005)

funded science. The *Patent and Trademark Law Amendments Act* of 1980 proceeded to give universities and small businesses the right to claim intellectual property protection for discoveries that resulted from federally-funded research, incentivising the commercialisation of biotechnology research.

4.3.2.2 Researchers <> Firms

The increase in patenting sat within a broader trend of biotechnology research becoming increasingly privatized. This became both a source of synergy and conflict between researchers and firms.

By the late 1970s, it was clear that the necessary R&D capabilities to fuel the commercialization of biotechnology were housed in universities and government-funded laboratories. A critical relationship that began to emerge was thus between research institutions and multinational companies, venture capitalists, and entrepreneurs. Many of the founders of early genetic engineering companies came directly from academic institutions and maintained university appointments as they pursued their entrepreneurial activities[85]. A study covering the years 1985 to 1988 found that the percentage of faculty members who held industry affiliations in the field of biotechnology was higher than the average university department, peaking at 31% for MIT's department of biology[86]. A 1994 survey found that 90% of the 210 surveyed life sciences companies had a relationship with an academic institution, with over 50% of these relationships resulting in 'patents, products and sales' as a direct result of the relationship[87].

During the 1980s, several significant university-industry relationships had taken shape, including between the Massachusetts General Hospital and Hoechst (a German multinational chemical

[85] Kenney, M. (1986). Biotechnology : the university-industrial complex. New Haven: Yale University Press.
[86] Krimsky, S., Ennis, J. G., & Weissman, R. (1991). Academic-Corporate Ties in Biotechnology: A Quantitative Study. *Science, Technology, & Human Values*, *16*(3), 275–287.
[87] Blumenthal, D., Causino, N., Campbell, E., & Louis, K. S. (1996). Relationships between Academic Institutions and Industry in the Life Sciences — An Industry Survey. *New England Journal of Medicine*, *334*(6), 368–374. https://doi.org/10.1056/NEJM199602083340606

company), and a contract between Washington University and Monsanto[88]. Relationships between research institutions and firms were seen as mutually beneficial. Universities were increasingly worried that public funding would be more difficult to come by and thus were eager to receive private capital. In turn, funders and funding corporations needed to obtain access to high calibre research talent and leading research to maintain their competitive edge. Between 1981 to 1982, transnational firms had invested approximately $250 million in biological research being conducted in universities. The importance of publicly funded research institutions was thus widely acknowledged as being critical to launching the biotechnology industry and sustaining its growth since the early 1980s[89].

However, the growing collaborations between academia and the biotechnology industry became a cause of concern for a segment of the research community. Their concerns centred around the impact that industry relationships would have on the academic environment, principally in relation to hampering the free exchange of information, delaying or impeding publication, and dampening interdepartmental collaborations[90]. These concerns were not unfounded. A study conducted in the 1980s surveyed university-industry research relationships in biotechnology. Of the biotechnology faculty who did not receive industry support, 68% felt that university-industry linkages were undermining the ethos of intellectual exchange and cooperation. Among faculty who did receive industry support a substantial 44% agreed with this sentiment[91].

---

[88] Ruttan, V. W.(2001). *The Role of the Public Sector in Technology Development: Generalizations from General Purpose Technologies* (Science, Technology, and Innovation Discussion Paper No. 11). Cambridge, MA: Harvard University Center for International Development. Retrieved from http://ageconsearch.umn.edu/record/13563/files/p01-11.pdf

[89] Additional studies that validate this include: Audretsch, D. B., & Stephan, P. E. (1996). Company-Scientist Locational Links: The Case of Biotechnology. *The American Economic Review*, *86*(3), 641–652.; McMillan, G. S., Narin, F., & Deeds, D. L. (2000). An analysis of the critical role of public science in innovation: the case of biotechnology. *Research Policy*, *29*(1), 1–8. https://doi.org/10.1016/S0048-7333(99)00030-X; Narin, F., Hamilton, K. S., & Olivastro, D. (1997). The increasing linkage between U.S. technology and public science. *Research Policy*, *26*(3), 317–330. https://doi.org/10.1016/S0048-7333(97)00013-9

[90] (National Academy of Sciences, 2005)

[91] Blumenthal, D., Campbell, E. G., Causino, N., & Louis, K. S. (1996). Participation of Life-Science Faculty in Research Relationships with Industry. *New England Journal of Medicine*, *335*(23), 1734–1739. https://doi.org/10.1056/NEJM199612053352305

The increase in patenting activity became a particular point of contention between the academic research community and firms. Researchers feared that the proliferation of patents would increase the cost of doing research for the public good. In the context of the Human Genome Project, for example, the launch of a privately funded effort in parallel to the public initiative attracted strong criticism given the private venture's stated intention of patenting genes of interest and charging subscribers for access to the data[92]. The late 1980s also featured the EST debate. The EST is a small region in the active part of a gene for which genomics companies and universities had begun to file patents. This sparked debate in the scientific community, many of whom believed that ESTs should not be patentable given their importance to the progression of public health research. Arthur Klug and Bruce Alberts, then-presidents of the Royal Society of London and the National Academy of Sciences, released a statement in 2000 criticising EST patenting practice as one that 'did not serve society well', calling for 'the human genome itself…[to] be freely available to all humankind'.[93]

Researchers also expressed concerns on the impact that the privatization of biotechnology research would have on the growth of the research knowledge base, critical for propelling further advances in the field. A study conducted in the 1980s surveyed university-industry research relationships in biotechnology and found that practices of secrecy had increased in universities[94]. Another study conducted in the 1990s found that 56% of the biotechnology companies surveyed reported that in practice the university research that they supported resulted in information that was kept confidential in order to protect its proprietary value, rather than being filed as public patents[95].

[92] The private initiative was led by Craig Venter in collaboration with DNA sequencing instrument manufacturer Applied Biosystems Inc. The data was to be held by company Celera Inc.
[93] (National Academy of Sciences, 2005)
[94] (Blumenthal, Campbell, et al., 1996)
[95] (National Academy of Sciences, 2005)

4.4 Phase 3: Consolidation and contestation [2001 – present]

In the early 2000s, biotechnology continued to see productive rates of growth. Between 2000 and 2007, revenues in the biotechnology industry added more than $100 billion to the U.S. economy[96]. Aggregate revenues continued to grow at annual rates of more than 10%; between 2007 and 2012, the growth in biotechnology revenue was the equivalent of over 5% of annual U.S. GDP growth every year[97]. In recent years, however, this growth has begun to show signs of slowing. The market capitalisation for the biotechnology sector in the U.S. fell from $891.2 billion in 2015 to $698.6 billion in 2016, and the number of IPOs by biotechnology firms in the U.S. peaked in 2006 and has since been dropping year on year. The amount of capital raised by both private and public biotechnology firms decreased between 2015 and 2016, and the number of public biotechnology firms has stagnated just above 440[98].

Simultaneously, the proliferation of capabilities to new state and non-state actors raised concerns of a correlated increase in the threat from biological warfare and terrorism. In a recent report to the BWC, the academic community warned that scientific advances 'could facilitate almost every step of a biological weapons programme'[99]. Particularly with the lowering barriers to entry and the rise of synthetic biology, academics and state-leaders alike have warned that it has become far easier for malicious actors to exploit advances in biotechnology[100].

---

[96] Carlson, R. (2008). Tracking the spread of biological technologies. *Bulletin of the Atomic Scientists*. Retrieved from https://thebulletin.org/2008/11/tracking-the-spread-of-biological-technologies/; Carlson, R. (2009). The New Biofactories. *McKinsey Quarterly*. Retrieved from http://www.synthesis.cc/the-new-biofactories/

[97] Carlson, R. (2016). Estimating the biotech sector's contribution to the US economy. *Nature Biotechnology*, *34*, 247.

[98] Ernst & Young. (2017). *Biotechnology Report 2017: Beyond borders - Staying the course*. Ernst & Young. Retrieved from https://www.ey.com/Publication/vwLUAssets/ey-biotechnology-report-2017-beyond-borders-staying-the-course/$FILE/ey-biotechnology-report-2017-beyond-borders-staying-the-course.pdf

[99] InterAcademy Partnership (IAP) Biosecurity Working Group. (2015). *The Biological and Toxin Weapons Convention: Implications of advances in science and technology*. The Royal Society. Retrieved from https://royalsociety.org/~/media/policy/projects/biological-toxin-weapons-convention/bwc-trends-booklet.pdf

[100] This is a point of debate within the synthetic biology community. For example, some claim that carrying out synthetic biology is not as easy as some would believe and that even experienced practitioners continue to face barriers. Fears that the DIY Biology community offers easy access for terrorists to tools have also been challenged by those who point out that the DIY Biology community have been active in promoting stringent safety and security rules and have partnered with the likes of law enforcement agencies to promote responsibility and oversight

In response, the defense and national security communities have called for a broader view of the biotechnology security threat which recognises that biotechnology has become irreversibly international, and as such information and capabilities are increasingly shared across national borders[101]. The DOD, and specifically DARPA, also appear to be reinvigorating investments in biodefense capabilities. In March 2014 then-DARPA Director Arati Prabhakar announced the Living Foundries project – a new DARPA programme aimed at providing 'game-changing manufacturing paradigms for the DOD' through developing and applying an 'engineering framework to biology'[102]. Approximately $90 million has been allocated to the project thus far[103]. More recently, the Biological Technologies Office of DARPA launched the Pre-emptive Expression of Protective Alleles and Response Elements (PREPARE) Program in 2018. Its stated objectives are to develop technological capabilities that would protect war-fighters, first responders, and civilian populations from biological threats[104].

The 2001 terrorist attacks (section 4.4.1.1) and a series of high-profile dual-use experiments (section 4.4.1.2) are pivotal moments which elevate biosecurity concerns in the U.S. Separately, the gene patent debate (section 4.4.1.3) introduces a new set of debates and conflicts in the biotechnology industry. Each event has distinct flow-on effects vis a vis the synergies and conflicts that emerge between the researchers, the state, and firms, which are described in section 4.4.2.

---

in the community. See: Jefferson, C., Lentzos, F., & Marris, C. (2014). Synthetic biology and biosecurity: challenging the "myths." *Front Public Health*, *2*. https://doi.org/10.3389/fpubh.2014.00115

[101] (National Research Council, 2007)

[102] Prabhakar, A. Statement - Department of Defense (DOD) Fiscal Year 2015 Science and Technology Programs: Pursuing Technological Superiority in a Changing Security Environment, § US Armed Services Committee Subcommittee on Intelligence, Emerging Threats & Capabilities (2014).

[103] Lentzos, F. (2014). The Performativity of Constructed Uncertainty: Military Money and Secrecy in Biology. *Science as Culture*, *23*(4), 585–589. https://doi.org/10.1080/09505431.2014.942263

[104] Specifically, the program intends to 'identify the specific gene targets that can confer protection, develop in vivo technologies for programmable modulation of those gene targets, and formulate cell- or tissue-specific delivery mechanisms to direct programmable gene modulators to the appropriate places in the body.'

4.4.1 Notable events

4.4.1.1 The aftermath of the September 11th and Amerithrax attacks

Perhaps the most notorious bioterrorist attack in history occurred in 2001, a mere week after the September 11 attacks ('9/11'). Known as Amerithrax from its Federal Bureau of Investigation (FBI) case name, the attack consisted of letters containing anthrax spores mailed to several news media offices and two U.S. senators. Five people were killed, and seventeen others were injured. By 2008, the sole culprit of the crime had been identified as Bruce Ivins, a scientist who had worked at the government's biodefense labs at Fort Detrick[105]. This was a defining moment for the development of biosecurity regulation in the U.S., triggering a rapid and sustained response from the U.S. government in the subsequent decades[106].

Immediately following the attacks, bioterrorism became a central focus for the Bush Administration. Two significant pieces of legislation were passed to this effect – the *United and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001* ('PATRIOT Act') and the *Public Health Security and Bioterrorism Prepared Act of 2002* ('Bioterrorism Preparedness Act'). Both acts implemented the Select Agent Program which has become a cornerstone in biosecurity regulation in the U.S. focused on the handling of pathogens and toxins of concern[107]. The PATRIOT Act put in place restrictions on the types of individuals who would be allowed to be in possession of or transport select biological agents or toxins; the Bioterrorism Preparedness Act added additional registration requirements for researchers and institutions working with these select agents and toxins[108].

---

[105] Harris, E. D. (2016). *Governance of Dual-Use Technologies: Theory and Practice*. Cambridge, MA: American Academy of Arts and Sciences.

[106] (Hoyt & Brooks, 2003; Institute of Medicine & National Research Council, 2006; National Research Council, 2007)

[107] The original Select Agent Program was created in 1996 under the Antiterrorism and Effective Death Penalty Act. The current Select Agent Program is administered jointly by the Centres for Disease Control and Prevention and the USDA. See: Centers for Disease Control and Prevention. (n.d.). Federal Select Agent Program. Retrieved October 17, 2018, from https://www.selectagents.gov/

[108] (Ari, 2012)

The PATRIOT Act and Bioterrorism Preparedness Act were two of seventeen bills introduced by the 107th Congress between 2001 and 2002 which had potential ramifications for research scientists working in biotechnology[109]. The U.S. government also set up an array of threat and vulnerability assessment exercises, prevention and protection efforts, and surveillance and detection programmes in quick succession[110]. U.S. biodefense spending skyrocketed in the following years, from $685 million in 2001 to over $8 billion in 2009[111].

4.4.1.2 Dual-use research concerns and reactions

Concerns about the dual-use nature of biotechnology research only seriously entered into public debate in the early 2000s, triggered by a series of controversial experiments. In response to these concerns, in 2002 leading journals in the life sciences and biological sciences jointly published a *Statement on Scientific Publication and Security*, publicly accepting responsibility for screening manuscripts with dual-use potential[112]. In 2004 a seminal report from the National Academy of Sciences – *Biotechnology Research in an Age of Terrorism* (otherwise known as the Fink Report) – recommended the establishment of the National Science Advisory Board for Biosecurity (NSABB) as a light touch mechanism for steering (but not regulating) dual-use research relevant to biosecurity issues[113]. On this recommendation, the NSABB was thus established in 2005.

The NSABB emphasized self-governance by researchers and published a *Proposed Framework for the Oversight of Dual Use Life Sciences Research* in 2007 to guide these self-governance efforts. The framework centred on a category of research which the NSABB described as 'dual-use research of concern' (DURC) – research that, 'based on current understanding, can be reasonably anticipated to provide knowledge, products, or technologies that could be directly misapplied by others to

[109] (Institute of Medicine & National Research Council, 2006)
[110] Lentzos, F. (2006). Rationality, Risk and Response: A Research Agenda for Biosecurity. *BioSocieties*, *1*(4), 453–464. https://doi.org/10.1017/S1745855206004066
[111] Franco, C. (2008). Billions for Biodefense: Federal Agency Biodefense Funding, FY2008-FY2009. *Biosecurity and Bioterrorism: Biodefense Strategy, Practice, and Science*, *6*(2), 131–146. https://doi.org/10.1089/bsp.2008.0025
[112] Atlas, R., Campbell, P., Cozzarelli, N. R., Curfman, G., Enquist, L., Fink, G., … Hammes, G. (2003). Statement on scientific publication and security. *Science*, *299*(5610), 1149–1149.
[113] (National Research Council, 2004)

pose a threat to public health and safety, agricultural crops and other plants, animals, the environment, or material.'[114]

Then, in 2011 two scientific papers became the focal point of an international controversy, thrusting dual-use research concerns in biotechnology into the spotlight[115]. The two papers, submitted for publication in *Science* and *Nature,* identified genetic mutations that conferred aerosol-based mammalian transmissibility to the H5N1 avian influenza, a highly pathogenic strain. This came to be known as the gain-of-function (GOF) controversy, where GOF refers to a category of research that aims to or is expected to increase the transmissibility and/or virulence of pathogens[116]. The papers were submitted to the NSABB for review and were unanimously recommended against publication. This triggered a backlash from the scientific community who criticised the NSABB for restricting their academic freedoms. The controversy became a matter of international debate – the World Health Organization (WHO) held a technical meeting in February 2012 to discuss the issue[117] and the Australia Group hosted discussions in relation to the use of export controls as a mechanism of oversight for dissemination of the results of these experiments[118]. Following further discussion, the NSABB voted in March 2012 to recommend publication of revised versions of both papers.

---

[114] National Science Advisory Board for Biosecurity. (2007). *Proposed Framework for the Oversight of Dual Use Life Sciences Research: Strategies for Minimizing the Potential Misuse of Research Information*. National Science Advisory Board for Biosecurity (NSABB).

[115] For a detailed recount of the GOF controversy, see: Medicine, I. of, & Council, N. R. (2013). *Perspectives on Research with H5N1 Avian Influenza: Scientific Inquiry, Communication, Controversy: Summary of a Workshop*. (K. Matchett, A.-M. Mazza, & S. Kendall, Eds.). Washington, DC: The National Academies Press. Retrieved from https://www.nap.edu/catalog/18255/perspectives-on-research-with-h5n1-avian-influenza-scientific-inquiry-communication

[116] GOF research is a specific category of dual-use research. The benefits of such experiments are usually in improving our understanding of disease causing agents, their interactions with human hosts and/or their potential to cause pandemics. They can be critical for informing public health and preparedness efforts, and for the development of countermeasures. However, they also pose obvious biosecurity and biosafety risks. A recent analysis suggests that GOF research could be conducted by up to approximately 40 research groups in the U.S. See: Berger, K., Stephan, R., Mauger, P., Venugopalan, G., & Casagrande, R. (2016). Biosecurity Risk Assessment of Acts Targeting a Laboratory. In Gryphon Scientific, *Risk and benefit Analysis of Gain of Function Research: Final Report*. Takoma Park: Gryphon Scientific. Retrieved from http://www.gryphonscientific.com/wp-content/uploads/2016/04/Risk-and-Benefit-Analysis-of-Gain-of-Function-Research-Final-Report.pdf

[117] The WHO meeting concluded that it was not possible nor desirable to limit access to information from the manuscripts; this conclusion was faced with much criticism.

[118] (Ari, 2012)

The GOF experiments and its surrounding controversy spurred the U.S. government to introduce a policy that would institutionalise the DURC framework, five years after the NSABB had recommended it do so. The 2012 *U.S. Government Policy for Oversight of Life Sciences Dual Use Research of Concern*, which was subsequently updated in 2014[119], applies to research involving fifteen specific agents and toxins and using one of seven types of experiments of concern. Researchers are mandated to undertake an initial assessment of potential risk and may be required to limit the venue and mode of communication of their results. Research institutions are also required to provide oversight through an Institutional Review Entity[120].

Further, in February 2013 the DHHS also conducted special reviews of request for funding of GOF experiments involving the H5N1 avian influenza strain. In 2014, the U.S. government instituted a pause in federal funding for certain GOF research[121]. The NSABB were specifically tasked with developing recommendations for a system of oversight for GOF research; the final set of recommendations were published in 2016[122] with subsequent implementation guidance released in 2017[123].

---

[119] The United States Government. (2012). United States Government Policy for Oversight of Life Sciences Dual Use Research of Concern. Retrieved from https://www.phe.gov/s3/dualuse/Documents/us-policy-durc-032812.pdf; The United States Government. (2014). United States Government Policy for Institutional Oversight of Life Sciences Dual use Research of Concern. Retrieved from https://www.phe.gov/s3/dualuse/Documents/durc-policy.pdf

[120] The policies reaffirmed a preference for research-led self-governance approaches, placing the responsibility on the principal investigators and research institutions to raise dual-use concerns and carry out the review process. Critically, they exclude research being conducted at facilities that do not receive U.S. government funding despite a strong NSABB recommendation that dual-use oversight should extend beyond academia to include other practitioners in the private sector. See: National Science Advisory Board for Biosecurity. (2010). *Addressing Biosecurity Concerns Related to Synthetic Biology*. Washington, D.C.: NSABB.

[121] This pause in federal funding remains in place pending agency implementations of review mechanisms consistent with guidance issued in January 2017 by the Office of Science and Technology Policy. See: The White House. (2014). *U.S. Government Gain-of-Function Deliberative Process and Research Funding Pause on Selected Gain-of-Function Research Involving Influenza, MERS, and SARS Viruses*. Washington, D.C.; Office of Science and Technology Policy. (2017). *Recommended Policy Guidance for Departmental Development of Review Mechanisms for Potential Pandemic Pathogen Care and Oversight*. Washington, D.C.: The White House.

[122] National Science Advisory Board for Biosecurity. (2016). *Recommendations for the Evaluation and Oversight of Proposed Gain-of-Function Research*. Washington, D.C.

[123] National Science Advisory Board for Biosecurity. (2017). *Responsible Communication of Life Sciences Research with Dual-Use Potential*. Washington, D.C.: National Institutes of Health (U.S.). Office of Biotechnology Activities. Retrieved from https://www.hsdl.org/?abstract&did=704404

Despite such efforts, a recent dual-use experiment reinvigorated criticisms of the inadequacy of existing DURC policies. In March 2017, the biotechnology company Tonix announced the results of an experiment that they had privately funded to synthesize the horsepox virus. The aim of the experiment was to contribute to the development of safer and more effective vaccines against smallpox. However, the experiment also acted as a proof of concept for the synthetic construction of a virus closely related to the smallpox virus, a highly contagious disease that was eradicated 40 years ago through an extensive global campaign[124]. The paper had been rejected by two leading science journals before it was eventually published in January 2018. The experiment was widely and heavily criticised for contributing to the potential re-emergence of a severe global threat to health security[125]. The successful publication of the study particularly demonstrated flaws in the governance of dual-use research at multiple stages of the process, from the design of the experiment through to the pre-publication review[126].

International fora have also begun to more explicitly address dual-use research concerns in the life sciences. The BWC convenings have been a primary site for dialogue and negotiation on issues ranging from harmonizing laboratory biosafety approaches to supporting education and training activities for researchers. Following the GOF controversy the BWC engaged more directly with

[124] Koblentz, G. D. (2017). The De Novo Synthesis of Horsepox Virus: Implications for Biosecurity and Recommendations for Preventing the Reemergence of Smallpox. *Health Security*, *15*(6), 620–628. https://doi.org/10.1089/hs.2017.0061

[125] DiEuliis, D., Berger, K., & Gronvall, G. (2017). Biosecurity Implications for the Synthesis of Horsepox, an Orthopoxvirus. *Health Security*, *15*(6), 629–637. https://doi.org/10.1089/hs.2017.0081; Inglesby, T. (2018). The problem of horsepox synthesis: new approaches needed for oversight and publication review for research posing population-level risks. Retrieved October 21, 2018, from http://www.bifurcatedneedle.com/new-blog/2018/1/19/the-problem-of-horsepox-synthesis-new-approaches-needed-for-oversight-and-publication-review-for-research-posing-population-level-risks; Lentzos, F. (2018). How do we control dangerous biological research? *Bulletin of the Atomic Scientists*. Retrieved from https://thebulletin.org/2018/04/how-do-we-control-dangerous-biological-research/

[126] Specifically, three weaknesses in DURC policies were evidenced through this study:

- Firstly, the horsepox virus is not listed as a pathogen that requires review, demonstrating the weakness in a list-based approach.
- Secondly, even if the horsepox virus had been listed, the nature of the experiment would not have qualified it as an experiment of concern because the review obligations only apply to government-funded research and this experiment was privately funded.
- Finally, the pre-publication review process found that the benefits of publication outweighed the risk in this case, demonstrating the subjectivity of such an assessment.

the matter of DURC via the Meetings of State Parties and Review Conferences[127]. At the UN level, two security council resolutions have been passed specifically targeted at mitigating the transfer of materials and intangible information that could be used for the development of biological weapons[128]. The NSABB have also established a working group of international scientific bodies specifically focused on bringing international harmonization to dual-use research guidelines[129].

4.4.1.3 The gene patent debate

The pivotal *Diamond v. Chakrabarty* case triggered a wave of patenting activity in the biotechnology industry across the 1980s and 1990s. In combination with the completion of the Human Genome Project in 2001, the U.S. Patent and Trademark Office (USPTO) has granted patents to nearly 60,000 DNA-based patents, with approximately 20% of the human genome patented in some form[130]. The US. holds up to 80% of the worldwide patent share in biotechnology, with the vast majority of them being held by U.S.-based biotechnology and pharmaceutical companies[131].

At the turn of the century, however, the rate of biotechnology patent issuance began to plateau. The annual rate of patenting peaked in 2001 and has been declining since[132]. A significant driver of this decreasing activity was the controversy surrounding gene patenting which, across the past two decades, triggered a shift in the legal treatment of biotechnology patents and generated uneasy tensions between the biotechnology industry and the USPTO.

---

[127] Lentzos, F. (2015a). *Dual Use in Biology and Biomedicine*. Nuffield Council on Bioethics. Retrieved from http://nuffieldbioethics.org/wp-content/uploads/Background-paper-2016-Dual-use.pdf

[128] In 2004 UNSC Resolution 1540 was adopted obliging all UN members not to provide 'any form of support to non-state actors that attempt to develop, acquire, manufacture, possess, transport or use nuclear, chemical or biological weapons.' In 2016 UNSC Resolution 2325 was adopted which 'encourages all states, as appropriate, to control access to intangible transfer of technology and to information that could be used for weapons of mass destruction and their means of delivery.'

[129] (National Research Council, 2007)

[130] Stone, K. (2018). The Gene Patents Debate. *The Balance*. Retrieved from https://www.thebalance.com/the-gene-patents-debate-2663137

[131] U.S. inventors filed more international patents on DNA sequences than any other country, including the combined total of all inventors in the European Union. Aside from industry patents, over 800 of the patents are held by the U.S. government, and approximately 5,000 or 15% of the issued patents are held by universities. See: (National Academy of Sciences, 2005)

[132] (National Academy of Sciences, 2005)

The gene patent debate is marked by several high profile patent protection controversies[133]. The first of these concerned the genes BRCA1 and BRCA2, identified as being linked to hereditary breast cancer. BRCA1 was first identified by a group of scientists at the University of Utah who subsequently filed for a patent for the gene and licensed exclusive rights to Myriad Genetics, a biopharmaceutical company founded by one of the lead researchers in the group. BRCA2 was simultaneously discovered by the same team as well as by the Institute for Cancer Research in the UK. Both groups filed patents for BRCA2 and were subsequently engaged in a legal dispute. In 1998 this was settled with Myriad paying for the exclusive rights to the UK patent, giving them an effective monopoly over diagnostic testing for BRCA1 and BRCA2. Myriad thus began enforcing its patent claims, specifically targeting universities for patent infringement[134]. This was considered uncommon practice in the biotechnology industry and was heavily criticised.

In 2009 these simmering tensions came to a boil. The American Civil Liberties Union (ACLU) and the Public Patent Foundation filed a suit against Myriad Genetics, the University of Utah Research Foundation and the USPTO on behalf of the Association of Molecular Pathology (referred to as the 'Myriad case'). ACLU claimed that this patenting practice violated the First Amendment and patent law, challenging the patentability of genes as 'products of nature' and the right of Myriad Genetics to restrict women's access to genetic screening for a hereditary disease. The case was escalated through to the Supreme Court which ruled, on June 13, 2013, that the naturally isolated DNA was not patentable but that the synthetic DNA was patentable[135]. The ramifications of this ruling for the biotechnology industry were significant. Specifically, the

[133] A gene patent refers to a patent that generally falls into one of the following four categories:
- Genes in whole or in part, including isolated nucleotide sequences;
- Proteins that genes encode and their function in organisms;
- Vectors used for the transfer of genes from one organism to another;
- Genetically modified cells or organisms, the processes used for making these genetically modified products, and the uses of genetic sequences or proteins for genetic tests

See: (Jamison, 2015)

[134] For example, in 19999 Clinical Genetics Lab at the University of Pennsylvania received a patent infringement notification form Myriad Genetics and were advised to cease their activities.

[135] The specific details of the ruling can be found in: (Stone, 2018)

decision invalidat4ed many existing patents – the USPTO had issued 2,645 patents for isolated DNA over the past three decades prior to the ruling, many of which were subsequently challenged in courts and legislatures[136].

The *Mayo Collaborative Services v. Prometheus Laboratories* U.S. Supreme Court Case of 2012 resurfaced the gene patent debate. Mayo Collaborative Services Inc., a private biotechnology company, sought to patent methods that determined the optimal dose of thiopurine to use for patients with inflammatory bowel disease using a diagnostic assay developed by Prometheus Laboratories. Prometheus sued Mayo for infringing on their already established patent for the assay. Ultimately, the U.S. Supreme Court ruled that Mayo's method was not patentable because the methods set forth were based on 'laws of nature'[137].

4.4.2 Relationships

4.4.2.1 Researchers <> State

In the wake of the 9/11 and Amerithrax attacks, the elevation of biosecurity as a national priority meant that the state was increasingly willing to restrict researcher activities. This resulted in conflict between the biotechnology research community and the state. The events of 2001 thus marked a transition in the research environment from voluntary compliance with recommended practices to the imposition of statutes and regulations in the name of national security. Within the research community, there emerged distinct disagreements about the role that scientists should play in upholding the norms of science versus acting as responsible citizens[138].

[136] (Jamison, 2015)
[137] (Battaglia, 2016)
[138] Campbell, E. G., Clarridge, B. R., Gokhale, M., Birenbaum, L., Hilgartner, S., Holtzman, N. A., & Blumenthal, D. (2002). Data withholding in academic genetics: evidence from a national survey. *Jama*, *287*(4), 473–480.; Kempner, J., Perlis, C. S., & Merz, J. F. (2005). Forbidden knowledge. *Science*, *307*(5711), 854–854.; Selgedid, M. J. (2007). A tale of two studies: ethics, bioterrorism, and the censorship of science. *Hastings Center Report*, *37*(3), 35–43.

These conflicts manifested in two forms – firstly as attempts to restrict research publications, and secondly as attempts at barring foreign researchers from the United States.

Restrictions on research publication

The classification of research was typically only applicable to research 'owned by, produced by or for, or under the control of the United States Government'; unless the research was clearly related to national security it was understood that classification did not apply[139]. However, by January 2002 over 6,500 unclassified documents relating to chemical and biological warfare information began to be withdrawn from public access under the new category of 'sensitive but unclassified' information. George Poste, a prominent science adviser to the U.S. DOD, urged publicly that some aspects of basic microbiological research be made classified, prompting heated debate within the research community[140]. In 2002, draft legislation was put forward which would have required researchers to obtain DOD approval to discuss or publish findings of all military-sponsored unclassified research. This was withdrawn in the face of considerable criticism from the research community[141].

Universities increasingly reported inconsistencies in the type of research that was considered classified. The lack of consistency in classification policies and practices frustrated researchers, resulting in many universities deciding not to pursue government-funded research for fear that this may place restrictions on the free flow of individuals and information on campus. A survey of 20 institutions in 2003 and 2004 found 138 attempts by the government to restrict the publication of data or foreign-national participation in research activities at U.S. universities[142].

---

[139] (Ari, 2012)
[140] McLeish, C., & Nightingale, P. (2007). Biosecurity, bioterrorism and the governance of science: The increasing convergence of science and security policy. *Research Policy*, *36*(10), 1635–1654. http://dx.doi.org/10.1016/j.respol.2007.10.003
[141] (Institute of Medicine & National Research Council, 2006)
[142] (National Research Council, 2007, p. 9)

However, the degree to which the state was in a position to enforce these restrictions was questionable. A paper, published in 2005, described research conducted to reconstruct the influenza virus that was responsible for the 1918 Spanish Flu epidemic. As the manuscript was undergoing peer review for publication in *Science,* the authors were urged to raise their concerns to the Office of the Secretary of the DHHS. This prompted a review by the NSABB of the paper; the NSABB consequently recommended publication of the paper with suggested changes. However, *Science* proceeded to publish the paper without the recommended changes. Then-editor in chief of *Science,* Donald Kennedy, issued a statement criticising the government's attempt to restrict publication of the paper: 'Government officials…can't order the non-publication of a paper just because they consider the findings 'sensitive'. No such category short of classification exists'[143]. Similar advice from the DHHS was ignored by the journal *PNAS* regarding a 2005 paper which provided a mathematical model of a bioterror attack on a food supply chain through the introduction of the botulinum toxin[144].

Regulations on foreign researchers

Another element of dual-use regulation that caused conflict between researchers and the state was the targeting of foreign researchers. Specifically, in categorising foreign researchers as 'deemed exports'[145] with access to dual-use information or technologies, various regulatory actions have progressively curtailed the ability of foreign nationals to conduct research in the U.S.[146].

Concretely, in the wake of the events in 2001, the regulatory regime made it more difficult for foreign scientists to engage in biotechnology research in collaboration with U.S. researchers and research institutions. This was achieved in part by the passing of the PATRIOT Act which required

[143] Kennedy, D. (2005). Editorial: Better Never than Late. *Science*, *310*(5746), 195–195.
[144] Wein, L. M., & Liu, Y. (2005). Analyzing a bioterror attack on the food supply: The case of botulinum toxin in milk. *Proceedings of the National Academy of Sciences of the United States of America*, *102*(28), 9984. https://doi.org/10.1073/pnas.0408526102
[145] Deemed export controls regulate the transfer of certain information to foreign nationals, thereby constraining who can participate in associated research and education activities.
[146] (Institute of Medicine & National Research Council, 2006)

the Attorney General to implement the foreign student visa-monitoring program established by the *Illegal Immigration Reform and Immigrant Responsibility Act of 1996*. Further, Section 501 of the *Enhanced Border Security and Visa Entry Reform Act*, passed in 2002, established a foreign student monitoring program to maintain information on foreign students and exchange visitors.

These changes have concretely impacted the ability for qualified individuals to conduct research in biotechnology. Numerous foreign researchers were barred from the U.S. in the first half of 2003, leading to the disruption of at least 24 research projects related to biodefense across 20 universities[147]. Further, from 2003 to 2004 the number of foreign students applying to U.S. graduate programs in the life sciences fell by 24%, at least in part due to the greater restrictions placed on non-U.S. citizens[148]. This reversed what had been a growing proportion of foreign-born U.S. scientists and engineers prior to 2001[149].

The research community have responded with protest. Promptly after the restrictions were tightened, the presidents of the National Academies issued a statement of warning[150]:

> Our visa processing system not only must provide genuine security against those who might do us harm, but also keep our borders open to the stream of scientific and technical talent that fuels our progress…the U.S. scientific, engineering and health communities cannot hope to maintain their present position of international leadership if they become isolated from the rest of the world.

---

147 (Hoyt & Brooks, 2003)
148 (Institute of Medicine & National Research Council, 2006)
149 In 1996 only 23% of science and engineering doctorates were foreign born, compared to 39% in 2000. Post 2001, these figures waned. See: Council of Graduate Schools (CGS). (2004). Council of Graduate Schools Finds Decline in New International Graduate Student Enrolment for the Third Consecutive Year. CGS.
150 Alberts, B., Wulf Wm, A., & Fineberg, H. (2002). Current visa restrictions interfere with US science and engineering contributions to important national needs. *National Academies*. Retrieved from http://www8.nationalacademies.org/onpinews/newsitem.aspx?RecordID=s12132002

As this warning failed to be heeded, on March 26th, 2003 researchers collectively raised vigorous protest in a House Science Committee hearing. Two weeks later, John Marbuger, the Director of the Office of Science and Technology Policy, also lent his support to addressing these visa issues in a speech at the AAAS Science and Technology Policy Colloquium[151]. In 2005 40 leading scientific societies and higher education associations released a joint statement demanding the easing of restrictions on foreign researchers, warning that the U.S. 'risk[s] irreparable damage to our competitive advantage in attracting international students, scholars, scientists, and engineers, and ultimately to our nation's global leadership'[152].

4.4.2.2 Firms <> State

The 9/11 and Amerithrax attacks placed biodefense at the centre of the Bush Administration's security agenda, and with that a call to arms for the biotechnology industry to cooperate with the government. In his keynote address at the Biotechnology Innovation Organisation (BIO) Convention in 2003, President Bush stated: 'The biotechnology industry finds itself on the front lines of some of the greatest challenges of our time. The first challenge is the need to fight terror.' Then-Secretary of Homeland Security, Tom Ridge, further emphasized the opportunity – both economically and symbolically – that biodefense programmes offered private firms[153]:

> Your work will help us detect biological weapons…Your work will help us treat the diseases they cause and identify their symptoms at an early age. Your work will help us find new ways to strengthen our food and water systems and other critical infrastructure that may be susceptible to an attack. Your work will help make our first responders less vulnerable, our hospitals less exposed, and our physicians and medical professionals much more effective.

---

151 (National Research Council, 2009b)
152 (McLeish & Nightingale, 2007)
153 Lentzos, F. (2007). The American Biodefense Industry: From Emergency to Nonemergence. *Politics and the Life Sciences*, *26*(1), 15–23.

BIO – the world's largest trade organisation for the biotechnology industry – have also asserted support for commercial biotechnology firms engaging with national security programmes. In their 2004 annual report they stated: 'Biotechnology scientists and executives are eager to use the technologies that have transformed mainstream healthcare to develop an arsenal of products for biodefense'[154]. Further, BIO hosted a conference in partnership with the Department of Homeland Security specifically aimed 'to facilitate the contribution of biotechnology to American defense'[155]. In subsequent years at their annual BIO conventions they have hosted a series dedicated to biodefense. They have also issued a series of press releases[156] and offered testimonies in Congressional hearings all to the effect of proclaiming industry willingness to participate in biodefense activities in partnership with the state[157] as well as industry preparedness to offer cutting edge technology products to these ends[158].

The biotechnology industry did indeed engage comprehensively in state biodefense activities. Between 1995 to the end of 2005 a total of 307 biodefense-related grants and contracts were awarded to private firms, accounting for approximately 30% of all biodefense projects undertaken by the U.S. government. This amounted to a total investment of $137.1 million in private firms[159]. Project BioShield, established in 2004, played a significant role in facilitating public-private cooperation in biodefense. Project BioShield was set up as a ten year effort to accelerate the awarding of grants for medical countermeasures (MCMs) research as well as create incentives for private companies to develop MCMs for inclusion in the national stockpile. This was a particularly

---

[154] Biotechnology Innovation Organization. (2004). *Milestones 2004: Biotechnology Industry Organization Annual Report*. Retrieved from https://www.bio.org/insights

[155] BIO. (2002). 35 Biotech Companies To Present New Technologies & Products for Homeland Security. *Biotechnology Innovation Organization*. Retrieved from https://www.bio.org/media/press-release/35-biotech-companies-present-new-technologies-products-homeland-security

[156] Indicative press release titles include: 'Bioterrorism: A challenge we cannot decline to meet' and 'Ethical use of biotechnology to promote public health and national security and to fight against bioterrorism.

[157] (Lentzos, 2007)

[158] BIO surveyed member firms post 9/11 and found that 'many biotechnology companies were already working on defense projects or were developing technologies that could be used for both conventional healthcare and for defense against biological agents.'. This was published in a press release titled: 'Biotechnology, Public Health and National Security: How the industry can develop biodefense product' (24 October 2002).

[159] (Lentzos, 2007)

prime target for industry collaboration given that there is limited to no commercial market for MCMs and the usual costs of developing MCMs for the government are obstructively high for most private companies. To further incentivise MCM development, Congress created the Biomedical Advanced Research and Development Authority (BARDA) in 2006; BARDA were responsible for investing $6 billion between 2004 and 2013 to advance the development and procurement of MCMs specifically via working with industry. These efforts have yielded a number of successes, including the addition of 12 MCMs to the national stockpile and the rapid transition of three vaccines and one therapeutic into clinical development in response to the Ebola crisis in 2014[160].

This industry-state partnership has not been without its challenges. Leaders in biotechnology firms have expressed frustration at the lack of clarity and the excess of bureaucracy associated with biodefense contracts. One executive summarises the issues as follows[161]:

> The current procurement process is cumbersome from two principal vantage points: 1) it is not transparent and 2) it does not provide sufficient information about future countermeasure needs. It costs over $150 million to bring a new biodefense drug to market and a typical drug development program takes 4-6 years. Companies, particularly small biotechnology companies…cannot afford to make these types of investments unless they believe there is a real and sustainable market for their products.

[160] (Blue Ribbon Study Panel on Biodefense, 2015)
[161] Wright, D. P. Statement by David Wright - Bioshield: Linking bioterrorism threats and countermeasure procurement to enhance terrorism preparedness, § Subcommittee on Emergency Preparedness, Science and Technology of the U.S. House of Representatives Committee on Homeland Security (2005).

Others have reported a lack of clarity from the government on how much market demand they would be willing to commit to[162] and when procurement contracts will materialise[163], thrusting companies into conditions of uncertainty that become intractable if they are to remain financially sustainable.

Biotechnology firms and private venture capitalists have also pointed out the fundamental mismatch in the risk-reward model of an innovative company engaged in commercially-motivated R&D versus a defense contractor to the government. As one executive notes at a 2003 Congressional hearing[164]:

> Efforts to attract the best people and companies to work for many years on high-risk countermeasure projects will fail if the reward structure is not aligned with the prevailing incentive in their industry. Venture capitalists do not, as a rule, invest in companies with business models such as professional services firms or companies aiming to build a business based on contract R&D at industry averages. We aim for our companies to produce products based on defensible intellectual property which have the kinds of margins seen in truly innovative software, pharmaceuticals, and electronic devices.

Indeed, the discrepancy in the expected rates of return for a typical biotechnology company compared to the those for a defense contractor are significant[165], leading many in the biotechnology industry to steer clear of government defense contracts unless they have no other option to stay

---

[162] Hollis, R. B. Statement by Richard Hollis - Bioshield: Linking bioterrorism threats and countermeasure procurement to enhance terrorism preparedness, § Subcommittee on Emergency Preparedness, Science and Technology of the U.S. House of Representatives Committee on Homeland Security (2005).
[163] Wysocki, B. (2005). US struggles for drugs to counter biological threat. *The Wall Street Journal*.
[164] Leighton, R. Leighton Read, statement on behalf of BIO - Furthering public health security: Project Bioshield, § Subcommittee on Health and Subcommittee on Emergency Preparedness and Response, of the Committee on Energy and Commerce, (2003).
[165] The average rate of return for a successful biotechnology company was 31.8% in 2001 and 28% in 2002. For major defense contractors the average rate of return was 8.5% in 2001 and 9.6% in 2002. See: (Lentzos, 2007)

in business[166]. To some extent this has been acknowledged by the state via proposed legislation for a Project BioShield II which would aim to move towards a model where biotechnology companies are engaged as entrepreneurs rather than defense contractors, with a risk-reward model that more closely mimics that in the commercial sector. The DOD have also begun to implement more innovative acquisition strategies, including the use of other transaction authorities (OTAs), in order to better enable industry participation in biodefense activities[167].

4.4.2.3 Researchers <> Firms

The gene patent debate caused conflicts between researchers and firms in the biotechnology industry largely due to differing goals when it comes to pursuing R&D activities. Firms, on the one hand, are conclusively supportive of patenting biotechnology research – holding proprietary technologies is a cornerstone of their business models and is the crux of their competitive advantage, particularly in the early stages of a firm.

Researchers, on the other hand, are largely against the patenting of biotechnology research. For one, they fear that patenting will hamper research progress by introducing licensing costs in order to enable use of patented technologies in research activities[168]. Broad patents in particular hinder research by limiting access across a broad range of technologies; this is common as a defensive patenting strategy among pharmaceutical companies. This concern has been salient when it comes to genomic data, a domain in which researchers have pushed strongly for freely available data access stored in the public domain from projects like the Human Genome Project, the Expressed Sequence Tag (EST) Project, and the SNP Consortium[169].

[166] Lieberman, J. Senator Joseph Lieberman's statement - Creating a BioDefense Industry: BioShield II, § Senate Judiciary and Senate HELP Committees (2004).
[167] (Blue Ribbon Study Panel on Biodefense, 2015)
[168] (Caulfield et al., 2006; Jamison, 2015; Stone, 2018)
[169] (National Academy of Sciences, 2005)

The research community have also expressed concern that patenting goes against a staple norm among scientists – that research results should be fully accessible to the public and that a culture of openness is critical for the conduct of collaborative research. The commercial incentives introduced by patenting incentivises faculty members to delay publication, keep research results secret, and become less willing to share research materials and data with other researchers. Indeed, there is evidence for this being the case among university researchers involved in genetics research. Industry funding is often associated with delayed publication, and several studies have found that commercial activity has had negative effects on the culture of openness in science[170].

Despite these prima facie conflicts between the goals of researchers versus firms, the evidence that such conflicts exist in practice is limited. Researchers have in fact been supportive of patenting to some extent, recognising that it can be beneficial for research. The majority of DNA patent holders are universities and non-profit organisations, and a norm of non-exclusive licensing to other university researchers as well as firms for modest fees has enabled more open research than would be the case if research results were held as trade secrets. Indeed, the NIH explicitly encourages its grantees to file for patents and thus license proprietary research tools as a means of ensuring broad access to the discovery. Further, there is a lack of empirical evidence that patenting has hampered research progress due to a combination of generous licensing practices, a lack of awareness of existing patents among researchers, and a reluctance on the part of firms to litigate against researchers[171]. Research institutions also often benefit from exemptions to U.S. patent law[172].

[170] (Caulfield et al., 2006)
[171] (National Academy of Sciences, 2005; Stone, 2018)
[172] National Academy of Sciences. (2004). *A Patent System for the 21st Century*. Washington, D.C.: National Academies Press.

4.5 Analysis and discussion

The evolution of modern biotechnology tells a number of interweaving stories about the relative power, interests, and capacities of biotechnology researchers, firms, and the U.S. government. The manner in which these actors evolve as biotechnology matures is described in section 4.5.1 and Table 4.5-1. Then, section 4.5.2 and Table 4.5-2 offer a critical overview of the relationships between these three actors.

4.5.1 The evolution of the actors

Across the phases of biotechnology development and deployment, the state became increasingly concerned about biosecurity risk mitigation – that is, protecting the nation from risks due to bioterrorism, biological warfare, and biosafety hazards. This became particularly central in phase 3 in the wake of the Amerithrax attacks in 2001 and the series of dual-use and gain-of-function experiments across the early 2000s. While interest in biotechnology's military applications saw an uptick in phase 3 with the emergence of synthetic biology, this remained a muted goal, in part due to the strong international norm established in phase 1 against the use of biological weapons.

With respect to the state's resources, the influx of private funding at the commencement of phase 2 meant that the early stage R&D funds provided by the state became more fungible with time. Conversely, the state was more willing and able to exercise its legislative capacity particularly as the public expressed escalating fears of bioterrorism, creating the mandate for state action in phase 3.

Firms pursued the maximisation of profit as a central goal throughout the development of modern biotechnology. Their innovation capacity strengthened as firms became more transnational. Simultaneously, they became increasingly constrained by the legislative environment particularly as it encroached on their global growth goals. The role of public concern did not appear to feature heavily in terms of influencing the behaviour of firms across the phases.

Researchers grew into a transnational research community with strong norms of self-governance. Across the phases, however, researchers also became increasingly wedded to the private biotechnology industry both for funding, and as licensees of their patented discoveries. This reduced the value of their early-stage innovation capacity insofar as the technology moved from basic research through to commercialisation, and to some extent weakened the ability of researchers to pursue research in an open, unconstrained manner.

4.5.2 The evolution of actor relationships

The relationship between the researchers and the state began cooperatively. In phase 1, the research community held the reins with the state participating as supportive funders of early stage R&D efforts. Simmering concerns about rDNA technology in the 1970s were quickly quashed via proactive self-governance measures on the part of the research community. However, as the risks from biotechnology became more salient, the state increasingly came into conflict with researchers in attempts to regulate the movement of individuals and materials across borders and restrict the conduct and publication of certain types of experiments.

Between firms and the state, there remained a consistent level of state support for the growth of the biotechnology industry. With the escalation of biosecurity efforts in phase 3, this synergy is strengthened with the involvement of industry in state-sponsored biodefense programmes. Specifically, the state's dependence on firms for the development of countermeasures meant that the state increasingly adapted its practices to cater to the business models of biotechnology firms.

Finally, between researchers and firms, the relationship was initially synergistic. As of phase 2, the line between researchers and firms began to blur as we saw a shift from public to private control of biotechnology research. The dynamic remained generally mutually beneficial save for some conflicts that emerged in relation to patenting activity, where the private norms of firms and the open norms of the research community collided.

Table 4.5-1: Summary of evolution of actors

		State	*Firms*	*Researchers*
Goals		Economic growth = Military leadership ↑ Risk mitigation ↑	Maximise profit =	Pursue research =
Resources and constraints	*R&D funding*	Resource ↓	Resource ↑	Constraint =
	Innovation capacity	(Resource)	Resource ↑	Resource ↓
	Legislative environment	Resource ↑	Constraint ↑	Constraint ↑
	Public concern	Constraint ↑	(Constraint)	(Resource)

Notes:
↑ means that the goal / resource / constraint becomes more advantageous / constraining as the technology matures
↓ means that the goal / resource/constraint becomes less advantageous / constraining as the technology matures
= means that the goal / resource / constraint remains constant as the technology matures
() means that the goal / resource / constraint is irrelevant in this case

Table 4.5-2: Summary of evolution of relationships

	Synergies	*Conflicts*
State <> *Firms*	State depends on access to commercial technologies ↑	State prevents firms from proliferating technologies ↑ (Firms face public backlash for selling technologies to the state)
State <> *Researchers*	State creates supportive R&D environment ↓	State prevents researchers from proliferating knowledge and talent ↑
Firms <> *Researchers*	Firms creates supportive R&D environment ↑	Researchers clash with firms on issues of ethics and societal consequences ↑

Notes:
↑ means that the synergy / conflict becomes stronger as the technology matures
↓ means that the synergy / conflict becomes weaker as the technology matures
() means that the synergy / conflict is irrelevant in this case

5 Cryptography

Cryptography has transformed the way in which we interact and transact in the digital world. Cryptographic technologies form the backbone of the Internet and global telecommunications systems, enabling the prerequisite security that has empowered us to engage in the likes of financial transactions, e-commerce, and mass communications online. As our economies and societies have transitioned towards digitalisation and globalisation, cryptography has become ever more critical to the goals of national security, economic growth, and the preservation of civil liberties[1].

In the past decade, a wave of modern cryptographic technologies has introduced new potential applications of cryptography. These technologies include: blockchains, which enable the creation of a decentralized, distributed digital ledger that records transactions reliably across a network; cryptocurrencies, which are digital currencies that rely on decentralized control, typically based on a blockchain and operated independently of traditional financial institutions; and smart contracts, a mechanism that allows users to enter into an enforceable agreement without relying on third parties. Whilst it would be pre-emptive to define the impact of these emerging cryptographic technologies, many have made claims of their transformative potential[2]. The Director of Financial and Enterprise Affairs at the Organisation for Economic Cooperation and Development (OECD) has stated that blockchain technology 'has the potential to completely revolutionise our economies and

[1] Committee to Study National Cryptography Policy, Computer Science and Telecommunications Board, & Commission on Physical Sciences, Mathematics, and Applications. (1996). *Cryptography's Role in Securing the Information Society*. (K. W. Dam & H. S. Lin, Eds.). Washington, D.C.: National Academies Press.

[2] Ito, J., Narula, N., & Ali, R. (2017). The Blockchain Will Do to the Financial System What the Internet Did to Media. *Harvard Business Review*. Retrieved from https://hbr.org/2017/03/the-blockchain-will-do-to-banks-and-law-firms-what-the-internet-did-to-media; Walport, M. (2016). *Distributed ledger technology: beyond block chain*. UK Government Office for Science. Retrieved from https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/492972/gs-16-1-distributed-ledger-technology.pdf

societies', gesturing to its applications in business, government, and international policy issues as just the beginning of a future 'which we can't even imagine today'[3].

The military value of cryptography dates even farther back in history. Methods of encryption have been central to the notion of security for as long as 4,000 years, used by leaders in ancient Egypt and Greece to protect state secrets. During World War II, cryptography played a pivotal role both for offensive and defensive purposes – namely in Germany's use of then-advanced encryption and Britain's corresponding cryptanalysis efforts[4]. Today, our governments rely on cryptography to protect national secrets from foreign adversaries and malicious actors, and cryptanalysis techniques underpin core intelligence gathering efforts.

Conversely, the capacity for cryptography to create significant harm stems from the usefulness of cryptographic technologies in enabling malicious behaviour. Encryption enables adversarial actors, whether they be hostile states, terrorist groups, or criminals, to conceal information and avoid detection by law enforcement and intelligence agencies. According to U.S. administration officials, cryptography in the hands of foreign adversaries have harmed national security interests by impairing intelligence gathering efforts, increasing the capabilities of adversaries to conceal the development of missile delivery systems and weapons of mass destruction, and increasing the costs of national security operations[5]. Cryptography also makes it more difficult for law enforcement agencies to recover useful information to aid their cases. Deputy Attorney General Rod Rosenstein claimed that in 2017 because of encryption 'the FBI was unable to access about 7,500 mobile devices submitted to its Computer Analysis and Response team, even though there was the legal authority to

[3] Medcraft, G. (2018). *The OECD and the Blockchain Revolution*. Presented at the OECD Friends of Going Digital Meeting, Paris. Retrieved from https://www.oecd.org/parliamentarians/meetings/meeting-on-the-road-london-april-2018/The-OECD-and-the-Blockchain-Revolution-Presentation-by-Greg-Medcraft-delivered-on-29-March-2018.pdf

[4] For a comprehensive history of cryptography, see: Kahn, D. (1996). *The Codebreakers: The comprehensive history of secret communication from ancient times to the internet*. Simon and Schuster.

[5] (Committee to Study National Cryptography Policy et al., 1996)

do so"[6]. Cryptography is also the core technology underpinning hidden online exchanges and marketplaces, enabling the emergence of the 'darknet'[7] – a cyber black market populated by a network of highly organised groups often connected with drug cartels, mafias, and terrorist cells[8].

Cryptanalysis techniques – methods for decrypting encrypted data – have also enabled cyber-attacks and cyber exploitation efforts by state and non-state actors. Whilst the technical details of how such attacks are conducted are not publicly available, it is highly probable that both the use of cryptanalysis and the absence of strong encryption were central to a number of cyber-attacks with significant repercussions, ranging from the destruction of physical infrastructure to the theft of data critical to the security of citizens and the state[9]. The cybersecurity threat has topped the list of global threats in the Worldwide Threat Assessment of the U.S. intelligence community since 2013[10].

The widespread use of cryptography is a double-edged sword. On the one hand, cryptography has and continues to enable opportunities for significant improvement in our quality of life. It has enabled the modern Internet, communications, and economic activity. It protects the trade secrets and proprietary information of businesses and protects nationally critical information from malicious espionage and theft. However, encryption threatens the effectiveness of intelligence gathering and law enforcement efforts and enables increasingly sophisticated malicious activity in cyberspace. Robert Hannigan, then-Director of the UK

---

[6] Rosenstein, R. J. (2017). Deputy Attorney General Rod J. Rosenstein Delivers Remarks on Encryption at the United States Naval Academy: Remarks as prepared for delivery.
[7] Biddle, P., England, P., Peinado, M., & Willman, B. (2002). The darknet and the future of content protection. In *ACM Workshop on Digital Rights Management* (pp. 155–176). Springer.
[8] Ablon, L., Libicki, M. C., & Golay, A. A. (2014). *Markets for Cybercrime Tools and Stolen Data: Hackers' Bazaar*. RAND Corporation. Retrieved from https://www.rand.org/pubs/research_reports/RR610.html
[9] Lin, H. (2016). Governance of Information Technology and Cyber Weapons. In E. D. Harris (Ed.), *Governance of Dual-Use Technologies: Theory and Practice*. American Academy of Arts and Sciences.
[10] National Academies of Sciences, Engineering, and Medicine. (2018). *Decrypting the Encryption Debate: A Framework for Decision Makers*. Washington, DC: The National Academies Press. Retrieved from https://www.nap.edu/catalog/25010/decrypting-the-encryption-debate-a-framework-for-decision-makers

intelligence agency Government Communications Headquarters (GCHQ), put it aptly in a 2016 speech on the challenges of encryption in the digital era[11]:

> At its root, the ethical problem presented by encryption is the problem presented by any powerful, good invention, including the internet itself, namely that it can be misused…The technology of the internet and the web is morally neutral, but those of us who use it aren't.

Section 5.1 describes the key actors who have been critical in shaping the trajectory of cryptography. Then, sections 5.2 to 5.5 step through the four phases of cryptography development and deployment – *emergence and promise*; *commercialisation and proliferation*; and two phases of *consolidation and contestation*. Finally, section 5.6 offers a summative analysis.

[11] Weitzner, D. J. (2016). The Encryption Debate Enters Phase Two. Retrieved from https://www.lawfareblog.com/encryption-debate-enters-phase-two

5.1 The actors

The trajectory of cryptography has been shaped by three actors – the state, the firms, and the researchers. In the following sections, each actor is described in the context of their engagement with the development and deployment of cryptography.

5.1.1 State

The case of cryptography starkly illustrates competing goals in relation to cryptography all housed within the umbrella of the U.S. government. The three goals at play are as follows:

- The strengthening of national security via limiting access to strong cryptographic technologies beyond national borders (represented by the National Security Agency, NSA, and to some extent domestic law enforcement represented by the Federal Bureau of Investigation, FBI);
- The strengthening of national security via domestic deployment of strong cryptographic technologies (represented by the FBI, and to some extent the Department of Justice, DOJ, and the NSA);
- The protection of civilian privacy (represented by Congress).

Whilst these competing interests are all facets of 'national interest', they proved to be to some extent irreconcilable in the case of cryptography. The divisions were most prominent between the NSA and FBI versus Congress. The former agencies have, for the most part, consistently advocated for unfettered access to decrypted information, whether through the deployment of cryptography products with built-in backdoors or halting the widespread dissemination of strong encryption that would hamper their information gathering efforts. Congress, for the most part, has played the role of representing the interests of citizens to have access to strong encryption to protect individual privacy and security. The following sections articulate these tensions in more detail.

5.1.1.1 National security and law enforcement

Both the national security and law enforcement components of the U.S. government holds two primary goals simultaneously: preventing the proliferation of strong cryptographic technologies to malicious actors; and enabling the deployment of strong cryptographic technologies for the protection of important national information.

For national security – namely the NSA – the primary mandate is to protect the country against attack by foreign adversaries. It has two functions: signals intelligence (SIGINT) and communications security (COMINT)[12]. SIGINT translates into activities such as the collection of intelligence on the capabilities and intentions of both friendly and hostile states, organisations and individuals. COMINT translates into activities to secure sensitive communication and information from foreign interference.

Consequently, cryptography is relevant to national security on a number of fronts. Cryptography is often considered to be the only serious barrier to SIGINT – the stronger the cryptographic capabilities of the opponents, the more difficult it is to gather intelligence. This concern underpins the NSA's stance against the widespread deployment of strong cryptographic systems and the adoption of strong cryptographic standards. The more proliferated and uniform the global market of cryptographic technologies, the more difficult it is for the NSA to extract information from an opponent. Simultaneously, for COMINT activities, the NSA are also heavily invested in strengthening the cryptographic technologies deployed for securing national infrastructure domestically[13].

Law enforcement has a number of reasons to support cryptography – it prevents information theft from businesses and individuals, secures law enforcement communications, and reliably

[12] (Diffie & Landau, 2010)
[13] Landau, S. (2014b). Under the Radar: NSA's Efforts to Secure Private-Sector Telecommunications Infrastructure. *Journal of National Security Law & Policy*, *7*(3), 1–31.

authenticates law enforcement officials. However, the FBI has been opposed to the widespread use of encryption primarily on the grounds that the benefits of cryptography do not outweigh the harm that it causes to law enforcement activities. Louise Freeh, then-Director of the FBI, testified before Congress in 1997 summarising the law enforcement perspective as follows[14]:

> Law enforcement is in unanimous agreement that the widespread use of robust, unbreakable encryption ultimately will devastate our ability to fight crime and prevent terrorism. Unbreakable encryption will allow drug lords, spies, terrorists, and even violent gangs to communicate about their crimes and their conspiracies with impunity. We will lose one of the few remaining vulnerabilities of the worst criminals and terrorist upon which law enforcement depends to successfully investigate and often prevent the worst crimes.

Decades later, James Comey, then-Director of the FBI, echoed the same sentiment in 2014[15]:

> [W]ith sophisticated encryption, there might be no solution, leaving the government at a dead end – all in the name of privacy and network security.

The DOJ have been less vocal than the FBI but have nevertheless expressed similar sentiments[16].

---

[14] Freeh, L. Hearing of the Terrorism, Technology and Government Information Subcommittee; Subject: Encryption Technology, § Senate Judiciary Committee (1997). Federal News Service.
[15] Comey, J. B. (2014). *Going Dark: Are Technology, Privacy, and Public Safety on a Collision Course?* Presented at the Brookings Institution, Washington, D.C. Retrieved from https://www.fbi.gov/news/speeches/going-dark-are-technology-privacy-and-public-safety-on-a-collision-course
[16] An example of this is in a statement from the Principle Associate Attorney General, Robert S. Litt: Litt, R. S. Prepared statement of Robert S. Litt, Principle Associate Deputy Attorney General; Subject: Privacy in a digital age: Encryption and mandatory access, § Senate Judiciary Committee, Subcommittee on the Constitution, Federalism, and Property Rights (1998). Federal News Service.

5.1.1.2 Congress

Whilst the stance of Congress has been far less homogeneous and consistent than those expressed by the NSA and the FBI, specific members of Congress have been particularly influential in pushing back on the dominance of the national security and law enforcement agendas. Among them are Senator Patrick Leahy who, in 1996, introduced the *Encrypted Communications Privacy Act* affirming the right to use any form of encryption domestically and relaxing export controls on cryptographic products. Senator Conrad Burns followed with the *Promotion of Commerce On-Line in the Digital Era Act* (PRO-CODE) liberalising export controls on cryptography and enshrining the freedom to sell and use any type of encryption domestically. Representative Bob Goodlatte proposed the *Safety and Freedom through Encryption Act* (SAFE) in 1999, prohibiting mandatory exceptional access for law enforcement and security agencies in cryptographic products, and permitting the export of strong encryption. Representative Maria Cantwell pioneered efforts to reform export controls on cryptographic products beginning in the 1990s. This is but a selection of key members of Congress who, across the years, have lobbied for industry and citizen interests within the state apparatus.

5.1.2 Firms

Within the cluster of private sector firms relevant to cryptography, there are three distinct sub-groups distinguished by different approaches to integrating cryptographic technologies into their business models. Nevertheless, all three groups require encryption as a central part of their business model and thus see cryptographic technologies primarily in the frame of a profit incentive.

The first group of firms are vendors of cryptographic products and services. These are perhaps the most directly relevant private actors insofar as their business model revolves around the development and sales of cryptographic technologies. These firms are typically

relatively small in size; their specialisation is in the early stages of the R&D pipeline and thus selling cryptographic products and services to larger firms.

Multinational technology corporations such as Google, Microsoft and Apple form the second sub-group of private sector firms. These firms incorporate cryptographic technologies as a central component of their products and services, and often are the clients of the aforementioned vendors of cryptographic technologies. As user demand for encryption increases, these firms have become more invested in advocating for strong encryption in the name of protecting user privacy and security, at least insofar as this is in line with ensuring that their user base continues to engage with their products and services. Consequently, this group of firms are perhaps most constrained by considerations of how their consumer base perceives their actions. Increasing rates of corporate espionage from foreign adversaries and governments have also caused these firms to invest more heavily in encryption of their own systems.

Finally, the third sub-group consists of service providers responsible for the storage and/or transmission of encrypted data. The most salient groups are internet service providers and telecommunications companies. These firms are also often clients of vendors of cryptographic technologies, and typically operate at a national scale rendering them most constrained by sector-specific national regulations. These companies are often less visible in the public and thus do not face the same degree of public scrutiny compared to multinational technology corporations.

With respect to the cryptography debate, the most visible schism between firms has been between the second and third groups – multinational technology companies and service providers. For example, in 2013 an NSA program targeted at Internet communications and stored data of non-US persons was revealed; known as the Prism program, the leaked information made it clear that there were different levels of cooperation between companies

and the NSA in providing decrypted data[17]. Similarly, in relation to law enforcement, telecommunications providers have been noted to be more willing to allow access to stored data whilst companies such as Yahoo and Google have publicly pushed back on requests from law enforcement for user data[18].

5.1.3 Researchers

Cryptography researchers are distinctly split between those who work for government agencies, and those who don't. Prior to the 1970s, cryptography research was more or less exclusively the domain of the government. Agencies such as the NSA and the GCHQ built up the world's leading cryptography research groups, and to this day retain some of the best talent in this field. These researchers are under strict secrecy requirements; their research is classified and information about their activities is sparse.

However, during the 1970s cryptographers beyond the closed doors of these intelligence agencies began to emerge. The first of the Crypto conferences occurred in 1981, marking the first congregation of the emerging open cryptography community. David Chaum, one of the most notable early cryptography researchers and businessmen, started the International Association for Cryptologic Research around the same time[19]. An independent academic community began to take shape.

A distinct feature of the cryptography research community was its blend of traditional academics with non-traditional independent researchers, hobbyists, and hackers. The latter came to loosely identify with the label of 'cypherpunks', a movement that came to represent

[17] Greenwald, G., & MacAskill, E. (2013). NSA Prism program taps in to user data of Apple, Google and others. *The Guardian*. Retrieved from https://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data

[18] Landau, S. (2014a). Making Sense from Snowden, Part II: What's Significant in the NSA Surveillance Revelations. IEEE Security & Privacy.

[19] Levy, S. (2001). Crypto: How the code rebels beat the government--saving privacy in the digital age. Penguin.

principles of privacy, freedom from surveillance, and anonymity. Despite their distinctive activism streak, the lines were blurred between the cypherpunks and cryptography academics. Whitfield Diffie, one of the inventors of public-key cryptography, was a case in point of this. Diffie never held a formal academic position, and throughout his career has simultaneously been a prolific cryptography researcher as well as an active member of the cypherpunk movement. Daniel Bernstein is another illustrative example. The *Bernstein v. United States* case became a lightning rod event for the cypherpunk movement representing their battle for the freedom of speech; Bernstein continued on to become a professor of mathematics and computer science and contributes actively to the development of cryptographic protocols.

5.2 Phase 1: Emergence and promise [1970 -1980]

Prior to the 1970s, cryptography was considered the domain of government. Their motivations for pursuing cryptography were twofold – to protect national secrets, and to access information about their friends and foes deemed necessary for national security and foreign policy[20].

Then, in the 1970s, this began to change. Specifically, this changed with the invention of public key cryptography in 1976 by Whitfield Diffie and Martin Hellman, two Stanford researchers[21]. Public key cryptography was a pivotal breakthrough – it allowed two users who had never communicated with one another to be able to exchange information securely, without fear of eavesdroppers being able to decrypt their communications. This crucially meant that the ability to securely encrypt data was a much more scalable process and could be extended to a network of mere strangers who simply needed access to a common database of public keys. This, in essence, meant that the backbone of secure internet commerce and digital communications suddenly became feasible[22].

Two years later, three researchers at the Massachusetts Institute of Technology (MIT) – Ronald Rivest, Adi Shamir, and Leonard Adleman - developed the first implementation of public key cryptography, which came to be known as the RSA algorithm[23]. The trio also invented digital signatures, enabling authentication as a fundamental component of the public key system. Public key cryptography could now concretely be implemented as part of a commercial product for individuals and institutions.

[20] (Banisar, 1999; Committee to Study National Cryptography Policy et al., 1996; Levy, 2001)
[21] Diffie, W., & Hellman, M. (1976). New directions in cryptography. *IEEE Transactions on Information Theory*, *22*(6), 644–654.
[22] Whilst I will not focus on the specific reasons why public key cryptography was a breakthrough relative to the predominant use of private keys prior to, robust technical overviews can be found in: (Kahn, 1996)
[23] Rivest, R. L., Shamir, A., & Adleman, L. (1978). A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM*, *21*(2), 120–126.

Phase 1 – *emergence and promise* – was thus when the doors on cryptography were blown open to researchers and firms, much to the consternation of the government agencies who had previously held the reins of control over the technology. Two tense relationships emerged in this phase – between the researchers and the state (described in section 5.2.1.1), and between firms and the state (described in section 5.2.1.2). The dynamics of these tensions seed the conflicts to come in later phases of cryptography's development.

5.2.1 Relationships

5.2.1.1 Researchers <> State

The origins of modern cryptography research are embedded within the state. In the U.S., the government was for decades the exclusive owner of cryptography research, the primary employer of cryptography researchers, and the dominant user of cryptographic technologies. However, as we entered into phase 1, a parallel strand of cryptography research emerged beyond the state's direct control. This revived a familiar friction between researchers and the state – namely, the debate about when it is appropriate for certain domains of research to be classified in the name of national security.

The legal basis for government control of scientific information exists in a number of forms; one of the first pieces of legislation addressing cryptography was in fact a law passed in the 1920s prohibiting the publication of information about diplomatic codes and ciphers[24]. The creation of a category of information known as Restricted Data was established in the *Atomic Energy Act* of 1946 in relation to data on the manufacture or use of atomic weapons or related nuclear material. This came to be extended to cryptography research, which the military and intelligence community deemed a threat to national security should it be disseminated[25].

[24] Bamford, J. (1982). The Puzzle Palace: Inside the National Security Agency. Penguin.
[25] Relyea, H. C. (1994). Silencing science: National security controls and scientific communication.

Thus, when two Stanford researchers followed by three MIT researchers – none of whom had existing connections with or loyalties to the government's classified cryptography research community – publicly announced critical breakthroughs in cryptography, government defense agencies became concerned. As more researchers followed in the footsteps of Diffie, Hellman, and the RSA trio, this concern escalated into active efforts by the NSA to limit the conduct and dissemination of public research on cryptography[26].

The first target was the primary funder of public research on cryptography, the National Science Foundation (NSF). In 1977, the NSA approached Fred Weingarten, then-Director of the Division of Computer Research at the NSF. Weingarten was told that federal law gave the NSA exclusive control over the conduct of cryptography research; when Weingarten challenged this claim, the NSA backed down and instead offered to review NSF grant proposals related to cryptography. The NSF agreed to this, whilst also making a point of explaining that the work that the NSA considered most troublesome tended to be serendipitous findings from theoretical research in computer science, hence their efforts to monitor all research relevant to cryptography were doomed to be flawed[27].

The NSA simultaneously began targeting researchers, particularly those on the brink of sharing their work publicly. In July 1977 NSA employee Joseph Meyer wrote to the Institute for Electrical and Electronics Engineers (IEEE) ahead of their planned October conference at Cornell University, the International Symposium on Information Theory, which was slated to feature a number of papers on encryption. The letter began by noting that 'in the past months…various IEEE groups have been publishing and exporting technical articles on encryption and cryptology – a technical field which is covered by federal regulations'. Meyer

[26] These efforts are particularly well documented in: Shearer, J., & Gutmann, P. (1996). Government, cryptography, and the right to privacy. *Journal of Universal Computer Science*, *2*(3), 113–146.
[27] Weingarten, F. W. (1992). Cryptography and National Security. *Information Systems Security*, *1*(1), 9–12. https://doi.org/10.1080/19393559208551309

then proceeded to warn the IEEE that they would be in violation of the law should they allow these presentations to proceed: 'I suggest that IEEE might want to review this situation, for these modern weapons technologies uncontrollably disseminated could have more than academic effect'[28]. The conference organisers subsequently issued a letter to the academics scheduled to present at the conference to inform them of the situation. Nevertheless, the conference proceeded as organised. A number of universities explicitly supported their professors to present their research publicly despite the warnings. When the NSA raised alarm at the posting of hard copies of one of these papers globally MIT's lawyers stepped in to successfully challenge this claim[29].

The NSA had another tool up their sleeves – the *Invention Secrecy Act* of 1951 – which they began to use in 1978 in an attempt to classify cryptography products that were designed by researchers. The *Invention Secrecy Act* allows the Patent Office to forward applications to government agencies in a specific subject area of interest; the agency can then classify the proposal if they determine that it threatens national security. Previously this had only been applied to government researchers and researchers who had signed secrecy orders prior to conducting research. However, in 1978 the NSA tried to block two patents from non-government cryptography researchers. The first was filed by Professor George Davida from the University of Wisconsin. When Davida went public about this, the university chancellor publicly denounced the NSA for obstructing academic freedom. The NSA subsequently rescinded the order[30]. The second was filed by free-lance researcher Carl Nicolai; after an outcry in the media, the secrecy order was also rescinded[31].

---

[28] Pierce, K. J. (1984). Public Cryptography, Arms Export Controls, and the First Amendment: A Need for Legislation. Cornell International Law Journal, 17(1), 197.
[29] (Levy, 2001)
[30] Kruh, L. (1986). The Control of Public Cryptgraphy and Freedom of Speech - A Review. *Cryptologia*, *10*(1), 2–9.; Markoff, J. (1992). A Public Battle Over Secret Codes. *The New York Times*.
[31] Gilbert, L. A. (1982). Patent Secrecy Orders: The Unconstitutionality of Interference in Civilian Cryptography Under Present Procedures. *Santa Clara Law Review*, *22*, 325.

After a series of surreptitious and largely unsuccessful efforts, the NSA began a public campaign to promote restrictions on cryptography research. In 1979, Bobby Ray Inman delivered what came to be known as his 'The Sky is Falling' speech at the Armed Forces Communications Electronics Association conference. Inman issued a strong call for encryption to be born classified: 'there is a very real and critical danger that unrestrained public discussion of cryptographic matters will seriously damage the ability of the government to conduct signals intelligence'[32]. This was quickly criticised by the research community. The American Association for the Advancement of Science (AAAS) promptly passed a resolution condemning these restrictions as going against the "principles of openness that are a fundamental tenet of both American society and the scientific process"[33].

5.2.1.2 Firms <> State

Whilst the NSA was less concerned about the private sector at this point, in phase 1 we saw the emergence of both a synergy and conflict between firms and the state. The synergy was an increasing reliance on commercial actors to develop cutting edge cryptographic technologies; the conflict was an increasing desire on the part of the state to weaken the proliferation of strong cryptographic technologies beyond national borders.

The development of the Data Encryption Standard (DES) serves as a useful anecdote to illustrate both the synergy and the conflict. The DES was the first encryption standard established which was intended to be used both for the protection of unclassified government information as well as for use in the private sector, marking the beginning of the blurring between government and civilian tools for encryption. In 1975, the National Bureau of Standards (NBS, which became NIST in 1988) opened a call for candidate algorithms to be adopted as the DES. IBM was one of the only technology companies that

[32] Schneier, B., & Banisar, D. (1997). The electronic privacy papers: documents on the battle for privacy in the age of surveillance. John Wiley & Sons, Inc.
[33] (Schneier & Banisar, 1997)

existed at the time with cryptography research capabilities, housed within their T. J. Watson Research Lab. IBM submitted their Lucifer algorithm, which was adopted as the DES in July 1977[34].

After the initial submission of the Lucifer algorithm, at the insistence of the NSA, IBM was tasked to significantly weaken the algorithm by reducing the key size by over half and revising some of the internal workings of a component of the system known as 'S Boxes'. This raised controversy over the role of the NSA in tampering with the standard, subsequently discouraging many companies from adopting the standard once the DES was established. Many believed that the deliberate weakening of the DES was to enable it to be breakable by the NSA[35]. Indeed, many years later, the DES was broken by a brute-force attack carried out by the EFF on a device that was built for less than $250,000[36].

[34] (Banisar, 1999)
[35] (Landau, 2014b)
[36] Electronic Frontiers Foundation. (1998). Cracking DES: Secrets of Encryption Research, Wiretap Politics & Chip Design. O'Reilly Media.

5.3 Phase 2: Commercialisation and proliferation [1981 -1990]

During phase 2 – *commercialisation and proliferation* – a number of trends in the broader economy popularised cryptography, encouraging its dissemination into a range of commercial sectors. Financial services were increasingly expanding digitally and globally, creating demand for encryption. Increasing use of computers and computer networks created demands at the level of the individual citizen for privacy and security of their electronic records and transmissions. An increase in the use of wireless communication increased the vulnerability of unauthorised interception of these communications, thus demanding stronger encryption products. Private sector actors began to prioritise protection of proprietary information to defend themselves against corporate espionage[37].

As the demand for encryption increased, the academic field of cryptography also became more mainstream. Degree programmes in encryption and computer security began to spring up at computer science departments in universities, and more corporate jobs for cryptographers were available to graduates from these programmes as the need for these skills became more commonplace in the corporate environment[38]. This was a distinct change from phase 1, when the dominant if not only viable career route for a cryptographer was through working for a government intelligence agency.

Against this backdrop, the NSA continued to fight a losing battle to restrict the publication of cryptography research (section 5.3.1.1). Simultaneously, with the increase in private sector activity in cryptography, the NSA escalated its efforts to restrict firm activity (section 5.3.1.2).

[37] (Committee to Study National Cryptography Policy et al., 1996)
[38] (Banisar, 1999)

5.3.1 Relationships

5.3.1.1 Researchers <> State

In the early 1980s, the Reagan Administration bolstered the NSA's ability to restrict the publication of cryptography research. In April 1982 Executive Order 12356 was signed, eliminating the requirement that there be a balancing of national security and public interests before information could be classified[39]. In September 1984, NSDD-145 was approved, expanding the security classification system to encapsulate 'sensitive but unclassified data'[40]. The effect of both of these directives was to make NSA the primary gatekeepers for cryptography, telecommunications systems security, and information systems security issues. Specifically, it gave the NSA the authority to prescribe standards, methods, and procedures for restricting cryptographic material, techniques and information in the name of national security[41]. In an internal NSA memorandum from 1992, Clinton C. Brooks, then-Special Assistant to the Director of the NSA, indicated that the NSA had lobbied government to secure this authority: 'NSA engineered a National Security Decision Directive, NSDD-145, through the Reagan Administration that gave responsibility for the security of all U.S. information systems to the Director of the NSA, removing NBS from this'.[42]

However, as the decade progressed, the NSA showed signs of acknowledging that restricting the dissemination of research was an increasingly futile effort. In 1980, Leonard Adleman – one of the inventors of the RSA algorithm – applied for a grant from the NSF which included

---

[39] The White House. (1982). Executive Order 12356 —National security information. Retrieved from https://www.archives.gov/federal-register/codification/executive-order/12356.html

[40] (Office of the White House Press Secretary, 1984)

[41] For a brief moment, the NSA's remit was even broader under an additional directive issued by national security advisor Admiral John Poindexter. However, the directive was abruptly withdrawn after five months due to protests from industry and civil liberties groups; see: Sanger, D. E. (1987).Rise and Fall of U.S. Data Directive. *The New York Times*. Retrieved from https://www.nytimes.com/1987/03/19/us/rise-and-fall-of-us-data-directive.html
In that same year, the NSA proposed a system in which they would become the exclusive provider of all encryption equipment and keys for use within the U.S.; this, too, was faced with huge push back; see: Kolata, G. (1986). NSA to provide secret codes. *Science*, *230*, 45–47.

[42] (Schneier & Banisar, 1997)

some research on cryptography. Adleman reportedly received a call from the NSF stating that the NSA were insistent that they fund the portion of his grant on cryptography. Adleman was furious – 'in my mind, this threatened the whole mission of the university and its place in society' – and was prepared to go public before Inman himself called Adleman to apologise, claiming that this was a mistake. The NSA proceeded to allow the NSF to fund the entirety of Adleman's grant[43].

The only documented effort to establish a pre-publication review system for cryptography research was initiated during this period by Inman, who asked the American Council on Education to create a Public Cryptography Study Group to examine the issue of limits on academic research of encryption. Initially, the panel was asked to 'review the acceptability of restrictions on domestic dissemination of non-governmental technical information relating to cryptography'. The panel rejected this suggestion, opting instead for a voluntary system where researchers would provide their research to the NSA of their own volition. A large number of academics complied; reportedly, the NSA only made suggestions to under 10% of the submitted papers[44].

One notable case in which the NSA did demand that a paper be suppressed was in relation to work submitted by Ralph Merkle, then a research scientist at Xerox PARC. Merkle had developed a set of algorithms that would significantly speed up cryptographic computation. In the same paper that described this breakthrough, Merkle also discussed in detail the inner workings of the Lucifer algorithm that underpinned the DES[45]. The NSA demanded that this paper be suppressed; Xerox, Merkle's employer at the time, complied. However, a version of the paper was leaked on the internet via one of the reviewers of Merkle's paper who objected to the NSA order. The NSA consequently rescinded its request to withhold

[43] (Levy, 2001)
[44] American Council on Education. (1981). *Report of the Public Cryptography Study Group*. ACE.
[45] Merkle, R. (1991). Fast Software Encryption Functions. In *Advances in Cryptology* (p. 476).

publication. Many perceived this as acknowledgement that the ability for the NSA to restrict the publication of research was weakening in the face of a research community empowered by an open-source culture and the interconnectedness of the Internet.

5.3.1.2 Firms <> State

As we entered into phase 2, the conflict between the firms and the state escalated as the state – specifically the NSA – increasingly prioritised the goal of mitigating the proliferation of cryptographic technologies beyond the U.S. in the interests of national security. Following controversy over the DES, the NSA subsequently appeared to regret advocating for the DES and tried to discourage its dissemination. In a 1987 letter to the NBS, then-Deputy Director for Plans and Policy at the NSA Gerald R. Young stated that the widespread use of DES 'could motivate a hostile intelligence organisation to mount a large scale attack'.

The NSA's suggested replacement was the use of NSA-developed classified algorithms embedded in tamper-proof chips that would only be issued to 'approved organisations'. The program that developed these chips was called the Commercial Communications Security Endorsement Program (CCEP) and was, in effect, the NSA's attempt to directly sponsor equipment that would compete with the DES.

Industry organisations strongly opposed this effort – there was widespread suspicion that the NSA had built these systems to enable the NSA full access to their contents. Further, companies had already expended a large amount of money in implementing DES and were frustrated by the actions of the NSA to undermine its security and implementation. An announcement from the NSA that it would not support recertification of the DES at its five year review mark in 1988 particularly infuriated the private sector. A representative from the American Bankers' Association stated: 'our industry has lost valuable momentum in adopting improved security technology, and it still remains to be seen if we can overcome the damage

that has been done to the perceived security of DES-based technologies'[46]. In the end, the NBS recertified the DES in 1988 over NSA's objections[47].

However, outside of the public spotlight, a synergy between the NSA and some firms began to emerge. In the early 1980s, the NSA were coming to recognise that the private sector could meet the NSA's needs for cryptographic capabilities at a much lower cost. The CCEP was thus established primarily as a system through which private companies would build communications security technology with the NSA's blessing. Companies would propose a product, and the NSA would vet the proposal; if deemed sound, the company would work in partnership with the NSA to bring the product to market. CCEP's successor, the User Partnership Program (UPP), broadened this scheme out to include several defense agencies. Both programs were mutually beneficial for both parties: private companies could secure government clients and proceed with product development assured that the product was in line with government requirements, whilst the NSA could cut back on their costs as well as get a head-start on examining industry security products before they reached market[48]. This proved to be the early stages of a subsequent increasing reliance from government agencies on private sector expertise.

[46] (Banisar, 1999)
[47] (Diffie & Landau, 2010)
[48] (Landau, 2014b)

5.4 Phase 3a: Consolidation and contestation [1991 – 2000]

Modern cryptography underwent two phases of *consolidation and contestation*. Each is described here in turn as phase 3a and phase 3b. For each phase, a set of notable events is first described which establish the context for the relationships that evolve between the actors in that phase.

In the first wave of *consolidation and contestation* – phase 3a – the cryptography market became distinctly global and central to computer security. Encryption technology was more easily available to individuals and small businesses, whereas a decade ago such security was only available to government agencies and large technology companies. Key trends in the cryptography product market included the miniaturisation of products and the growth of hybrid software/hardware products. Both of these trends made encryption technology easier to install and use, decreasing the barrier to entry for individuals seeking security.

The DES and RSA algorithms were broadly considered two of the strongest algorithms on the market, and cryptography products implementing DES and RSA came to be widely available both domestically in the U.S. as well as abroad. Whilst U.S. firms held approximately 50% of the market share for cryptographic products internationally, reports from the Software Publishers Association (SPA) at the time cite 210 cryptographic products that were made outside of the U.S. (compared to 288 made in the U.S.). Federal government clients also decreased as a percentage of the market for cryptographic products relative to private sector and individual users[49].

The 1990s also saw the rise of the open-source movement in cryptography. Pretty Good Privacy (PGP) became the first widely used open-source encryption software utilising public key cryptography; it was easily downloadable from the Internet and became a popular tool for file encryption. Firms also began to find that open-source operating systems resulted in better

[49] Hoffman, L., Ali, F., Heckler, S., & Huybrechts, A. (1994). Cryptography policy. *Association for Computing Machinery. Communications of the ACM*, *37*(9), 109. https://doi.org/10.1145/182987.184079

reliability due to more rapid bug fixes and increased popularity of their systems due to convenient customisation. Open source software thus came to be a major element in the software marketplace, bolstered by the rapid growth of a community of computer enthusiasts and cypherpunks[50].

Nevertheless, surveys at the time indicated that the cryptography market still had room to grow. Surprisingly few users regularly used encryption technology, and many organisations were either unaware of the benefits of encryption or were wary of using encryption due to controversies in regulation at the time[51]. Section 5.4.1 runs through the notable events that characterised phase 3a of cryptography's development. Section 5.4.2 then proceeds to describe how these controversies manifested as conflicts between the state, firms, and researchers.

5.4.1 Notable events

5.4.1.1 The Digital Signature Standard

The development of a Digital Signature Standard (DSS) to protect unclassified, sensitive information held by government agencies and multinational corporations was one of the first actions assigned to NIST under the *Computer Security Act* (CSA) of 1989. The NIST/NSA technical working group that was established under the CSA began working on the standard; the NSA advocated for the FBI to join the working group.

NIST initially proposed to make the RSA algorithm the standard with the rationale that this was the preferred algorithm already in use by the majority of the market. The NSA pushed back on this – it was opposed to widespread use of something as strong as the RSA algorithm. Instead, the NSA proposed a classified DSS algorithm as an alternative. Under significant pressure from both the NSA and the FBI, NIST eventually adopted the NSA DSS proposal in August 1991. Upon the

[50] Diffie, W., & Landau, S. (2001). *The Export of Cryptography in the 20th Century and the 21st*. Retrieved from https://privacyink.org/pdf/export_control.pdf

[51] Pascoe, E. (1998). The average Net user wants more, not less government involvement in data protection. *The Independent (London)*.

announcement of the DSS, there was a strong negative reaction from industry groups. Over 100 companies, trade associations and individuals submitted comments to NIST, the vast majority of which were critical of the new DSS algorithm. Among the critiques were its lack of compatibility with the industry-preferred RSA algorithm. In spite of the overwhelmingly negative response, in May 1994 NIST formally announced the adoption of the DSS as a Federal Information Processing Standard (FIPS)[52].

5.4.1.2 Clipper chip I and II

As the debate about the DSS went on publicly, and NSA, FBI and DOJ coordinated to lobby the incoming Clinton Administration to advocate for a new approach to encryption that would provide strong protection for private communications but allow exceptional access to government agencies to intercept and decrypt communications on demand[53]. This approach was underpinned by a method of encryption known as key escrow which in essence made it possible for the keys needed to decrypt data to be held simultaneously 'in escrow' by a third party[54]. The standard that would implement this was the Escrowed Encryption Standard (EES) which was introduced in February 1993. The EES called for the integration of microelectronic integrated circuit chips called 'Clipper chips' into devices used for voice communications; these chips implemented a key escrow system that would provide exceptional access to law enforcement agencies.

On April 15, 1993, President Clinton signed Presidential Decision Directive 5 authorising the Clipper initiative[55]. In announcing the new initiative, President Clinton hailed this as a solution to the dual-use nature of encryption: 'The chip is an important step in addressing the problem of encryption's dual-edged sword: encryption helps the privacy of individuals and industry, but it can

[52] (Banisar, 1999; Landau, 2014b)
[53] For a detailed recount of efforts by the Nsa, FBI, DOJ, and to some extent the CIA in lobbying for the Clipper initiative, see: (Banisar, 1999; Levy, 2001)
[54] For a more detailed technical description of key escrow and the Clipper Chip initiatives, see: Denning, D. E., & Smid, M. (1994). Key escrowing today. *IEEE Communications Magazine*, *32*(9), 58–68.
[55] Office of the White House Press Secretary. (1993). Presidential Directive / NSC-5: Public Encryption Management. The White House. Retrieved from https://fas.org/irp/offdocs/pdd/pdd-5.pdf

also shield criminals and terrorists.' Whilst the Clipper initiative was established as a voluntary scheme, it included a number of elements to make it more palatable to industry in order to incentivise its uptake. Firstly, the encryption algorithm used on the chip – known as the Skipjack algorithm – would offer considerably more protection against brute-force attacks compared to the DES and was thus understood to be a much stronger encryption algorithm than what the industry was then allowed to export[56]. Relatedly, the State Department announced that it would relax export controls on products that contained Clipper Chips. NIST also announced that it would not reapprove DES in 1998, leaving Skipjack the only official government standard for protecting unclassified information[57].

The Clipper initiative was developed in secret until the date of signing. The first public news of its establishment was via a *New York Times* article reporting on an 'NSA-designed cryptosystem that would enable law enforcement access to the keys under court order'[58]. The proposal was met with extremely negative reactions from industry and civil liberties groups – its announcement in the Federal Register generated 320 comments, all of which were negative bar two. Notably, opposition came not just from outside of government, but also from within. Agencies such as the Department of Energy and the Nuclear Regulatory Commission submitted letters opposing adoption of the Clipper standard. Member of Congress, most notably Senator Patrick Leahy, vowed to fight Clipper in hearings held in May 1994[59]. A poll conducted by March 1994 found that 80% of the public opposed the Clipper proposal[60].

Criticisms of the Clipper initiative fell into three broad categories. Firstly, industry was sceptical of the ability to sell Clipper products beyond the U.S. – they believed that no foreign buyers would

[56] In the summer of 1993, an independent study conducted by a group of researchers led by Dorothy Denning published a report confirming the strenght of the Skipjack algorithm.
[57] (Committee to Study National Cryptography Policy et al., 1996)
[58] Markoff, J. (1993a). Electronics Plan Aims to Balance Government Access with Privacy. *The New York Times.*; Markoff, J. (1993b). Communication Plan Draws Mixed Reaction. *The New York Times.*
[59] (Landau, 2014b; Levy, 2001)
[60] Dewitt, P. E. (1993). Who should keep the keys? *TIME.*

want products that had built-in backdoors for U.S. law enforcement and security agencies. The Computer System Security and Privacy Advisory Board, a NIST-appointed federal advisory committee, was publicly critical of the effort, citing concerns about the difficulty of marketing Clipper products abroad. Secondly, civil liberties groups feared that the proposed system would be a forerunner to universal surveillance despite it being voluntary at the time. Declassified FBI files that were subsequently released in 1995 confirmed the agency's intention to move in that direction[61]. Finally, researchers at AT&T found that the key forfeiture mechanism built into the Clipper chips could easily be bypassed, undermining the technical robustness of the system[62].

By late 1995, the Clipper initiative was generally acknowledged to have failed. Aside from the 9,000 Clipper-enabled devices that the DOJ had agreed to purchase from AT&T in order to seed the market, fewer than 8,000 other Clipper-enabled devices were sold[63]. With the failure of this first attempt at promoting key escrow, the NSA and NIST began joint work with Georgetown University and Trusted Information Systems (a private security company) to develop a software mechanism similar in function to the Clipper chip. This came to be known as Clipper II. The key distinction was that this time, the keys would be held by a 'trusted third party' instead of a government agency; this was termed the 'key recovery' approach. These trusted third parties could be compelled to provide the keys to appropriate law enforcement officials if presented with a warrant[64].

---

[61] (Shearer & Gutmann, 1996)

[62] Blaze, M. (1994). Protocol failure in the escrowed encryption standard. In *Proceedings of the 2nd ACM Conference on Computer and Communications Security* (pp. 59–67). ACM.; Markoff, J. (1994). Scientist Insists U.S. Computer Chip Has Big Flaw. *Detroit Free Press*.; Quittner, J. (1994). U.S. Nears Standard on Coding Messages. *Newsday*.

[63] (Landau, 2014b)

[64] Singleton, S. (1998). *Encryption Policy for the 21st century: A future without government-prescribed key recovery*. Cato Institute Policy Analysis. Retrieved from https://www.cato.org/publications/policy-analysis/encryption-policy-21st-century-future-without-governmentprescribed-key-recovery

In July 1996, then-Vice President Al Gore announced Clipper II[65]. Again, to incentivise industry participation, the announcement included a relaxation of export controls for products that implemented the key recovery system. Companies were given two years to comply.

The reception from industry was uniformly negative. Representatives from several of the largest hardware manufacturers and software publishers claimed that the proposal still promoted weakened encryption through the use of short keys and key forfeiture. A group of the world's leading cryptography experts published a landmark paper in 1977 detailing the major technical limitations of any key escrow or key recovery scheme[66]. Thirteen leading computer and software manufacturers, including Intel, Microsoft and Sun Microsystems, retaliated by proposing an alternative to the key recovery proposal based on a system of 'private doorbells'[67]. Ultimately, Clipper II suffered a similar fate to Clipper I, with limited uptake both domestically and internationally[68].

5.4.1.3 The battle over export controls

A key lever in the government's control of encryption since the 1970s has been export controls. The *Arms Export Control Act* (AECA) of 1976 authorised the DOD and other government agencies to regulate dual-use products, including encryption software and hardware. For those that did not classify as munition under the AECA, the *Export Administration Act* (EAA) of 1979 gave the DOC the ability to regulate encryption products. Strong encryption products thus required explicit approval from the state; in practice, such exemptions were rarely granted[69]. This resulted in a two-

[65] Gore, A. (1996). Administration Statement on Commercial Encryption Policy. Retrieved from https://www.epic.org/crypto/key_escrow/wh_cke_796.html
[66] Abelson, H., Anderson, R. J., Bellovin, S. M., Benaloh, J., Blaze, M., Diffie, W., … Schiller, J. I. (1997). The risks of key recovery, key escrow, and trusted third-party encryption. *World Wide Web Journal*, *2*(3), 241–257.
[67] Helwich, D. (2001). Cryptography, critique and power: A critical inquiry into the federal encryption regulation controversy.
[68] Global Internet Liberty Campaign. (1998). Cryptography and Liberty 1998: An International Survey of Encryption Policy. Retrieved from http://gilc.org/crypto/crypto-survey.html
[69] (Singleton, 1998)

tiered system of export-grade cryptography. Within the U.S., strong cryptography was permitted; however, only cryptography of a substantially weaker grade could be exported abroad[70].

As private sector interests in cryptography increased across the 1990s, so did the industry's opposition to the export control regime. Studies cited losses in the scale of hundreds of millions of dollars in sales to foreign competitors. A landmark report from the National Research Council came down firmly against strict export control of cryptographic products, concluding that not only did export control laws limit the ability for U.S. companies to retain market dominance but they also reduced the domestic availability of strong encryption due to many U.S. vendors only investing resources into developing one export-grade product line[71]. Another National Research Council report warned that "if the U.S. does not allow vendors of commercial systems to export security products and products with relatively effective security features, large multinational firms as well as foreign consumers will simply purchase equivalent systems from foreign manufacturers"[72]. Many companies had reportedly resorted to using foreign subsidiaries to provide strong encryption, including the likes of Network Associates, RSA Data Security Inc., and Sun Microsystems[73].

Members of Congress stirred into action in the early 1990s, most notably Representatives Maria Cantwell and Sam Gejdenson. In October 1993, Cantwell and Gejdenson held a subcommittee hearing to draw attention to the problem. Notably, a testimony from Steve Walker, a former NSA official, referred to statistics that demonstrate how widespread cryptographic products were beyond U.S. borders: 'The U.S. government is succeeding only in crippling a vital American industry's exporting ability'[74]. Cantwell prepared the *Legislation to Amend the Export Administration*

---

[70] Buchanan, B. (2016). Cryptography and Sovereignty. *Survival*, *58*(5), 95–122. https://doi.org/10.1080/00396338.2016.1231534

[71] (Committee to Study National Cryptography Policy et al., 1996)

[72] National Research Council. (1991). *Computers at Risk: Safe Computing in the Information Age*. Washington, DC: The National Academies Press. Retrieved from https://www.nap.edu/catalog/1581/computers-at-risk-safe-computing-in-the-information-age

[73] Proctor, P., & Byrnes, C. (1999). The politics of cryptography. Performance Computing, 17(11), 25–29.

[74] (Levy, 2001)

Act of 1979 in November 1993; if passed, the bill would substantially relax export regulations on public-domain encryption software. Two days before the bill went to vote, then-Vice President Al Gore wrote to Cantwell indicating that the Administration was about to put forward a proposal for a key recovery system that would, in effect, achieve what her bill proposed. Cantwell subsequently dropped her bill.

Years later, the Clinton Administration took a number of steps to significantly relax export controls on encryption products. On September 16, 1998, Al Gore announced reforms to the export control regime that would allow U.S. companies to export encryption products to their overseas subsidiaries. The reforms also streamlined the licensing review process and brought the key-length requirements closer to marketplace realities for international encryption standards[75]. Both law enforcement officials and industry representatives expressed support for these reforms[76]. In January 2000, the White House announced further substantive changes to the cryptographic export control regime that would provide U.S. companies much greater freedoms in exporting cryptographic products, specifically those intended for retail use. This marked the end to a long battle over export controls – industry opposition ended, as did congressional attempts to modify the export control regime[77].

5.4.2 Relationships

5.4.2.1 Firms <> State

The events described in section 5.4.1 are clear demonstrations of the state's primary goal – that of limiting the proliferation of strong cryptographic technologies beyond national borders, motivated by national security concerns – and of the state's persistent willingness to exercise their legislative

[75] Gore, A. (1998). Holds news briefing on encryption.
[76] (Helwich, 2001)
[77] Christie, R. (2000). U.S. limbers up for encryption sales: Companies are cheered as rules are eased on exporting privacy software. *Financial Times (London)*.; Crocker, T. E. (2000). Decoding rules of encryption: The ins and outs of new regulations governing exports. *Legal Times*.; Sanger, E., & Clausing, J. (2000). U.S. removes more limits on encryption. *The New York Times*.

capacity to pursue this goal. This was in opposition to the main goal of firms – to be able to gain global market share via proliferation of commercial cryptographic technologies – forming the basis of conflict between firms and the state. In the promulgation of the DES and DSS, the state opted for standards that were not in line with industry preferences, creating additional compliance costs for firms. Throughout the Clipper I and II debates, firms consistently opposed these initiatives primarily on the grounds that key escrow products would not gain traction with foreign buyers and would undermine the security of their systems.

Export controls became the primary battleground between firms and the state. The export control regime for cryptographic products prior to the reforms in 2000 posed a number of challenges to firms. For one, the degree of regulatory uncertainty about how the export control laws would be enforced was a consistent source of frustration. It was unclear to firms which foreign companies were subject to U.S. export control laws nor how broad or narrow the definition of cryptographic products was. It was often not possible for firms to find out in advance of submitting a product for review; hence, firms faced the possibility that entire product lines that they had invested in may end up being restricted to the domestic market. The reasoning behind a license request being rejected was also often classified and firms had no ability to appeal the decisions made. This had the effect of forcing firms into conservative planning scenarios and product development that drove towards the 'lowest common denominator' cryptographic solution, resulting in weak cryptographic products on the domestic market.

With time, the harm caused to the U.S. industry by the export control regime became a point of consensus among firms and portions of the state apparatus. The Computer Systems Security and Privacy Advisory Board, a federal body, stated that 'current controls are negatively impacting U.S. competitiveness in the world market and are not inhibiting the foreign production and use of cryptography'[78]. The Committee for the Study of National Cryptography Policy, led by then-

[78] (Hoffman et al., 1994)

Deputy Secretary of State Kenneth W. Dam, concluded that 'U.S. export controls have had a negative impact on the cryptographic strength of many integrated products with encryption capabilities available in the U.S.', recommending that the government promote widespread commercial use of cryptography[79]. Even the FBI conceded that 'the use of export controls may well have slowed the speed, proliferation, and volume of encryption products sold in the U.S'.[80] Thus, whilst the conflict raged across the 1990s, the conclusion of the export controls debate by 2000 was largely perceived to have swung in favour of firms.

However, a synergy between firms and state continued to exist outside of the public eye when it came to the state relying on commercial technologies for the pursuit of their goals. AT&T, for example, was a critical enabler for the Clipper initiatives by agreeing to incorporate the chips into their product line to enable the first batch of sales. Trusted Information Systems, a private security company, worked closely with NIST to develop the key recovery proposal which became Clipper II. Thus, for the firms less constrained by public scrutiny of their actions, cooperation with the government remained an attractive strategy for their goal of pursuing profit.

5.4.2.2 Researchers <> State

Whilst researchers were much less of a focal point in the debate during phase 3a, specific events driven by researchers had substantial influence on the discourse. Notably, researchers tended to side with industry interests throughout this phase. For example, during the backlash against the Clipper initiatives, a petition organised by the Computer Professionals for Social Responsibility (CPSR) group gathered nearly 50,000 signatures, primarily from two camps – leading cryptography researchers and leading computer security professionals[81].

[79] (Committee to Study National Cryptography Policy et al., 1996)
[80] (Committee to Study National Cryptography Policy et al., 1996)
[81] (Landau, 2014b)

Insofar as there was direct conflict between researchers and the state, they were matters related to the export control regime – specifically in relation to the export of technical data. Technical data related to cryptography was regulated by the same export control laws that regulated cryptographic products and encapsulated cryptographic algorithms that were described in a manner that was not machine-executable. The same regulatory uncertainty that plagued firms also troubled academic institutions and researchers. They were unclear, for example, whether activities like discussing cryptography with a foreign citizen, teaching courses on cryptography that involve non-U.S. graduate students, or allowing foreign citizens residing in the U.S. to work on source code for cryptographic products were illegal under the regime[82].

Two cases are often cited as examples of the export control regime unnecessarily restricting the actions of researchers. First was the case of Pretty Good Privacy (PGP), spearheaded by free-lance software programmer Philip Zimmermann. Zimmermann was prompted to release PGP as an act of retaliation against what he perceived as an impending tightening of government control of cryptographic technologies[83]. PGP was thus released in 1991 as an open-source program used to encrypt mail messages end-to-end; a subsequent improved version of PGP was released in 1992 with the support of what had at that point become a truly international group of contributors, ranging from Amsterdam to Auckland. In 1993, Zimmermann became the target of a criminal investigation based on a possible violation of export control laws; the case was eventually dropped in 1996[84].

The second was the case of Daniel Bernstein who in 1995 had developed an encryption algorithm that he wished to publish and implement in the form of a computer program intended for distribution. He was prevented from doing so under export control laws and thus filed a suit against the government seeking to challenge their ability to bar the restriction of publications of

[82] (Committee to Study National Cryptography Policy et al., 1996)
[83] (Buchanan, 2016; Levy, 2001)
[84] Cocoran, E. (1996). U.S. Closes Investigation in Computer Privacy Case. *Washington Post*.

cryptographic documents and software. Bernstein's case rested on the claim that the export control regime was an "impermissible prior restraint on speech, in violation of the First Amendment". At both the district court level and in the Appeals court for the Ninth Circuit, Bernstein's case won. Judge Betty Fletcher from the Ninth Circuit court issued a landmark defense of cryptography as a vital component of democracy: "Government attempts to control encryption…may well implicate not only First Amendments rights of cryptographers, but also the constitutional rights of each of us as potential recipients of encryption's bounty."[85] The case was escalated to the Supreme Court but has since been indefinitely postponed. Nevertheless, in both cases, it would appear that researchers won against the state in staking claim to their right to publish and disseminate cryptography research.

[85] (Diffie & Landau, 2010)

5.5 Phase 3b: Consolidation and contestation [2001 to present]

The beginning of the twenty-first century marked the end of the what came to be known as the 'Crypto-wars' – the flurry of conflict, legislation and protest surrounding the events of phase 3a. As we entered into the second phase of *consolidation and contestation* - phase 3b – the consensus at least within the U.S. was that civil liberties and business interests had prevailed. The proliferation of strong encryption had become an agenda that even the security and law enforcement agencies had emerged in support of, in large part because they recognised the futility of trying to prevent the dissemination of software products and algorithms.

As the dust settled, cryptographic technologies of increasing sophistication were being developed and disseminated around the world with little regulatory friction. More competition thus meant that American products became a decreasing proportion of the market share internationally. A survey conducted in 2016 of the worldwide market for encryption products found 865 hardware or software encryption products on the market from 55 different countries; 546 of these products were from outside the U.S. The vast majority of the products were produced by private companies, indicating that cryptography had well and truly shifted from being controlled by governments to being developed and deployed by commercial actors. Notably, of these products 66% were based on proprietary technologies whilst 34% were open source[86].

Cryptography continued to grow into an active research field in which new encryption techniques continued to be developed, standardized, and deployed. NIST launched a call for the development of an Advanced Encryption Standard (AES) to replace DES; the winner was announced in 2000, awarded to an algorithm from a Belgian team, and AES was adopted as a standard in 2001[87]. A common way to use AES, called AES-Galois, was developed in 2005. AES came to become widely

[86] Schneier, B., Seidel, K., & Vijayakumar, S. (2016). *A Worldwide Survey of Encryption Products*. Retrieved from https://www.schneier.com/academic/paperfiles/worldwide-survey-of-encryption-products.pdf
[87] (National Academies of Sciences, Engineering, and Medicine, 2018)

used around the world as one of the strongest standardised algorithms. Indeed, by 2016 there was no detectable difference in the advertised strength of encryption products produced within versus outside of the U.S. – the liberalisation of export controls by the end of phase 3a had demonstrably worked to harmonise these standards between the domestic and international markets[88]. Further modern cryptographic breakthroughs include a new method of encrypting credit card data called format-preserving encryption, which was standardized in 2013. Public key ciphers designed to withstand quantum computers are now being developed; they are expected to be standardized by the mid-2020s[89].

Despite the friendly regulatory environment and the advancement of the technology, cryptography did not see the explosion in usage that many expected. Analysts attribute this to the lack of uniform standards – the market is fragmented amongst several non-interoperable suites of cryptographic algorithms, at least partially inherited from the two-tiered export grade cryptography system promulgated by the U.S. until the late 1990s. Countries outside the U.S. have also begun to seriously invest in national cryptography systems as a component of their national security strategies. Europe reportedly undertook a broad program to develop cryptographic tools to support the region's information security needs, and China commenced the development of new families of cryptographic systems[90]. The rise of modern cyber threats and economic espionage has made this need more salient as states – most notably Russia and China – have turned to cyberattacks and cyber exploitation as tools of statecraft[91]. The more that nation states pursue cryptography as a national tool for security, the less likely it is that internationally interoperable cryptographic standards will be established.

[88] (Schneier et al., 2016)
[89] (National Academies of Sciences, Engineering, and Medicine, 2018)
[90] (Diffie & Landau, 2010)
[91] (Buchanan, 2016; Lin, 2016)

We now turn to notable events which reignited debates around cryptography development, deployment, and regulation. Some have coined this recent period 'Crypto-wars II' as many of the same dynamics between firms, researchers, and the state have re-emerged. Section 5.5.1 runs through a description of these events and their relevance to the cryptography debate. Section 5.5.2 proceeds to analyse how the impacts of these events manifested in the relationships between the actors.

5.5.1 Notable events

5.5.1.1 Snowden revelations

The leaking of Edward Snowden's documents revealed multiple strategies deployed by the NSA to subvert encryption across and beyond the U.S. The most prominent was a highly classified decryption program called Bullrun. The objective of the Bullrun program was to crack encryption of online communications and data, targeting widely used online protocols such as HTTPS, voice-over-IP and Secure Sockets Layer (SSL)[92]. The NSA appeared to utilise a number of methods, including computer network exploitation, industry relationships, and collaboration with foreign intelligence entities[93].

The Snowden leaks also revealed a number of large scale efforts by the NSA to intercept and collect data, including: the bulk collection of domestic telecommunications metadata[94] and internet communications[95]; the targeting of internet communications and stored meta-data of non-U.S.

[92] Ball, J., Borger, J., & Greenwald, G. (2013). Revealed: how US and UK spy agencies defeat internet privacy and security | US news. *The Guardian*. Retrieved from https://www.theguardian.com/world/2013/sep/05/nsa-gchq-encryption-codes-security

[93] Koops, B.-J., & Kosta, E. (2018). Looking for some light through the lens of "cryptowar" history: Policy options for law enforcement authorities against "going dark." *Computer Law & Security Review*, *34*(4), 890–900. https://doi.org/10.1016/j.clsr.2018.06.003

[94] Greenwald, G. (2013). NSA collecting phone records of millions of Verizon customers daily. *The Guardian*. Retrieved from https://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order

[95] Poitras, L., & Greenwald, G. (2013). NSA whistleblower Edward Snowden: "I don't want to live in a society that does these sort of things" – video. *The Guardian*. Retrieved from https://www.theguardian.com/world/video/2013/jun/09/nsa-whistleblower-edward-snowden-interview-video

persons[96]; the targeted collection of data on close U.S. allies[97]; and the collection of inter-datacentre traffic from both Google and Yahoo[98].

In September 2013, it was further revealed that the NSA had strategically sought to undermine strong encryption by creating backdoors in numerous hardware and software products; instead of advocating publicly for key escrow, they had instead been engineering exceptional access surreptitiously[99]. One primary way in which the NSA sought to achieve this was in compromising the Secure Hash Algorithm (SHA) standard[100]. In 2007, NIST announced a competition to replace the hash standard SHA-1 whose weaknesses had become evident in recent years[101]. In 2012, a winner was announced to be SHA-3; however, in August 2013, NIST proposed an abbreviated version of the winning algorithm that would diminish the algorithm's robustness, to the consternation of industry and researchers alike[102]. The Snowden documents revealed that this was the doing of the NSA, who had engineered to subvert the standard by proposing a weak random bit generator in the hash algorithm (NSA's random bit generator had been demonstrated to be vulnerable by two Microsoft researchers back in 2007[103]). The New York Times thus reported that

---

[96] Greenwald, G., & MacAskill, E. (2013). NSA Prism program taps in to user data of Apple, Google and others. *The Guardian*. Retrieved from https://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data

[97] SPIEGEL Staff. (2013). Embassy Espionage: The NSA's Secret Spy Hub in Berlin. *Spiegel Online*. Retrieved from http://www.spiegel.de/international/germany/cover-story-how-nsa-spied-on-merkel-cell-phone-from-berlin-embassy-a-930205.html

[98] Gellman, B., & Soltani, A. (2013). NSA Infiltrates Links to Yahoo, Google Data Centers Worldwide, Snowden Documents Say. *Washington Post*. Retrieved from https://www.washingtonpost.com/world/national-security/nsa-infiltrates-links-to-yahoo-google-data-centers-worldwide-snowden-documents-say/2013/10/30/e51d661e-4166-11e3-8b74-d89d714ca4dd_story.html

[99] Meinrath, S. D., & Vitka, S. (2014). Crypto War II. *Critical Studies in Media Communication*, *31*(2), 123–128. https://doi.org/10.1080/15295036.2014.921320; Simonite, T. (2013). NSA's Own Hardware Backdoors May Still Be a "Problem from Hell." *MIT Technology Review*. Retrieved from https://www.technologyreview.com/s/519661/nsas-own-hardware-backdoors-may-still-be-a-problem-from-hell/

[100] (Ball et al., 2013)

[101] Wang, X., Yin, Y. L., & Yu, H. (2005). Finding collisions in the full SHA-1. In *Annual international cryptology conference* (pp. 17–36). Springer.

[102] Kelsey, J. (2013). *SHA3: Past, Present, and Future*. Presented at the Workshop Cryptographic Hardware and Embedded Systems. Retrieved from https://csrc.nist.gov/CSRC/media/Projects/Hash-Functions/documents/kelsey_ches2013_presentation.pdf

[103] Shumow, D., & Ferguson, N. (2007). *On the Possibility of a Back Door in the NIST SP800-90 Dual Ec Prng*. Retrieved from http://rump2007.cr.yp.to/15-shumow.pdf

the NSA worked to 'insert vulnerabilities into commercial encryption systems' and 'influence policies, standards and specifications for commercial public key technologies'[104].

5.5.1.2 The 'Going Dark' debate

In December 2015, the city of San Bernardino in California witnessed a terrorist attack. Fourteen people were shot to death, and many were severely injured. The culprits were a couple – Rizwan Farook and Tafsheen Malik – who were killed in a police shootout that same day. It emerged in the subsequent investigation that the FBI were in possession of an iPhone that belonged to Farook; however, they were unable to examine its contents due to the device being encrypted. When the FBI requested that Apple decrypt the iPhone, Apple refused to comply. The FBI proceeded to take Apple to court. In February 2016, the District Court of the Central District of California ordered Apple to provide 'reasonable technical assistance to assist law enforcement agents in obtaining access to the data [on the device]'. Apple opposed, claiming that this equated to a request for them to build a version of their iOS that would create a backdoor in their system, therein undermining 'the basic security and privacy interests of hundreds of millions of individuals around the globe' in possession of an iPhone. In March 2016, the FBI withdrew its motion to compel Apple's assistance having reportedly found an alternative means of obtaining access to the phone[105].

The *Apple v. FBI* case revived the debate on appropriate controls on cryptography, triggering a number of bills being introduced in Congress[106]. Critically, the case became a lightning rod event in what had already been an escalating conflict between technology firms and law enforcement with respect to encryption. Following Snowden, there was a wave of announcements from major

---

[104] The New York Times. (2013). Secret Documents Reveal N.S.A. Campaign Against Encryption. *The New York Times*. Retrieved from https://archive.nytimes.com/www.nytimes.com/interactive/2013/09/05/us/documents-reveal-nsa-campaign-against-encryption.html

[105] (Koops & Kosta, 2018)

[106] Lichtblau, E., & Benner, K. (2017). Apple Fights Order to Unlock San Bernardino Gunman's iPhone. *The New York Times*. Retrieved from https://www.nytimes.com/2016/02/18/technology/apple-timothy-cook-fbi-san-bernardino.html; Schulz, W., & Van Hoboken, J. (2016). *Human Rights and Encryption* (UNESCO Series on Internet Freedom). UNESCO. Retrieved from http://unesdoc.unesco.org/images/0024/002465/246527E.pdf

technology companies that they would imminently be strengthening encryption on their products and services. In September 2014 Apple announced that it would include default encryption on its devices in iOS 8[107]; Google followed suit by announcing that Lollipop, the next version of the Android operating system, would enable encryption by default[108]. In November 2014 WhatsApp announced that it would support an end-to-end encryption protocol[109] and in March 2015 Yahoo introduced source code for an extension that encrypts messages in Yahoo Mail[110]. This caused grave concern amidst the U.S. intelligence and law enforcement communities[111]. James Comey, then-Director of the FBI, coined this as the 'Going Dark' problem, claiming that law enforcement's interception channels were progressively, and rapidly, becoming inaccessible, 'leaving the government at a dead end'[112]. This narrative was being echoed in the UK simultaneously, triggered by the Charlie Hebdo attacks in Paris on January 7, 2015. A few days after the attacks, Prime Minister David Cameron took a firm stance on enabling government access to communications[113].

The FBI stirred into action to put forward proposals for exceptional access for law enforcement. The likes of Comey and then-Director of the NSA Admiral Mike Rogers framed these proposals as 'front doors', pre-empting retaliation to the well-treaded controversy around the use of government backdoors: 'We aren't seeking a back-door approach. We want to use the front door,

---

[107] Sanger, D. (2014). Signaling Post-Snowden Era, New iPhone Locks Out N.S.A. *The New York Times*. Retrieved from https://www.nytimes.com/2014/09/27/technology/iphone-locks-out-the-nsa-signaling-a-post-snowden-era-.html

[108] Timberg, C. (2015). Newest Androids will join iPhones in offering default encryption, blocking police. *Washington Post*. Retrieved from https://www.washingtonpost.com/news/the-switch/wp/2014/09/18/newest-androids-will-join-iphones-in-offering-default-encryption-blocking-police/

[109] Greenberg, A. (2014). Whatsapp Just Switched on End-to-End Encryption for Hundreds of Millions of Users. *Wired*. Retrieved from https://www.wired.com/2014/11/whatsapp-encrypted-messaging/

[110] Stamos, A. (2015). User-Focused Security: End-to-End Encryption Extension for Yahoo Mail. Retrieved from https://yahoo.tumblr.com/post/113708033335/user-focused-security-end-to-end-encryption

[111] Gasser, U., Gertner, N., Goldsmith, J., Landau, S., Nye, J., O'Brien, D. R., … Zittrain, J. (2016). *Don't Panic: Making Progress on the "Going Dark" Debate*. The Berkman Center for Internet & Society.

[112] Comey, J. B. (2014). *Going Dark: Are Technology, Privacy, and Public Safety on a Collision Course?* Presented at the Brookings Institution, Washington, D.C. Retrieved from https://www.fbi.gov/news/speeches/going-dark-are-technology-privacy-and-public-safety-on-a-collision-course

[113] Watt, N., Mason, R., & Traynor, I. (2015). David Cameron pledges anti-terror law for internet after Paris attacks. *The Guardian*. Retrieved from https://www.theguardian.com/uk-news/2015/jan/12/david-cameron-pledges-anti-terror-law-internet-paris-attacks-nick-clegg

with clarity and transparency, and with clear guidance provided by law'.[114] It was suggested that Silicon Valley companies could become partners to the intelligence and law enforcement communities by providing 'golden keys for their cryptographic systems'[115]. It was never made clear what this would look like in technical implementation.

After approximately a year of heated debate, the White House declared in October 2015 that it would not pursue a legislative solution to addressing the rise of encryption on communications devices[116]. This was partially in response to growing pressure on President Obama from industry to issue a statement strongly disavowing a legislative mandate and supporting widespread encryption[117]. Analysts saw this as a win for industry, leaving the FBI in a position of needing to encourage companies to voluntarily comply with law enforcement requests[118].

5.5.2 Relationships

5.5.2.1 Firms <> States

There are two distinct facets of the relationship between firms and the state during phase 3b. The first is a synergy arising from the state's increasing dependence on commercial technologies for the implementation of national security goals. The second is a conflict in the form of firms being

[114] (Comey, 2014)
[115] Nakashima, E., & Gellman, B. (2015). As encryption spreads, U.S. grapples with clash between privacy, security. *Washington Post*. Retrieved from https://www.washingtonpost.com/world/national-security/as-encryption-spreads-us-worries-about-access-to-data-for-investigations/2015/04/10/7c1c7518-d401-11e4-a62f-ee745911a4ff_story.html
[116] Perlroth, N., & Sanger, D. (2015). Obama Won't Seek Access to Encrypted User Data. *The New York Times*. Retrieved from https://www.nytimes.com/2015/10/11/us/politics/obama-wont-seek-access-to-encrypted-user-data.html; The White House. (2015). *NSC Draft Options Paper on Encryption*. Retrieved from https://www.scribd.com/document/281807768/NSC-Draft-Options-Paper-on-Encryption
[117] Nakashima, E., & Peterson, A. (2015a). Obama faces growing momentum to support widespread encryption. *Washington Post*. Retrieved from https://www.washingtonpost.com/world/national-security/tech-trade-agencies-push-to-disavow-law-requiring-decryption-of-phones/2015/09/16/1fca5f72-5adf-11e5-b38e-06883aacba64_story.html
[118] Nakashima, E., & Peterson, A. (2015b). Obama administration opts not to force firms to decrypt data – for now. *Washington Post*. Retrieved from https://www.washingtonpost.com/world/national-security/obama-administration-opts-not-to-force-firms-to-decrypt-data--for-now/2015/10/08/1d6a6012-6dca-11e5-aa5b-f78a98956699_story.html; Wittes, B. (2015). The Obama Administration's Encryption Wrangling. Retrieved August 14, 2018, from https://www.lawfareblog.com/obama-administrations-encryption-wrangling

unwilling to be seen to cooperate with government in the pursuit of activities which the public, and specifically their consumers, deemed to be violations of civilian privacy and security.

Increasing state dependence on commercial technologies

At the turn of the century, the synergy between government agencies and private technology companies was growing steadily. From the perspective of the government agencies, this was motivated by a need to partner with the private sector in order to gain access to commercial cryptographic technologies; this was seen as the only way for them to retain their technological advantage. The *Information Technology Management Reform Act* of 1996 had made it a requirement for the military to use commercial off-the-shelf technologies (COTS) where possible. This mandate appeared to be embraced wholeheartedly by the NSA. In a 2002 keynote speech at the annual Black Hat computer security conference, then-NSA technical director Richard George laid out a clear intention to cooperate with the commercial sector: 'We have a responsibility to do everything we can to work with U.S. industry to make U.S. products the best in the world; to make U.S. security products the products of choice world-wide'.[119] Programs such as the User Partnership Program (UPP) and the Commercial Solutions for Classified (CSfC) initiative concretely sought to integrate commercial products into government technologies[120].

The private sector and government also began to acknowledge that their security needs were increasingly converging to be one and the same. By 2005, it had become evident that cyberattacks were being launched not only at the U.S. government and defense contractors such as Lockheed Martin and Northrop Grumman, but also at firms across all industries, ranging from Disney in entertainment and Exxon Mobil in energy to consumer-oriented multinational companies such as Google, Yahoo, and Sony[121]. When Google discovered that it had been hacked, the company even

[119] George, R. (2002). Keynote Address by Richard George, Technical Director, Security Evaluations Group, National Security Agency. Presented at the Black Hats Briefing.
[120] Roeper, F., & Ziring, N. (2012). Address by Fred Roeper, Technical Director, National Security Agency & Neal Ziring, Technical Director, National Security Agency. Presented at the RSA Conference 2012.
[121](Landau, 2014b)

turned to the NSA for help in securing its systems[122]. In a 2015 *Washington Post* op-ed, former NSA Director Mike McConnell, former DHS Secretary Michael Chertoff, and former Deputy Defense Secretary William Lynn summarised this interdependence as a necessity[123]:

> Strategically, the interests of US businesses are essential to protecting US national security interest…if the United States is to maintain its global role and influence, protecting business interests from massive economic espionage is essential.

Both the emergence of a shared threat and the growing reliance on a shared technology base meant that the NSA, at least visibly, occupied a more consistent stance in support of strong encryption. For example, in 2003 the AES was approved for the protection of all levels of classified traffic. Further, in 2005 the NSA announced a full suite of public algorithms – 'Suite B' – as the approved standard for the protection of all levels of classified information. The government's increasing use of unclassified algorithms acknowledges that in an increasingly interconnected world, interoperability between civilian and military infrastructure had become critical. The NSA also hoped that this would lower the cost of acquiring security equipment as they became increasingly reliant on private firms to produce military products. This was the case for elliptic curve cryptography (ECC) – a public-key cryptographic approach developed by Neal Koblitz and Victor Miller – which came into wide use in 2004 and 2005[124]. The NSA subsequently paid Certicom, the company who owned the ECC patents, $25 million to license the technology such that it could be used to develop products for national security[125]. Clearly, phase 3b marked a new equilibrium

[122] Drummond, D. (2010). A new approach to China. Retrieved from https://googleblog.blogspot.com/2010/01/new-approach-to-china.html
[123] McConnell, M., Chertoff, M., & Lynn, W. (2015). Why the fear over ubiquitous data encryption is overblown. *Washington Post*. Retrieved from https://www.washingtonpost.com/opinions/the-need-for-ubiquitous-data-encryption/2015/07/28/3d145952-324e-11e5-8353-1215475949f4_story.html
[124] Koblitz, A. H., Koblitz, N., & Menezes, A. (2011). Elliptic curve cryptography: The serpentine course of a paradigm shift. *Journal of Number Theory*, *131*(5), 781–814.
[125] (Diffie & Landau, 2010)

between the NSA and the industry based on their aligned goals of deploying strong encryption systems within and beyond U.S. borders[126].

The firm push-back on state cooperation

Then, the Snowden revelations and the *Apple v. FBI* case abruptly reversed this narrative of cooperation to one of conflict. Silicon Valley companies were pitched against the government – specifically the NSA and FBI – and both sides adopted a publicly adversarial stance toward the other[127]. Tim Cook, the CEO of Apple, was an archetypical voice of industry during this period. In a 2014 announcement about Apple's decision to strengthen its encryption systems, Cook stated: 'I want to be absolutely clear that we have never worked with any government agency from any country to create a backdoor in any of our products or services. We also have never allowed access to our servers. And we never will'.[128] He framed the *Apple v. FBI* case as a broader battleground between industry and the government – 'We feel we must speak up in the face of what we see as an overreach by the U.S. government' – and translated this into resistance on a number of cases during those years where Apple was being ordered to decrypt iPhones for law enforcement purposes[129]. In March 2016, over 40 technology companies including Facebook, Google, Microsoft, and LinkedIn filed amicus briefs in support of Apple's stance[130].

The Snowden revelations shed light on a schism between firms, some of whom were willing to cooperate with the government, and some of whom were adamantly against it. A number of the

[126] Landau, S. Testimony for House Judiciary Committee Hearing on "The Encryption Tightrope: Balancing Americans" Security and Privacy"," § House Judiciary Committee (2016a). Retrieved from https://judiciary.house.gov/hearing/the-encryption-tightrope-balancing-americans-security-and-privacy/
[127] Bankston, K. (2015). West Coast vs. East Coast. *Slate Future Tense*. Retrieved from http://www.slate.com/articles/technology/future_tense/2015/02/yahoo_s_alex_stamos_and_nsa_s_mike_rogers_fight_about_encryption.html?wpsrc=sh_all_dt_tw_top; Bennett, C. (2015). Silicon Valley spars with Obama over "backdoor" surveillance. *The Hill*. Retrieved from http://thehill.com/policy/cybersecurity/236512-silicon-valley-spars-with-obama-over-backdoor-surveillance
[128] Cook, T. (2014). A message from Tim Cook about Apple's commitment to your privacy. Retrieved from https://www.apple.com/privacy/
[129] The Economist. (2016). Taking a bite at the Apple. *The Economist*. Retrieved from https://www.economist.com/science-and-technology/2016/02/27/taking-a-bite-at-the-apple
[130] Sircar, S. (2017). The Crypto Wars: Interpreting the Privacy Versus National Security Debate from a Standards Perspective. Georgetown University, Washington, D.C.

revelations revealed how the NSA was surreptitiously tapping into private companies' systems against their will, and often without their knowledge. The Prism program, for example, was a large-scale NSA effort to obtain data from U.S. companies. Yahoo was reportedly threatened by the U.S. government with a fine of $250,000 per day if it did not join the program; a number of companies claimed to have been unaware of their data being obtained until the Snowden revelations. The private company that was hosting Edward Snowden's encrypted email account, Lavabit, was ordered by the FBI to turn over its SSL private keys; the service decided to suspend its operations in order to avoid having to do so[131].

In response to the Snowden revelations, a number of technology companies introduced stronger encryption in their products and services seemingly to defend themselves against government intrusion. Apple announced that it was introducing end-to-end encryption, as did a number of other private companies[132]. Google accelerated their efforts to encrypt inter-datacentre communication; Yahoo and Microsoft announced the intention to do the same[133]. Companies such as Yahoo and Google have become more active in contesting orders from law enforcement under FISA and have been pressing for permission to publish transparency reports on the number of government requests they receive for data. U.S. companies such as Cisco and Verizon Communications have also reported financial losses as a result of the Snowden revelations due to a lack of trust among foreign customers, further aggravating their relationship with the state[134].

---

[131] Schneier, B. (2015). Data and Goliath: The hidden battles to collect your data and control your world. WW Norton & Company.

[132] Van Hoboken, J., & Rubinstein, I. (2013). Privacy and security in the cloud: Some realism about technical solutions to transnational surveillance in the Post-Snowden Era. *Maine Law Review*, *66*, 487.

[133] Fung, B. (2013). Even after NSA revelations, Yahoo won't say if it plans to encrypt data center traffic. *Washington Post*. Retrieved from https://www.washingtonpost.com/news/the-switch/wp/2013/10/30/even-after-nsa-revelations-yahoo-wont-say-if-it-plans-to-encrypt-data-center-traffic/; Timberg, C. (2013). Google Encrypts Data Amid Backlash against NSA Spying. *Washington Post*. Retrieved from https://www.washingtonpost.com/business/technology/google-encrypts-data-amid-backlash-against-nsa-spying/2013/09/06/9acc3c20-1722-11e3-a2ec-b47e45e6f8ef_story.html; Timberg, C., Gellman, B., & Soltani, A. (2013). Microsoft, suspecting NSA spying, to ramp up efforts to encrypt its Internet traffic. *Washington Post*. Retrieved from https://www.washingtonpost.com/business/technology/microsoft-suspecting-nsa-spying-to-ramp-up-efforts-to-encrypt-its-internet-traffic/2013/11/26/44236b48-56a9-11e3-8304-caf30787c0a9_story.html

[134] (Schneier, 2015)

Conversely, the Snowden revelations also revealed several instances of firms cooperating with the intelligence and law enforcement communities, rarely challenging demands for broad collection of metadata and in some cases providing unlimited access to their underseas cables[135]. Indeed, throughout the SHA-3 debacle, Reuters reported that the NSA had struck an agreement with RSA Data Security Inc. for $10 million to make their weak random bit generator a default component in their products[136]. Beyond Snowden, a survey in 2010 found that 1,931 private corporations were actively working on intelligence and counter-intelligence projects and that 70% of the U.S. intelligence budget was spent on contracts with private firms. Companies have been reported to be building cyberweapons for states, and there remains a strong revolving door between the personnel at this subset of private firms and government agencies[137]. This web of cooperation remains mostly out of the public spotlight, and thus less subject both to public criticism as well as sensitivity to events such as the Snowden revelations.

5.5.2.2 Researchers <> State

As the second round of the Crypto-wars commenced, leading cryptography researchers moved into playing a similar role to that from the 1990s – that of activism, largely in support of the industry's stance and against the government's stance. The *Apple v. FBI* case particularly brought researchers to the fore, with well-known figures such as Susan Landau and Bruce Schneier coming out strongly against the court's orders for Apple to comply[138]. Landau in particular made a case for why the *Apple v. FBI* case was illustrative of the FBI's need to invest in better surveillance capabilities that do not rely on weakening encryption systems[139]; her argument was corroborated

[135] Landau, S. (2013). Making Sense from Snowden: What's Significant in the NSA Surveillance Revelations. IEEE Computer and Reliability Societies.
[136] Menn, J. (2013). Exclusive: Secret contract tied NSA and security industry pioneer. *Reuters*. Retrieved from https://www.reuters.com/article/us-usa-security-rsa/exclusive-secret-contract-tied-nsa-and-security-industry-pioneer-idUSBRE9BJ1C220131220
[137] (Schneier, 2015)
[138] (Gasser et al., 2016; Sircar, 2017)
[139] Landau, S. (2016b). The real security issues of the iPhone case. *Science*, *352*(6292), 1398. https://doi.org/10.1126/science.aaf7708

in a post hoc analysis by the DOJ identifying the FBI's failure to mobilise investigative powers and resources[140].

In the revival of the key escrow debate, a notable contribution from the research community was a study conducted by several of the world's leading cryptographers concluding that backdoor proposals 'are unworkable in practice, raise enormous legal and ethical questions, and would undo progress on security at a time when Internet vulnerabilities are causing extreme economic harm'.[141] The study specifically criticises the notion of exceptional access to cryptographic systems as a 'U-turn from the technical best practices now being deployed to make the Internet more secure', thus putting critical infrastructure at higher risk of attack from bad actors. Whilst consensus among researchers was unequivocally against exceptional access, academics have been to some extent cooperative with government efforts as well. Several computer scientists proposed possible technologies for exceptional access, and researchers have been engaging in due process to evaluate the integrity of such proposals[142]. Thus, as with firms, researchers willing to cooperate with the government exist, but largely not in the public eye.

---

[140] Landau, S. (2018). Revelations on the FBI's Unlocking of the San Bernardino iPhone: Maybe the Future Isn't Going Dark After All. Retrieved from https://www.lawfareblog.com/revelations-fbis-unlocking-san-bernardino-iphone-maybe-future-isnt-going-dark-after-all; Office of the Inspector General. (2018). *A Special Inquiry Regarding the Accuracy of FBI Statements Concerning its Capabilities to Exploit an iPhone Seized During the San Bernardino Terror Attack Investigation*. U.S. Department of Justice. Retrieved from https://oig.justice.gov/reports/2018/o1803.pdf

[141] Abelson, H., Anderson, R., Bellovin, S. M., Benaloh, J., Blaze, M., Diffie, W., … Neumann, P. G. (2015). Keys under doormats: mandating insecurity by requiring government access to all data and communications. *Journal of Cybersecurity*, *1*(1), 69–79.

[142] Bellovin, S. M., Blaze, M., Boneh, D., Landau, S., & Rivest, R. L. (2018). Analysis of the CLEAR Protocol per the National Academies' Framework. Retrieved from https://mice.cs.columbia.edu/getTechreport.php?techreportID=1637; Levy, S. (2018). Can This New Encryption Method Finally Crack the Crypto War? *Wired*. Retrieved from https://www.wired.com/story/crypto-war-clear-encryption/

5.6 Analysis and discussion

The life cycle of modern cryptography has gone through four phases of development and deployment – notably, two heated periods of *consolidation and contestation* featuring high-profile clashes between the U.S. government, technology firms, and to a lesser extent, cryptography researchers. Section 5.6.1 and Table 5.6-1 offer a summary of how the actors evolved across the technology life cycle. Section 5.6.2 and Table 5.6-2 proceed to summarize the relationships that developed between these actors.

5.6.1 The evolution of the actors

The state's primary goal was consistently the preservation of national security. As the phases progressed, however, their strategy evolved. During phases 1, 2 and 3a, preventing the proliferation of strong cryptographic technologies beyond U.S. borders was the primary mandate of the state. However, as the market for cryptographic technologies became increasingly global and open-source, the state turned towards a strategy of encouraging the development and integration of commercial technologies in order to strengthen the domestic technology base, implicitly acknowledging the futility of their attempts at halting the proliferation of cryptographic technologies.

The willingness of the state to exercise its legislative capacity increased over time, driven by the growing salience of the perceived national security threat. Conversely, the importance of the state as an R&D funder became less relevant as the technology matured and non-state actors developed the capacity to carry out cryptography R&D. As these efforts came to compete with the NSA's closed cryptography community, the state turned towards the private sector for its innovation capacity. A corollary of the field shifting from public to private hands is that in the state's efforts to retain some semblance of control and influence over private activities, their interventions came under increasing public scrutiny.

Firms maintained a goal of maximising profit from the commercialisation and proliferation of cryptographic technologies, and consistently held an edge over other actors in possessing leading innovation capacity in pursuit of this goal. However, particularly in phase 3b, the importance of public concern in shaping the actions of firms increasingly constrained their activities, particularly for consumer-facing multinational technology firms. For firms who operated largely out of the public eye – namely service providers and small vendors of cryptographic technologies – this constraint was less applicable. As firms sought expansion into global markets, they also found that they were increasingly constrained in doing so by the legislative environment created by the state.

The emergence of a community of cryptography researchers independent of the NSA was pivotal to kickstarting modern cryptography. However, beyond phase 1, researchers played a relatively minor role in the development and deployment of cryptography. The importance of their innovation capacity decreased as the bulk of the activity in cryptography shifted from fundamental research to products and applications. Nevertheless, the independent cryptography research community remains lively to this day, particularly in defending civil liberties associated with cryptographic technologies and in many ways channelling public concerns with respect to the behaviour of firms and the state.

5.6.2 The evolution of actor relationships

The most prominent arc of the story of cryptography is the escalation of conflict between the state and firms, and to some extent between the state and cryptography researchers.

Between the state and firms, the conflicts began to emerge in phase 2 and intensified in phases 3a and 3b. At first, the vendors of cryptographic products were the actors pushing back against state control of their proprietary technologies, particularly in efforts to restrict the proliferation of their products beyond national borders. This later became multinational technology corporations who were huge users of cryptographic technologies, and thus pushed back against state control of how

they were to use cryptographic technologies particularly vis a vis supporting intelligence and law enforcement activities. On both of these fronts, it would appear that firms had won against the state in pushing for liberalised export controls in phase 3a and limited compulsory government access to decrypted data in phase 3b.

Between the state and researchers, from phase 1 there was already a strong rift between the incentives for non-government researchers to publish their research, and the desire for the state to control cryptography research and restrict its dissemination beyond U.S. borders. The state was quick to acknowledge that their efforts to restrict the publication of cryptography research were destined to be unsuccessful; by phase 2, the NSA had turned most of their attention to addressing the dissemination of cryptographic products from private firms, leaving the cryptography research community to pursue work largely unmonitored. As conflicts between firms and the state began to heat up in phases 3a and 3b, researchers came in indirect opposition to the state via playing the role of advocating for strong encryption. The researcher community became synonymous with representing the principles of privacy and freedom of speech, markedly influenced by the *Bernstein v. United States* case and their membership of the cypherpunks movement.

For both firms and researchers, a distinctive undercurrent in the narrative is one of willing cooperation with the state despite the public-facing conflicts. A sub-set of firms – predominantly service provider companies and security companies – participated in state programs and complied with state requests related to cryptography. Thus, as the state became more reliant on the private sector for the provision of cryptographic capabilities and decrypted data, they found willing cooperation among some private actors. Similarly, researchers were willing to comply with the voluntary pre-publication review scheme demanded by the NSA, and were often willing technical advisers to the state, whether that be to members of Congress or the intelligence and law enforcement agencies.

Table 5.6-1: Summary of evolution of actors

		State	*Firms*	*Researchers*
Goals		Economic growth ↑ Military leadership = Risk mitigation =	Maximise profit =	Pursue research =
Resources and constraints	*R&D funding*	Resource ↓	Resource ↑	Constraint =
	Innovation capacity	Resource ↓	Resource ↑	Resource ↓
	Legislative environment	Resource ↑	Constraint ↑	(Constraint)
	Public concern	Constraint ↑	Constraint ↑	Resource =

Notes:
↑ means that the goal / resource / constraint becomes more advantageous / constraining as the technology matures
↓ means that the goal / resource/constraint becomes less advantageous / constraining as the technology matures
= means that the goal / resource / constraint remains constant as the technology matures
() means that the goal / resource / constraint is irrelevant in this case

Table 5.6-2: Summary of evolution of relationships

	Synergies	*Conflicts*
State <> *Firms*	State depends on access to commercial technologies ↑	State prevents firms from proliferating technologies ↑ Firms face public backlash for selling technologies to the state ↑
State <> *Researchers*	State creates supportive R&D environment ↓	State prevents researchers from proliferating knowledge and talent ↑
Firms <> *Researchers*	Firms creates supportive R&D environment ↑	(Researchers clash with firms on issues of ethics and societal consequences)

Notes:
↑ means that the synergy / conflict becomes stronger as the technology matures
↓ means that the synergy / conflict becomes weaker as the technology matures
() means that the synergy / conflict is irrelevant in this case

6 Squaring theory with history

The tales of aerospace technology, biotechnology, and cryptography are deeply nuanced. Indeed, recall the differences between the case studies, as evidenced in the preceding chapters: from the conditions necessary for their emergence, to the drivers of commercialization, and ultimately the culmination of politics between the actors.

Nevertheless, there is also a tale of commonality that binds these cases together. This is a tale of a strategic GPT that is of deep interest to states, firms, and researchers. This is tale of the synergies and conflicts that emerge given these sometimes aligned, sometimes competing interests. This thus becomes a tale which claims that, underpinning the nuance, there are common trends and outcomes which describe a predictable pattern of politics surrounding the emergence, proliferation, and maturation of this reference class of strategic, general purpose technologies.

A general version of this tale is captured in the model introduced in Chapter 2. The model follows a life cycle of a strategic GPT. It focuses on three actors – the state, firms, and researchers. Each actor is defined by their goals, resources and constraints. The model then analyses the relationships between these actors – specifically, the synergies and conflicts that emerge between them as their goals, resources and constraints interact.

In this chapter, the cases of aerospace technology, biotechnology, and cryptography are held up against this model. In section 6.1, we examine how accurate the model was in capturing the evolution of the actors and actor relationships that emerged across the course of these case studies. Then, in section 6.2, we critique the model by identifying missing contextual factors which systematically explain the instances where history deviated from the theory. Section 6.3 summarises and looks ahead to how it may be applied to the contemporary case of artificial intelligence.

6.1 What was accurate about the model?

6.1.1 The evolution of actors

In the model, there are four common resources and constraints that describe each actor's capacity and inclination to act. These are: research and development (R&D) funding; innovation capacity; the legislative environment; and public concern. The model maps how these resources become more or less advantageous for an actor, and how these constraints become stronger or weaker, across the technology life cycle.

R&D funding is a resource that both states and firms have access to, and a constraint that applies to researchers. The model predicts that states begin as the primary providers of R&D funding given their larger appetite for risk relative to firms in the emergence and promise phase. However, as the technology matures, the state is replaced by firms as the dominant funders of R&D either through in-house expenditure or through external private investments or acquisitions. Researchers remain consistently constrained by their dependence on an external source of R&D funding yet find themselves constrained in different ways depending on the strings that come attached with public versus private sources of funding.

The case studies strongly validate these trends in R&D funding. In the emergence and promise phase, the aerospace industry benefitted from substantial amounts of state funding, largely tagged for defense R&D. As the Cold War came to an end, the contraction of state funding for aerospace programs was offset by the steady influx of private investments as the aerospace industry turned towards commercial and civilian applications. Biotechnology saw a similar transition at the turn of the commercialization and proliferation phase. In large part triggered by the landmark *Diamond v. Chakrabarty* case and the consequent uptick in biotechnology patents, firms rapidly scaled up their investments in biotechnology R&D,

quickly dwarfing the amounts provided by the state. The shift from public to private funding was less stark in the case of cryptography, perhaps due to the small amounts of funding required to fuel early-stage cryptography R&D. Nevertheless, early-stage federal funding for cryptography research carried out within the NSA and at academic institutions was soon replaced by private R&D funding as researchers themselves started up companies such as RSA Security Inc. and as publicly available research was integrated into proprietary cryptography products by established technology firms such as IBM.

Innovation capacity refers to the ability of an actor to push the frontier of technology development and deployment. The model describes researchers as those with critical innovation capacity in the emergence and promise phase of the technology, when fundamental research is necessary and disproportionately important for fueling technological progress. The state may also initially have access to innovation capacity via government labs or within-agency R&D programs. As the field and industry grows, the capacity to conduct applied research at scale and to translate research into products and applications becomes a priority. This is the forte of firms, and rarely of researchers nor the state; hence in the model, innovation capacity increases for the former and decreases for the latter two actors.

This trend was corroborated most clearly in the case of biotechnology. As the technology life cycle progressed into the commercialization and proliferation phase, the frontiers of innovation were increasingly being pushed by biotechnology start-ups and the multinationals that acquired them, rather than the academic labs which generated the fundamental breakthroughs in genetic engineering and recombinant DNA. Cryptography saw a similar shift from pure mathematical research carried out by the likes of Whitfield Diffie and Martin Hellman at Stanford towards the development of cryptographic standards and integrated products at IBM's Thomas J. Watson Research Center (better known as the IBM Watson Lab). The core of innovation in the aerospace industry shifted increasingly away from in-

house NASA and DOD programs and towards the research teams at industry giants such as Lockheed Martin and Boeing, and later towards new firms such as SpaceX and Blue Origin.

The model describes the ability to shape the *legislative environment* is a resource unique to the state, and their willingness to do so increases as the technology industry matures. Firms and researchers are naturally constrained by the legislative environment in which they operate, more so as they scale in size and importance. While these trends were consistently observed in the case studies, the drivers for increased legislation varied. For the aerospace industry, the perceived rise of China as a threat to U.S. dominance in outer space spurred congressional attention and more restrictive legislation on the export of satellites. For the biotechnology industry, the uptick in legislative activity was in large part triggered by elevated biosecurity concerns in the wake of the 2001 Amerithrax attacks and a string of dual-use experiments across the early 2000s. For cryptography, legislation increased in light of the growing cybersecurity threat paired with the state's fears of their intelligence sources 'going dark' due to encryption.

The model describes *public concern* as a constraint on state and firm behavior. Researchers were modelled to act as a channel for public concerns, thereby making this a resource for gaining influence. However, the case studies were inconclusive on the importance of public concern as either a constraint or resource for these actors. Certainly, growing public concerns about bioterrorism increased pressure on the U.S. government to more closely regulate the biotechnology industry, and growing public fears of privacy infringements caused cryptography firms to take explicit stances against cooperating with the FBI or NSA. As such, there is something to be said for public concern being a constraint insofar as for the state it represents voter opinion, and for firms it represents consumer and user preferences. However, these trends were not sufficiently consistent across the case studies to warrant much confidence in this component of the model.

6.1.2 The evolution of actor relationships

As the actors interact, the model posits synergies and conflicts that emerge between pairs of actors. These either become stronger or weaker as the technology life cycle progresses, driven by how each actor evolves in terms of their goals, resources, and constraints.

Between states and firms, the *state's dependence on access to commercial technologies* is a synergy that becomes stronger as the technology matures, and as innovation capacity shifts away from the state and state-funded researchers towards firms. An underpinning driver is the state's pursuit of military leadership, which equates to the integration of cutting edge technologies into the military technology base. As firms begin to dominate the R&D pipeline for producing such leading technologies, the state responds with attempts to increase their access to firm technologies. NASA and DOD, for example, began to lease capacity from commercial satellites and introduced new policies to enable contracting for the delivery of space launch and transportation services through commercial partners. Similarly, government schemes such as Project BioShield placed biotechnology firms central to achieving the state's biosecurity strategy. In cryptography, the Commercial Communications Security Endorsement Program (CCEP) and the User Partnership Program (UPP) were introduced as of phase 2 in order to enable the state to access commercial technologies to serve its national security goals.

The conflict of the *state preventing firms from proliferating technologies* also strengthens with time. This is fueled by the perceived looming security risks – in the case of aerospace this was China; in the case of biotechnology this was bioterrorism; and in the case of cryptography this was cyber threats and foreign espionage. As the state moves to mitigate these security risks, they turn to halting the proliferation of technologies to global markets and potential adversaries. They are increasingly willing and able to do so via exercising their ability to shape the legislative environment that constrains the actions of firms. A common legislative tool

used was export controls – the U.S. government tightened rules around the export of satellites, cryptography products, and materials for conducting biotechnology R&D. The case of cryptography featured several more tools used by the state in this vein, including the use of the Invention Secrecy Act to seize security-relevant patents, and covert lobbying by the NSA to promote weaker encryption standards such as the Data Encryption Standard (DES), the Digital Signature Standard (DSS), and the infamous Clipper I and II schemes.

The hypothesis that *firms would face public backlash for selling technologies to the state* proved to be only weakly validated by the case studies. In the cases of aerospace technology and biotechnology, this conflict did not emerge between the state and firms. In the case of cryptography, there was indeed substantial public criticism of the activities of the NSA and of firms that cooperated with the U.S. government in the wake of the Snowden leaks and the *Apple v. FBI* case.

When it came to the relationship between the state and researchers, the *state creating a supportive R&D environment* is a synergy that weakens with time as state R&D funding decreases, and the research community turns more towards industry support. Indeed, in all three cases, the decrease in state funding as a proportion of overall R&D funding meant that while the state appeared to remain supportive of researchers, their role in creating a thriving R&D environment lost salience. Conversely, between firms and researchers, the *firms creating a supportive R&D environment* is a synergy that strengthens with time, evidenced by the influx of private capital into the research community and the establishment of university-industry relationships, most notably in the case of biotechnology.

The *state also seeks to prevent researchers from proliferating knowledge and talent,* increasingly so as the technology matures and as security risks from dual-use research become more salient. In the case of biotechnology this took the form of explicit legislation as part of the PATRIOT Act and Bioterrorism Preparedness Act which introduced deemed export control rules and visa

restrictions on foreign researchers engaged in biotechnology. Beyond explicit legislation, the state also promoted a range of softer governance tools to manage the design and publication of dual-use research of concern (DURC) by, for example, establishing the National Science Advisory Board for Biosecurity (NSABB), restricting funding for Gain of Function (GOF) experiments, and encouraging research institutions to establish Institutional Review Boards (IRBs) and Institutional Biosafety Committees (IBCs). In the early phases of the cryptography case, the state – specifically the NSA – sought to prevent the proliferation of cryptography research via several means, including the use of a pre-publication review system, private pressure on researchers to retract publications and conference papers, and implementing restrictions on NSF cryptography grants. The Pretty Good Privacy (PGP) and Bernstein cases are two particularly well-known demonstrations of this conflict in action.

Between firms and researchers, *researchers clashing with firms on issues of ethics and societal consequences* did not emerge as a conflict in the cases of aerospace technology and cryptography. In the case of biotechnology, this conflict manifested in the debate surrounding the patenting of biotechnology research, with researchers and firms clashing on issues such as the levels of openness and collaboration in biotechnology R&D environments, and whether large-scale projects such as the Human Genome Project should be allowed to be patentable by private firms.

6.2 Where did the case studies deviate from the model?

There were several instances where the case studies deviated from the model's predicted patterns of politics. Analyzing these deviations reveal elements that are missing from the model. Specifically, there are three contextual factors that explain these deviations: whether a technology originated from defense versus civilian priorities; the role that the state plays as a technology consumer; and the differential treatment of firms by the public and by researchers.

6.2.1 Contextual factor #1: Defense versus civilian origins

The first factor concerns the origins of the technology at the *emergence and promise* phase – specifically, whether the technology was initially conceived of by the state as a defense technology versus being seeded by researchers and/or firms as a civilian technology. Whether a technology originated as 'defense-first' versus 'civilian-first' shapes several components of the model; the most important effect is on the prioritization and sequencing of the state's goals of economic growth, military leadership, and risk mitigation.

For example, aerospace technology was clearly defense-first. The Space Race was fundamentally about bolstering national security and U.S. military leadership, and the earliest applications of aerospace technology – telecommunications and satellite navigation – were founded to serve defense needs first, prior to finding civilian and commercial demand. This meant that for the state, the goals of military leadership and security risk mitigation were at the forefront since the very beginning; conversely, the goal of pursuing aerospace technology for its economic value emerged later.

Cryptography was also a defense-first technology insofar as it was incubated covertly within the NSA, originally to support wartime efforts. These origins clearly shaped the state's priorities, despite modern cryptography being independently seeded in public academic

institutions. As in the case of aerospace technology, the state prioritized security risk mitigation and to a lesser extent military leadership form the beginning; capturing the economic value of cryptographic technologies barely featured as a salient state goal.

Biotechnology, on the other hand, is a civilian-first technology. The foundations of the industry were built on public research –funded by the state, but in a hands-off manner. The state consequently prioritized economic growth as a goal; risk mitigation became a central focus much later, and largely due to raised biosecurity and bioterrorism concerns. It is worth noting, too, that in the case of biotechnology there was an early establishment of an international norm against the development and use of offensive biological weapons via the Biological Weapons Convention. This strongly disincentivized states from pursuing the goal of military leadership for decades; it has only been in recent years that the DOD and DARPA have proceeded to invest in biotechnology.

Beyond the difference in the sequencing and salience of the state's goals, there may be further flow-on effects of distinguishing between defense-first versus civilian-first technologies. It is plausible that for defense-first technologies, for example, one could expect the state to be more invested in preventing the proliferation of security-relevant products and research; as such, the conflicts centered around this between the state, firms and researchers would be more prominent. One can also imagine that for civilian-first technologies, firms and researchers would be less constrained by the legislative environment because the state could be less willing to exercise constraints on industries that are prima facie not central to national defense and security interests. Unfortunately, evidence from the case studies is insufficient at this stage to test such hypotheses robustly.

6.2.2 Contextual factor #2: The state as a critical technology consumer

Of all the cases, aerospace technology deviated the most from the model. A contextual factor that contributed to this is the structure of the aerospace industry – namely, that the commercial viability of the aerospace industry necessitates the active participation of the state as a consumer of aerospace technologies.

With rare exception, aerospace firms rely on government contracts in order to sustain their business. This includes the new wave of aerospace firms such as SpaceX and Blue Origin: despite their crafted public image of distinguishing themselves from traditional contractors, and despite their stated goals of pioneering civilian space tourism, they currently compete for NASA contracts alongside the Boeings and the Lockheed Martins. This dependence on the state as a consumer does not hold true for cryptography firms nor biotechnology firms – in both industries the proportion of revenue sourced from the government is minor.

This contextual factor affects several components of the model. At a high level, the main effect is to increase the relative power of the state as an actor, meaning that its resources are more advantageous, and its constraints are less restrictive. For example, state funds for aerospace R&D remained relevant for longer. Further, the state's lack of innovation capacity proved to be less of a concern given its direct and assured access to the innovation capacity of aerospace firms. The aerospace industry is also heavily regulated – partially because the state has stronger incentives to legislate, and partially because the deployment of aviation technologies prior to outer space technologies meant that there was already regulatory groundwork laid for the aerospace industry. Public concern over state activities in outer space is also less of a constraint given the mainstream view that the aerospace industry is, by its nature, wedded to serving the state's interests, whatever those may be.

Conversely, firms and researchers are, in relative terms, less capable of wielding their resources and are more constrained. For one, the continued heavy involvement of the state as R&D funders means that firms and researchers are more restricted in pursuing R&D and commercialization activities that are not in line with the state's interests. We see this in the early phases of the technology life cycle where, for example, aerospace researchers worked exclusively on militarily-relevant projects, and aerospace firms could only pursue the development of satellite technology with support and funding from the state. A more restrictive legislative environment also implies that the state is more likely to succeed in passing legislation that goes against the interest of firms and researchers, as observed in the case of export controls on satellite technology. Finally, the public would tend to view aerospace firms and researchers as aligned with and embedded within the state; hence, public concern becomes largely irrelevant in shaping their behavior.

6.2.3 Contextual factor #3: Inconsistent critique of firms

The model proposes three related claims:

- *Claim 1*: that public concern is an important constraint on firms and a meaningful resource for researchers to channel;
- *Claim 2*: that firms will face public backlash for selling technologies to the state; and
- *Claim 3*: that conflicts would emerge between researchers and firms on ethical and social grounds.

The case studies provide only weak evidence for any one of these claims, as highlighted in section 6.1. This gestures towards a missing contextual factor – the differences in expectations of firms. Across the case studies, there were two types of firms that emerged – firms that were comfortable selling technologies to the state, and firms that weren't. The

default assumption should be that firms would sell their products to the state, given their goal of pursuing profit and thus seeing government demand as a market opportunity.

However, *claim 2* hypothesizes that for some firms, the public would take issue with the firm providing their products to the state, hence some would choose not to do so. Further, *claim 3* also hypothesizes that researchers would similarly take issue and thus constrain firms from selling to the state. These claims are both underpinned by *claim 1,* which is that firms are meaningfully constrained by public views of their actions, and that researchers seek to channel public concerns as a mechanism of influence against firms. While these claims proved to be true in some instances, there were several exceptions to the rule. These exceptions can be explained by challenging the comprehensiveness of these claims and pointing out where they may not apply to specific types of firms.

In the instance of *claim 1,* it proved to be that only some firms were meaningfully constrained by public concern. Take the case of cryptography, for example. Large consumer-facing technology companies such as Apple and Google were certainly responsive to public concern; however, the less visible service providers and infrastructure operators were not so, resulting in the latter type of firm cooperating with the NSA to provide user data where the former publicly and adamantly stated that they would never do so.

This has flow-on effects that challenge *claim 2* – that only some firms will face public backlash for selling technologies to the state, whereas others would not. The case of aerospace technology is illustrative here. Aerospace firms are largely irresponsive to public concern in large part due to contextual factor #2 above – the assumption that the aerospace industry is set up to serve state interests. As such, aerospace firms never appeared to face public backlash for engaging with government contracts. Biotechnology firms engaged with biodefense activities were also rarely critiqued, in part because they were not as visible to the public.

Finally, *claim 3* is challenged by the lack of consistency by which researchers will channel public concerns that seed conflicts with firms. For cases where researchers were tightly bound to firms as their employers – as in the case of aerospace technology – this conflict between researchers and firms did not emerge. For cases where researchers were bifurcated between those employed by firms versus those who remained independent – as in the cases of biotechnology and cryptography – the propensity for researchers to express concerns remained weak, perhaps due to this bifurcation in the research community.

As such, given that firms are differentially responsive to the concerns of the public and of researchers, this means that they are differentially likely to sell technologies to the state and to face conflicts with researchers on issues of ethics and societal consequences. The weak predictability of these conflicts emerging should thus be reflected in the model.

6.3 Summary

Overall, we find that the model performs well in describing the nature of the actors and actor relationships as they evolve across the life cycles of aerospace technology, biotechnology, and cryptography. Tables 6.3-1 to 6.3-4 summarise the case studies through the lens of the model and systematically explain the deviations from the model in terms of the contextual factors described in section 6.2.

Improvements to this model would reflect these contextual factors and further hypothesize what effects they would have on components of the model. In looking to the case of artificial intelligence, an attempt at accounting for these factors is warranted – namely, categorizing AI as either a defense-first or civilian-first technology; identifying whether the state is a necessary and central customer for AI technologies; and acknowledging the inconsistencies with which AI firms will be subject to public and researcher critique.

Table 6.3-1: Summary of evolution of actor goals, resources and constraints

State		**Theory**	**Aerospace**	**Biotechnology**	**Cryptography**
Goals	*Economic growth*	=	=	=	↑
	Military leadership	=	=	↑	=
	Risk mitigation	=	=	↑	=
Resources	*R&D funding*	↓	↓	↓	↓
	Legislative environment	↑	=	↑	↑
	Innovation capacity	↓	↓	()	↓
Constraints	*Public concern*	↑	()	↑	↑
Firms		**Theory**	**Aerospace**	**Biotechnology**	**Cryptography**
Goals	*Maximise profit*	=	=	=	=
Resources	*R&D funding*	↑	↑	↑	↑
	Innovation capacity	↑	↑	↑	↑
Constraints	*Legislative environment*	↑	=	↑	↑
	Public concern	↑	()	()	↑
Researchers		**Theory**	**Aerospace**	**Biotechnology**	**Cryptography**
Goals	*Pursue research*	=	=	=	=
Resources	*Innovation capacity*	↓	()	↓	↓
	Public concern	=	()	()	=
Constraints	*R&D funding*	=	=	=	=
	Legislative environment	↑	=	↑	()

Notes:
↑ means that the goal / resource / constraint becomes more important as the technology matures
↓ means that the goal / resource/constraint becomes less important as the technology matures
() indicates that the goal / resource / constraint is not relevant in this case
= indicates that the goal / resource / constraint remained constant as the technology matures

Table 6.3-2: Summary of deviations in an actor's goals, resources or constraints from the theory

State		**Expected according to theory**	**Deviating case**	**Deviation**	**Explanation**
Goals	*Economic growth*	=	Cryptography	↑	Contextual factor #1: Defense origins of cryptography
	Military leadership	=	Biotechnology	↑	Contextual factor #1: Early international norm against biological weapons
	Risk mitigation	=	Biotechnology	↑	Contextual factor #1: Commercial origins of biotechnology
Resources	*R&D funding*	↓	No deviations		
	Legislative environment	↑	Aerospace	=	Contextual factor #2: Existing legislative environment for aviation
	Innovation capacity	↓	Biotechnology	()	Contextual factor #1: Commercial origins of biotechnology
Constraints	*Public concern*	↑	Aerospace	()	The aerospace industry lost public salience after the Space Race ended.
Firms		**Expected according to theory**	**Deviating case**	**Deviation**	**Explanation**
Goals	*Maximise profit*	=	No deviations		
Resources	*R&D funding*	↑	No deviations		
	Innovation capacity	↑	No deviations		
Constraints	*Legislative environment*	↑	Aerospace	=	Contextual factor #2: Existing legislative environment for aviation
	Public concern	↑	Aerospace	()	Contextual factor #1: Defense origins of aerospace industry
			Biotechnology	()	Contextual factor #3: Biotechnology industry dominated by non-consumer-facing firms
Researchers		**Expected according to theory**	**Deviating case**	**Deviation**	**Explanation**
Goals	*Pursue research*	=	No deviations		

Resources	*Innovation capacity*	↓	Aerospace	()	Contextual factor #2: Aerospace researchers largely subsumed within the state
	Public concern	=	Aerospace	()	In both cases, researchers did not appear to channel elements of the public concern in evident ways.
			Biotechnology	()	
Constraints	*R&D funding*	=	No deviations		
	Legislative environment	↑	Aerospace	=	Contextual factor #2: Existing legislative environment for aviation
			Cryptography	()	Cryptography researchers did not appear to be substantially constrained perhaps owing to their small size.

Notes:
↑ means that the goal / resource / constraint becomes more important as the technology matures
↓ means that the goal / resource/constraint becomes less important as the technology matures
() indicates that the goal / resource / constraint is not relevant in this case
= indicates that the goal / resource / constraint remained constant as the technology matures

Table 6.3-3: Summary of evolution of actor relationships

State <> Firms		***Theory***	***Aerospace***	***Biotechnology***	***Cryptography***
Synergy	*State depends on access to commercial technologies*	↑	↑	↑	↑
Conflict	*State prevents firms from proliferating technologies*	↑	↑	↑	↑
	Firms face public backlash for selling technologies to the state	↑	()	()	↑
State <> Researchers		***Theory***	***Aerospace***	***Biotechnology***	***Cryptography***
Synergy	*State creates supportive R&D environment*	↓	↓	↓	↓
Conflict	*State prevents researchers from proliferating knowledge and talent*	↑	()	↑	↑
Firms <> Researchers		***Theory***	***Aerospace***	***Biotechnology***	***Cryptography***
Synergy	*Firms create supportive R&D environment*	↑	↑	↑	↑
Conflict	*Researchers clash with firms on issues of ethics and societal consequences*	↑	()	↑	()

Notes:
↑ means that the synergy / conflict becomes more important as the technology matures
↓ means that the synergy / conflict becomes less important as the technology matures
() means that the synergy / conflict is not relevant in this case
= means that the synergy / conflict remained constant as the technology matures

Table 6.3-4: Summary of deviations in actor relationships from the theory

State <> Firms		***Expected according to theory***	***Deviating case***	***Deviation***	***Explanation***
Synergy	*State depend on access to commercial technologies*	↑	No deviation		
Conflict	*State prevents firms from proliferating technologies*	↑	No deviation		
	Firms face public backlash for selling technologies to the state	↑	Aerospace	()	Contextual factor #1: Defense origins of aerospace industry
			Biotechnology	()	Contextual factor #3: Biodefense firms were non-consumer-facing
State <> Researchers		***Expected according to theory***	***Deviating case***	***Deviation***	***Explanation***
Synergy	*State creates supportive R&D environment*	↓	No deviation		
Conflict	*State prevents researchers from proliferating knowledge and talent*	↑	Aerospace	()	Contextual factor #2: Aerospace researchers were largely subsumed within the state or firms; thus, no direct conflicts emerged.
Firms <> Researchers		***Expected according to theory***	***Deviating case***	***Deviation***	***Explanation***
Synergy	*Firms create supportive R&D environment*	↑	No deviation		
Conflict	*Researchers clash with firms on issues of ethics and societal consequences*	↑	Aerospace	()	Contextual factor #2: Aerospace researchers subsumed within the state and firms
			Cryptography	()	The cryptography research community were largely on the side of firms in conflict with the state.

Notes:
↑ means that the synergy / conflict becomes more important as the technology matures
↓ means that the synergy / conflict becomes less important as the technology matures
() means that the synergy / conflict is not relevant in this case
= means that the synergy / conflict remained constant as the technology matures

7 Artificial Intelligence

We are entering an era of artificial intelligence – an era that is becoming starkly politicised and deeply competitive between some of the world's most powerful actors. This is, and will increasingly become, an arena of politics that warrants our close attention and careful assessment, particularly with an eye towards the implications of what is to come.

AI possesses the features of an emerging strategic GPT. Its economic value is potentially vast; its military applications could be transformative; and its general purpose nature could fuel complementary innovation across several domains. Conversely, the risks that it poses to individual, societal, and global security raises the stakes of the competition between powerful actors in pursuit of this AI bounty.

The field of artificial intelligence (AI) aims to build and understand intelligent entities[1]. Present day AI refers to a variety of machines and systems that demonstrate general-purpose capabilities such as perception and logical reasoning, to more specific capabilities such as playing computer games and captioning images. Certain areas of AI, particularly within the sub-field of machine learning (ML), have seen rapid progress in recent years – most notably in computer vision, speech recognition, and deep learning[2].

In our everyday lives, AI takes a variety of forms and serves a variety of functions. AI algorithms are embedded in familiar software systems such as search engines, electronic commerce platforms, and social networks. Beyond the prosaic, AI is being used to power

[1] Russell, S. J., & Norvig, P. (2010). *Artificial intelligence: a modern approach* (3rd ed.). Upper Saddle River, N.J.: Prentice Hall.

[2] This is drawn from a list of the most impressive, significant and/or surprising examples of progress to academic AI researchers, provided by technical advisors to the Open Philanthropy Project, a philanthropic funding body for research on safe and beneficial artificial intelligence - Karnofsky, H. (2016). Some Background on Our Views Regarding Advanced Artificial Intelligence. Retrieved April 7, 2018, from https://www.openphilanthropy.org/blog/some-background-our-views-regarding-advanced-artificial-intelligence

multilingual translation systems[3], shape hedge fund trading strategies[4], and model climate risks and forecasts[5]. When combined with hardware such as physical sensors and robotic systems, AI systems have enabled the automation of production lines, the creation of autonomous vehicles, and the embodiment of personal assistants in virtual form. It is increasingly difficult to find an industry or a dimension of our socio-political lives that has not been affected by AI. Indeed, the potential impact of AI has been likened to electricity[6] and other GPTs[7]. Leading economists have hypothesized that as AI advances it could fundamentally alter the nature of industrial structure[8] and science innovation[9].

The potential of AI to transform military capabilities has become a focal point of interest for state leaders around the world[10]. Indeed, there has been a notable increase in the uptake of AI by defense institutions in recent years. Military robotics, for example, has seen a triple-fold increase in worldwide spending between 2000 to 2015, and DARPA is actively working on bringing AI into cyber defense[11].

---

[3] Lewis-Kraus, G. (2016). The Great A.I. Awakening. *The New York Times Magazine*. Retrieved from https://www.nytimes.com/2016/12/14/magazine/the-great-ai-awakening.html

[4] Pressman, A., & Roberts, J. J. (2018). Data Sheet: What AI Will Do to the Financial System. *Fortune*. Retrieved from http://fortune.com/2018/05/31/data-sheet-ai-finance-jp-morgan-chase/

[5] Jones, N. (2017). How machine learning could help to improve climate forecasts. *Nature News*, *548*(7668), 379. https://doi.org/10.1038/548379a

[6] Clifford, C. (2018). Google CEO: A.I. is more important than fire or electricity. *CNBC*. Retrieved from https://www.cnbc.com/2018/02/01/google-ceo-sundar-pichai-ai-is-more-important-than-fire-electricity.html

[7] Trajtenberg, M. (2018). AI as the Next GPT: A Political-Economy Perspective. In A. K. Agrawal, J. Gans, & A. Goldfarb (Eds.), *The Economics of Artificial Intelligence: An Agenda*. Cambridge, Mass: National Bureau of Economic Research. Retrieved from https://www.nber.org/chapters/c14025

[8] Varian, H. (2018). Artificial Intelligence, Economics, and Industrial Organization. In A. K. Agrawal, J. Gans, & A. Goldfarb (Eds.), *The Economics of Artificial Intelligence: An Agenda*. Cambridge, Mass: National Bureau of Economic Research. Retrieved from https://www.nber.org/chapters/c14017

[9] Cockburn, I. M., Henderson, R., & Stern, S. (2018). The Impact of Artificial Intelligence on Innovation: An Exploratory Analysis. In A. K. Agrawal, J. Gans, & A. Goldfarb (Eds.), *The Economics of Artificial Intelligence: An Agenda*. Cambridge, Mass: National Bureau of Economic Research. Retrieved from https://www.nber.org/chapters/c14006

[10] For example, a white paper commissioned by the U.S. Army and the UK Ministry of Defense recently recommended the rapid integration of AI technologies into U.S. and UK defense forces. Pearson, G., Jolley, P., & Evans, G. (2018). A Systems Approach to Achieving the Benefits of Artificial Intelligence in UK Defence. *ArXiv:1809.11089 [Cs]*. Retrieved from http://arxiv.org/abs/1809.11089

[11] Allen, G., & Chan, T. (2017). *Artificial Intelligence and National Security*. Belfer Center for Science and International Affairs.

For all its potential, the threats that AI poses to security, safety, and strategic stability are as wide-ranging as they are grave. For example, novel AI capabilities wielded by malicious actors could cause harm by expanding the landscape of threats to digital, physical, and political security[12]. In the digital realm, a 2017 survey conducted by cybersecurity firm Cylance found that '62% of [information security] experts believe that artificial intelligence will be used for cyberattacks in the coming year'[13]. In the physical realm, the development of autonomous weapon systems is being pursued by American[14], Israeli[15] and French[16] companies, among several others. In the political realm, threats from AI could arise in the form of deep fake technology[17], facial recognition technology[18], and more broadly, the use of AI for the widespread distribution of misleading or inaccurate information[19].

AI systems deployed in the real world are also at risk of causing accidents, sometimes with fatal consequences[20]. The field of AI safety is broadly concerned with the mitigation of accident harm caused by existing and prospective AI systems. A seminal paper in this field published by leading researchers from Google, OpenAI, UC Berkeley, and Stanford

---

[12] Brundage, M., Avin, S., Clark, J., Toner, H., Eckersley, P., Garfinkel, B., … Amodei, D. (2018). *The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation*. Future of Humanity Institute. Retrieved from https://maliciousaireport.com/

[13] Cylance. (2017). Black Hat Attendees See AI as Double-Edged Sword. Retrieved from threatmatrix.cylance.com/en_us/home/black-hat-attendees-see-ai-as-double-edged-sword.html.

[14] BAE Systems. (n.d.). Taranis. Retrieved March 6, 2019, from https://www.baesystems.com/en/product/taranis

[15] Israel Aerospace Industries. (n.d.). HARPY NG. Retrieved March 6, 2019, from http://www.iai.co.il/2013/36694-16153-en/Business_Areas_Land.aspx

[16] Jeangene Vilmer, J.-B. (2017). The French Turn to Armed Drones. *War on the Rocks*. Retrieved from https://warontherocks.com/2017/09/the-french-turn-to-armed-drones/

[17] Chesney, R., & Citron, D. K. (2019). Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security. *California Law Review*, *107*. Retrieved from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3213954

[18] Chan, T. F. (2018). Parts of China are using facial recognition technology that can scan the country's entire population in one second. *Business Insider US*. Retrieved from https://www.businessinsider.sg/china-facial-recognition-technology-works-in-one-second-2018-3/

[19] Howard, P. N., & Woolley, S. C. (2017). *Computational Propaganda Worldwide: Executive Summary* (Computational Propaganda Research Project No. Working Paper No. 2017.11). Oxford, United Kingdom: Oxford Internet Institute. Retrieved from http://comprop.oii.ox.ac.uk/wp-content/uploads/sites/89/2017/06/Casestudies-ExecutiveSummary.pdf

[20] The Economist. (2018). Why Uber's self-driving car killed a pedestrian. *The Economist*. Retrieved from https://www.economist.com/the-economist-explains/2018/05/29/why-ubers-self-driving-car-killed-a-pedestrian

University nominates a typology of the types of unintended and harmful behaviours that may emerge from poorly designed 'unsafe' AI systems[21]. A number of these types of accidents have come to bear in AI systems being developed by labs today[22].

Further, as AI systems scale in capability, we run the risk of tipping into ever more precarious modes of strategic instability[23]. Andrea L. Thompson, then-Undersecretary for Arms Control and National Security, flagged AI as a key emerging threat to strategic stability in testimony before the Senate Foreign Relations Committee[24]. Richard Danzig, former Secretary of the Navy and member of the President's Intelligence Advisory Board, warns that AI and other emerging technologies could threaten the stability of U.S. national security, and thus the U.S. pursuit for technological superiority[25]. RAND Corporation warns that AI could destabilise the already delicate balance holding nuclear war at bay since 1945[26].

With so much at stake, the challenge is first to make sense of the politics of this contemporary case of a strategic GPT. This chapter looks across the technology life cycle of artificial intelligence to date, parsing the events and dynamics as per the proposed model introduced in Chapter 2. Section 7.1 outlines the key actors who have been critical in shaping the

---

[21] Amodei, D., Olah, C., Steinhardt, J., Christiano, P., Schulman, J., & Mané, D. (2016). Concrete Problems in AI Safety. *ArXiv*. Retrieved from https://arxiv.org/abs/1606.06565

[22] For a list of examples of AI systems engaging in 'specification gaming' see: Krakovna, V. (2018). Specification gaming examples in AI. Retrieved from https://vkrakovna.wordpress.com/2018/04/02/specification-gaming-examples-in-ai/; For a list of examples of AI systems that utilise evolutionary algorithms behaving in unexpected ways, see: Lehman, J., Clune, J., Misevic, D., Adami, C., Altenberg, L., Beaulieu, J., … Yosinski, J. (2018). The Surprising Creativity of Digital Evolution: A Collection of Anecdotes from the Evolutionary Computation and Artificial Life Research Communities. *ArXiv:1803.03453 [Cs.NE]*. Retrieved from https://arxiv.org/abs/1803.03453

[23] Dafoe, A. (2018). *AI Governance: A Research Agenda*. Retrieved from Future of Humanity Institute website: https://www.fhi.ox.ac.uk/wp-content/uploads/GovAIAgenda.pdf

[24] Bidwell, C. A., & MacDonald, B. W. (2018). *Emerging Disruptive Technologies and Their Potential Threat to Strategic Stability and National Security*. Federation of American Scientists. Retrieved from https://fas.org/wp-content/uploads/media/FAS-Emerging-Technologies-Report.pdf?utm_source=FAS+General&utm_campaign=9b44d2bccd-EMAIL_CAMPAIGN_2017_02_21_COPY_01&utm_medium=email&utm_term=0_56a7496199-9b44d2bccd-199323333

[25] Danzig, R. (2018). *Technology Roulette*. Washington, D.C.: Center for a New American Security. Retrieved from https://www.cnas.org/publications/reports/technology-roulette

[26] Geist, E., & Lohn, A. (2018). *How Might Artificial Intelligence Affect the Risk of Nuclear War?* RAND Corporation. Retrieved from https://www.rand.org/pubs/perspectives/PE296.html

trajectory of artificial intelligence to date. Then, sections 7.2 and 7.3 step through the first two phases of the technology life cycle of artificial intelligence. Finally, section 7.4 uses the model to conduct a stock take of the trends that have been observed and are emerging, such that we may speculate as to what may be on the horizon for the case of AI.

7.1 The actors

The pursuit of AI has become a site of competition and conflict between important actors. The following section describes the three most prominent actors – states, firms, and researchers – in terms of the interests and capabilities that they each have with respect to AI.

7.1.1 The state

Leading nations have expressed clear intentions to invest heavily in AI as a matter of national interest. To date, over two dozen countries have released national AI strategies, and the likes of the European Union, the United Nations and the Group of 7 countries (G7) have issued strong statements of commitment and diverted resources towards the pursuit of AI[27].

The two nations at the forefront of this pursuit are the U.S. and China – and for both states, the pursuit of technological dominance in AI is playing out on both the commercial and military fronts. In May 2016, the Obama administration announced the formation of a new National Science and Technology Council (NSTC) subcommittee on machine learning and artificial intelligence to help coordinate federal activity in AI. Across 2016, the White House proceeded to host public workshops[28] and a request for information on AI[29]. Following this, a series of reports were published laying out an assessment and recommendations for federal activity with respect to AI moving forward[30]. While the Trump administration was initially

[27] Future of Life Institute. (n.d.). National and International AI Strategies. Retrieved December 11, 2018, from https://futureoflife.org/national-international-ai-strategies/

[28] Felten, E. (2016). Preparing for the Future of Artificial Intelligence. Retrieved April 8, 2018, from https://obamawhitehouse.archives.gov/blog/2016/05/03/preparing-future-artificial-intelligence

[29] Science and Technology Policy Office. (2016). Request for Information on Artificial Intelligence. Retrieved April 8, 2018, from https://www.federalregister.gov/documents/2016/06/27/2016-15082/request-for-information-on-artificial-intelligence

[30] The three reports published were as follows:

- National Science and Technology Council. (2016a). *Preparing for the Future of Artificial Intelligence*. Washington DC: Executive Office of the President.
- Executive Office of the President. (2016). *Artificial Intelligence, Automation, and the Economy*. Washington DC: Executive Office of the President.
- National Science and Technology Council. (2016b). *The National Artificial Intelligence Research and Development Strategic Plan*. Washington DC: Executive Office of the President.

inactive on AI, in May 2018 President Trump hosted a Summit on Artificial Intelligence for American Industry at the White House during which the administration announced its goals of maintaining American leadership in AI[31]. Consequently, a Select Committee on AI was created to advise the White House on AI R&D priorities[32] and in February 2019 President Trump signed an executive order launching the American AI Initiative, making the development of AI a national priority[33].

In parallel, the Department of Defense (DOD) conducted a series of studies focused on the applicability of AI – specifically deep learning and automation – to DOD missions and interests[34]. Further, AI has been regarded as a core technology in achieving the U.S. strategy for retaining military dominance as outlined in the 'Third Offset Strategy'[35]. This has translated into initiatives such as the establishment of an Algorithmic Warfare Cross-Functional Team whose explicit remit is to 'accelerate DOD's integration of big data and

---

[31] Office of Science and Technology Policy. (2018a). *Summary of the 2018 White House Summit on Artificial Intelligence for American Industry*. Washington, D.C.: The White House. Retrieved from https://www.whitehouse.gov/wp-content/uploads/2018/05/Summary-Report-of-White-House-AI-Summit.pdf

[32] Office of Science and Technology Policy. (2018b). Readout from the Inaugural Meeting of the Select Committee on Artificial Intelligence. Retrieved from https://epic.org/privacy/ai/WH-AI-Select-Committee-First-Meeting.pdf

[33] The White House. Executive Order on Maintaining American Leadership in Artificial Intelligence (2019). Retrieved from https://www.whitehouse.gov/presidential-actions/executive-order-maintaining-american-leadership-artificial-intelligence/

[34] The reports included:

- Defense Science Board. (2016). *Summer Study on Autonomy*. Washington, DC: United States Defense Science Board. Retrieved from https://www.hsdl.org/?abstract&did=794641
- Department of Defense Office of Net Assessment. (2016). *Summer Study: (Artificial) Intelligence: What questions should DoD be asking*. Washington, DC: Department of Defense.
- JASON. (2017). *Perspective on Research in Artificial Intelligence and Artificial General Intelligence Relevant to DoD*. Washington, DC: The MITRE Corporation.

[35] Carter, A. (2016). *Keynote Address: The Path to the Innovative Future of Defense*. Presented at the Center for Strategic and International Studies: Assessing the Third Offset Strategy: Progress and Prospects for Defense Innovation, CSIS Headquarters, Washington, D.C. Retrieved from https://csis-prod.s3.amazonaws.com/s3fs-public/event/161028_Secretary_Ashton_Carter_Keynote_Address_The_Path_to_the_Innovative_Future_of_Defense.pdf

machine learning'[36] and a DARPA project on Explainable Artificial Intelligence[37]. In an attempt to introduce more cohesion to these efforts, in June 2018 the Pentagon established the Joint Artificial Intelligence Center (JAIC), an initiative to integrate and maintain oversight over all service and defense agency AI efforts[38].

7.1.2 Firms

The private sector is, by far, where most of the financial and human resources are concentrated when it comes to the development and deployment of AI. The growth of AI as an economic sector has been astounding in both scale and rapidity. Since 2000 there has been a fourteen-fold increase in the number of active AI start-ups and a six-fold increase in the annual investment levels by venture capital investors into U.S. based AI start-ups[39]. Recent analysis by Pricewaterhouse Coopers (PwC) predicts that AI could contribute up to $15.7 trillion to the global economy in 2030[40].

AI has become a core business interest for the world's largest multinational firms. By way of illustration, one can compare the top ten firms by market capitalisation in the world. In 2007, Microsoft was the only software company within the top ten and at that time were not investing in AI. Ten years later, in 2017, seven of the top ten firms – Apple, Alphabet, Microsoft, Amazon, Alibaba Group, Tencent and Facebook – are technology firms that have

---

[36] In the memorandum establishing Project Maven, Robert Work (32nd US deputy secretary of defense) states: "As numerous studies have made clear, the Department of Defense (DoD) must integrate artificial intelligence and machine learning more effectively across operations to maintain advantages over increasingly capable adversaries and competitors." - Work, R. (2017). *Establishment of an Algorithmic Warfare Cross-Functional Team (Project Maven)*. Department of Defense. Retrieved from http://dodcio.defense.gov/Portals/0/Documents/Project%20Maven%20DSD%20Memo%2020170425.pdf

[37] Gunning, D. (n.d.). Explainable Artificial Intelligence (XAI). Retrieved April 8, 2018, from https://www.darpa.mil/program/explainable-artificial-intelligence

[38] Freedberg Jr., S. J. (2018). Joint Artificial Intelligence Center Created Under DoD CIO. *Breaking Defense*. Retrieved from https://breakingdefense.com/2018/06/joint-artificial-intelligence-center-created-under-dod-cio/

[39] Shoham, Y., Perrault, R., Brynjolfsson, E., Clark, J., Manyika, J., Carlos Niebles, J., … Bauer, Z. (2018). *The AI Index 2018 Annual Report*. Stanford, CA: AI Index Steering Committee, Human-Centered AI Initiative.

[40] PwC. (2017). Sizing the prize: What's the real value of AI for your business and how can you capitalise? Pricewaterhouse Coopers.

all invested significantly in AI as a core part of their business[41]. As of 2018, seven of the twelve largest companies worldwide are heavily engaged in AI[42] and these very companies – including Amazon, Alphabet, Intel, and Microsoft – were the top R&D spenders in the U.S. in the 2017 financial year[43].

AI has become a site of intense private sector competition, as signalled by statements from CEOs[44], the expansion in the number and geographic distribution of AI labs[45], and the aggression with which these companies are acquiring AI start-ups[46]. Only a handful are capable of engaging in this scale of competition: seven firms – Google, Facebook, IBM, Microsoft, Amazon, Apple, and Baidu – hold AI capabilities that vastly outstrip all other institutions[47].

---

[41] Financial Times. (2007). FT Global 500 December 2007. Retrieved from https://im.ft-static.com/content/images/813c979e-0faa-11dd-8871-0000779fd2ac.pdf; Financial Times. (2017). FT Global 500 December 2017. Retrieved from https://www.ft.com/signup?offerId=1dbc248e-b98d-b703-bc25-a05cc5670804&ft-co=markets-inline. Credit to Allan Dafoe for first making this illustrative comparison.

[42] Goldfarb, A., & Trefler, D. (2018). AI and International Trade. In A. K. Agrawal, J. Gans, & A. Goldfarb (Eds.), *The Economics of Artificial Intelligence: An Agenda*. Cambridge, Mass: National Bureau of Economic Research. Retrieved from https://www.nber.org/chapters/c14012

[43](Hogarth & Benaich, 2018)

[44] Notable examples include:

- In his 2016 letter to shareholders, Jeff Bezos of Amazon emphasise machine learning as critical to "improving core operations". - Bezos, J. (2017). 2016 Letter to Shareholders. Retrieved April 7, 2018, from https://blog.aboutamazon.com/working-at-amazon/2016-letter-to-shareholders
- In an email to employees, Satya Nadella of Microsoft announces a number of organisational shifts to streamline resources towards cloud and AI. - Nadella, S. (2018). Satya Nadella email to employees: Embracing our future: Intelligent Cloud and Intelligent Edge. Retrieved April 7, 2018, from https://news.microsoft.com/2018/03/29/satya-nadella-email-to-employees-embracing-our-future-intelligent-cloud-and-intelligent-edge/

[45] Examples include:

- Google has announced a new China-based research lab focused on AI. – Russell, J. (2017). Google is opening a China-based research lab focused on artificial intelligence. *TechCrunch*. Retrieved from https://techcrunch.com/2017/12/12/google-opening-an-office-focused-on-artificial-intelligence-in-china/
- Alibaba sets up its first research centre outside China in Singapore, focused on AI. - Choudhury, S. R.(2018). Alibaba just set up its first joint research center outside China to focus on A.I. *CNBC*. Retrieved from https://www.cnbc.com/2018/02/28/alibaba-sets-up-joint-a-i-research-lab-in-singapore.html

[46] CB Insights. (2018). The Race For AI: Google, Intel, Apple In A Rush To Grab Artificial Intelligence Startups. Retrieved from https://www.cbinsights.com/research/top-acquirers-ai-startups-ma-timeline/

[47] Iyengar, V. (2016). Why AI consolidation will create the worst monopoly in US history. *TechCrunch*. Retrieved from http://social.techcrunch.com/2016/08/24/why-ai-consolidation-will-create-the-worst-monopoly-in-us-history/; Jang, E. (2017). What Companies Are Winning The Race For Artificial Intelligence? *Forbes*. Retrieved from https://www.forbes.com/sites/quora/2017/02/24/what-companies-are-winning-the-race-for-artificial-intelligence/

It is notable that the leading AI companies are either American or Chinese; the relationship between these firms and the state is consequently of central interest. Of the companies that have invested the most in AI, the majority are predominantly based in the U.S. – including Google, Amazon, Apple, Microsoft and Facebook – although these companies have expanded rapidly beyond the US, and increasingly into China[48]. Chinese companies, on the other hand, are catching up quickly, with Baidu, Alibaba, and Tencent leading the way[49].

7.1.3 Researchers

The number of researchers engaged in AI has rapidly grown in recent years, driven by the substantial resource being invested in AI research by countries and companies around the world[50]. Between 2012 and 2017, course enrolment numbers in introductory AI courses tripled at several leading computer science universities in the U.S.; for introductory ML courses enrolment numbers increased by five times. Notably, at Tsinghua University – a leading Chinese institution – combined AI and ML courses saw a sixteen-fold increase from 2010 and 2017[51].

The volume of research activity in AI has also grown rapidly. The number of AI papers on Scopus increased by seven-fold between 1996 and 2017, outstripping the five-fold increase in computer science papers. Attendance at the largest AI conferences has grown by up to seven-fold between 2012 and 2017[52]. At the forefront of the field, competing head to head for both talent and research breakthroughs, are firms and universities. Of the top ten contributors to the NIPS 2017 Conference – one of the most prestigious events in the field

[48] Krauth, O. (2018). The 10 tech companies that have invested the most money in AI. *TechRepublic*. Retrieved from https://www.techrepublic.com/article/the-10-tech-companies-that-have-invested-the-most-money-in-ai/
[49] (Ding, 2018)
[50] Karmanov, F., & Hudson, S. (2018). *Global AI Talent Report 2018*. jfg. Retrieved from http://www.jfgagne.ai/talent/
[51] (Shoham et al., 2018)
[52] (Shoham et al., 2018)

– three were companies and seven were universities, with Google leading in the number of contributions overall[53].

As the field of AI research has grown, it has quickly become globally distributed. Sampling from academic papers presented at major AI research conferences, one observes a drop from 41% in 2012 to 34% in 2017 of the proportion of authors from U.S. institutions. Comparably, the proportion of Chinese authors increased from 10% to 24% across the same period. As of 2017, 83% of the papers on AI published on Scopus originated from outside the U.S., and the number of papers specifically from China increased by 150% between 2007 and 2017. International collaboration between researchers in different countries has also been steadily increasing[54].

[53] (Hogarth & Benaich, 2018)
[54] (Shoham et al., 2018)

7.2 Phase 1: Emergence and promise [1956 – 2012]

The *emergence and promise* phase of AI features two failed attempts at spurring the field forward between the 1950s and 1990s, before a final and sustained wave of breakthroughs in the 2000s which has carried us through to the current paradigm of AI R&D[55].

The theoretical grounding for the first two waves of AI drew on several intellectual threads, including foundational work by Alan Turing[56], initial conceptualizations of simple neural networks by Warren McCulloch and Walter Pitts[57], contributions from wartime research in cryptography and mathematical modelling[58], and early ideas by Charles Babbage and Ada Lovelace[59], among others. The seminal coining of the term 'artificial intelligence' by John McCarthy in 1956 marks the convergence of these threads into a unified vision of a distinct field. Section 7.2.1 runs through a series of milestones which follow from 1956, describing the initially unsuccessful attempts at delivering on the promises of AI before a final attempt that has, thus far, succeeded at fuelling substantial progress in the field. Section 7.2.2 then highlights the dynamics that emerged between the state, firms, and researchers across this period.

7.2.1 Notable events

7.2.1.1 The Dartmouth Summer Project and the First AI Spring [1956 – 1973]

The Dartmouth Summer Project was bold in its ambition: a two month, ten man study of artificial intelligence with the goal of making significant advances on the problem of 'how to make machines use language, form abstractions and concepts, solve kinds of problems now

[55] A sincere than you to Nathan Calvin who helped to compile a lot of the information in this section.
[56] Turing, A. M. (1950). Computing machinery and intelligence. *Mind*, *59*(236), 433.
[57] McCulloch, W. S., & Pitts, W. (1943). A logical calculus of the ideas immanent in nervous activity. *Bulletin of Mathematical Biophysics*, *5*.
[58] (Reed Jr, 1952)
[59] (Knight, 2006)

reserved for humans, and improve themselves'[60]. The Dartmouth Summer Project did not lead to any direct breakthroughs. However, the exchange of ideas and the research collaborations that it enabled led to several high-profile achievements which seeded a golden-age of AI research[61].

This period also saw considerable amounts of military-earmarked state funds directed towards the field[62]. This was enabled by the founding of the Advanced Research Projects Agency (ARPA) in 1958. ARPA became a crucial institution in supporting computing technology in the U.S., specifically via the Information Processing Techniques Office (IPTO) which housed ARPA's substantial investments in AI research[63]. ARPA provided major funding for AI research at renowned institutions such as MIT, Carnegie Mellon University,

---

[60] McCarthy, J., Minsky, M. L., Rochester, N., & Shannon, C. E. (2006). A Proposal for the Dartmouth Summer Research Project on Artificial Intelligence, August 31, 1955. *AI Magazine*, *27*(4). Retrieved from https://aaai.org/ojs/index.php/aimagazine/article/view/1904

[61] For example:

- Drawing primarily on techniques based on formal symbolic reasoning, researchers developed tools capable of human-like performance in narrow fields such as geometric proofs, algebra, and simple games such as checkers. See Samuel, A. L. (1967). Some studies in machine learning using the game of checkers. II—Recent progress. *IBM Journal of Research and Development*, *11*(6), 601–617.\
- John McCarthy made significant progress in the period following Dartmouth developing LISP (LISt Processor) which became an important programming language for AI researchers.
- Marvin Minsky formalized means of reasoning, including pattern recognition and heuristic processes, contributing substantially to our understanding of human cognition. See Minsky, M. L. (1956). *Heuristic Aspects of the Artificial Intelligence Problem* (No. Report 34-55 ASTIA Doc. No. AS236885). Cambridge, MA: MIT Lincoln Laboratory.; Minsky, M. L. (1979). The Society Theory of Thinking. In P. H. Winston & R. H. Brown, *Artificial Intelligence: An MIT Perspective* (pp. 423–450). Cambridge, MA: MIT Press.
- Herbert Simon and Allen Newell – a research collaboration which ultimately contributed substantially to the intellectual foundations of the AI field – began their work on the simulation of human thought at the Dartmouth Sumer Project. This resulted in their work on the Logic Theorist – a computer program capable of proving theorems found in the *Principia,* regarded by many as the first successful AI program. See Newell, A., & Simon, H. A. (1956). *Current developments in complex information processing*. Santa Monica, California: RAND Corporation.
- Simon and Newell proceeded to develop another well-known AI program, the General Problem Solver, which was capable of solving an array of problems by simulating the way a human being would solve them. See Newell, A., Shaw, J. C., & Simon, H. A. (1959). *Report on a general problem solving program*. Santa Monica, California: RAND Corporation.

[62] Crevier, D. (1993). AI: The Tumultuous Search for Artificial Intelligence. New York: Basic Books.; Moravec, H. (1995). Mind Children: The Future of Robot and Human Intelligence. Cambridge, MA: Harvard University Press.

[63] Roland, A., & Shiman, P. (2002). *Strategic Computing: DARPA and the Quest for Machine Intelligence, 1983 - 1993*. Cambridge MA: The MIT Press. Retrieved from https://ondoc.logand.com/d/2721/pdf

and Stanford University, largely with no strings attached. ARPA was subsequently renamed the Defense Advanced Research Projects Agency (DARPA) in 1972.

7.2.1.2 The First AI Winter [1974 – 1979]

By the early 1970s progress in the field of AI had begun to stall. For one, it became clear that despite early advances, AI systems as conceived then remained far more limited in their capabilities than had been expected. Specifically, researchers realized that the trial-and-error approach that underpinned many AI algorithms at the time would require exponential amounts of computer processing power, which was infeasible given hardware limitations at the time[64].

During this period, a series of government-commissioned reports issued scathing assessments of the field, triggering state-funding cutbacks. In 1966, the Automatic Language Processing Advisory Committee to the U.S. government reported slow progress in the domains of natural language processing and automated translation, leading to the termination of all research funding from the National Research Council[65]. In 1973, at the request of the British Scientific Research Council, Sir James Lighthill published a survey which surmised considerable scepticism about the field of AI, criticising the failure of AI research to live up to its 'grandiose objectives'[66]. This led to a cessation of AI research funding in Britain and, eventually, similar cutbacks in the U.S.

---

[64] De Spiegeleire, S., Maas, M., & Sweijs, T. (2017). *Artificial Intelligence and the Future of Defense: Strategic Implications for Small and Medium Sized Force Providers*. The Hague, Netherlands: The Hague Centre for Strategic Studies. Retrieved from https://hcss.nl/sites/default/files/files/reports/Artificial%20Intelligence%20and%20the%20Future%20of%20Defense.pdf

[65] Hutchins, J. (2005). *The history of machine translation in a nutshell*. Retrieved from http://www.hutchinsweb.me.uk/Nutshell-2005.pdf

[66] Lighthill, J. (1973). Artificial Intelligence: A General Survey. In *Artificial Intelligence: A Paper Symposium*. Science Research Council. Retrieved from www.math.snu.ac.kr/~hichoi/infomath/Articles/Lighthill%20Report.pdf

7.2.1.3 The Second AI Spring [1980 – 1987]

The temporary standstill in AI research came to an end with the emergence of expert systems – rule-based programs that answer questions or solve problems within a specified domain of knowledge. In part as a response to Japan's ambitious project in this vein, the U.S. invested heavily in AI research based on expert systems[67]. In parallel, the commercial potential of expert systems led to an influx of private funding from industry as well. From 1980 to 1988, sales of expert systems grew from a few million to $2 billion[68].

In 1983, DARPA announced the Strategic Computing Initiative (SCI), marking a significant boost in their investment in applied AI research[69]. The ambition of the SCI was to enable a machine that could 'see, hear, speak, and think like a human' through the pursuit of machine intelligence and high performance computing[70]. DARPA committed $1 billion over ten years to this goal, tripling its funding for research in the process[71]. It also established specific applications of R&D that were intended to spark the military services' interest in developing AI technology based on fundamental research[72].

---

[67] (De Spiegeleire et al., 2017)
[68] (S. J. Russell & Norvig, 2010)
[69] DARPA. (1983). Strategic Computing--New Generation Technology: A Strategic Plan for Its Development and Application to Critical Problems in Defense. Arlington, VA: - Defense Advanced Research Projects Agency (DARPA).
[70] The SCI has four main goals:

- Advance machine intelligence technology and high performance computing, including speech recognition and understanding, natural language computer interfaces, vision comprehension systems, and advanced expert systems development; and to do so by providing significant increases in computer performance through parallel-computer architectures, software, and supporting microelectronics.
- Transfer technology from DARPA-sponsored university research efforts to the defense industry through competitive research contracts, with industry and universities jointly participating.
- Develop more new scientists in AI and high-performance computing through increased funding of graduate student research in these areas.
- Provide the supporting research infrastructure for AI research through advanced networking, new microcircuit fabrication facilities, advanced emulation facilities, and advanced symbolic processors.

See: Kahn, R. (1988). Later Years at IPTO. In H. W. Sams (Ed.), *Expert Systems and Artificial Intelligence: Applications and Management* (By T. C. Bartee). Indianapolis, Ind.: Sams Technical Publishing.
[71] McCorduck, P. (2004). Machines who Think: A Personal Inquiry Into the History and Prospects of Artificial Intelligence: AK Peters.
[72] The specific applications included: a pilot's association for the Air Force; an autonomous land vehicle for the Army; and an aircraft battle management system for the Navy.

7.2.1.4 The Second AI Winter [1988 – 1993]

At the turn of the 1990s, progress and interest in AI stalled once again. The flagship AI research programs established in the U.S., Japan, and Europe largely failed to meet their objectives, particularly as expert systems proved of limited practical utility. Several specialised AI hardware companies collapsed after 1987 with the emergence of more affordable desktop computer produced by the likes of Apple and IBM[73].

The success of the SCI was mixed. In critical areas such as computer vision and natural language processing, researchers faced significantly more difficult problems than they had expected at the outset. By the end of the 1980s the leadership of DARPA's IPTO pronounced that AI was not the 'next wave' that they had hoped for, and that AI researchers had once again over-promised and under-delivered. This led to severe cuts to the SCI, leaving only programs that were of direct military relevance.

7.2.1.5 The emergence of Deep Learning [1994 – 2012]

Following the second AI winter, the field saw a lull in progress for the good part of a decade. Then, the mid-2000s heralded a series of conceptual breakthroughs which laid down the cornerstones of the deep learning paradigm; this remains to this day the dominant approach in AI research[74]. These breakthroughs coincided with the novel availability of large volumes

[73] (De Spiegeleire et al., 2017)

[74] In broad terms, the conceptual breakthroughs in sequence were as follows:

- In 1986, Geoffrey Hinton, David Rumelhart, and Ronald Williams published a seminal paper titled 'Learning representations by back-propagating errors'. This paper popularised backpropagation as an effective way of training multi-layered neural networks. Rumelhart, D. E., Hinton, G. E., & Williams, R. J. (1986). Learning representations by back-propagating errors. *Nature*, *323*, 533–536.
- In 1989, Yann LeCun applied backpropagation to training neural nets to recognise handwritten zip codes[74]. LeCun's application was notable for its implementation of what came to be known as convolutional neural networks – a new neural net architecture that proved to be particularly effective for computer vision tasks. LeCun, Y., Boser, B., Denker, J. S., Henderson, D., Howard, R. E., Hubbard, W., & Jackel, L. D. (1989). Backpropagation Applied to Handwritten Zip Code Recognition. *Neural Computation*, *1*(4), 541–551.
- In 2012, Geoffrey Hinton publishes a breakthrough idea – Dropout – which is a mechanism to reduce overfitting of neural networks to training data[74]. This became critical to improving the performance of these algorithms. Hinton, G. E., Srivastava, N., Krizhevsky, A., Sutskever, I., & Salakhutdinov, R. R. (2012). Improving neural networks by preventing co-adaptation of feature detectors. *ArXiv Preprint ArXiv:1207.0580*.

of training data, as well as increasingly affordable computing power, faster networks, and advanced cloud infrastructures[75].

In concert, these trends fuelled a reincarnation of AI. Significant progress followed, particularly in the domains of image classification, speech recognition, language modelling and comprehension, and generalisation of learning across contexts[76]. The application of deep neural networks specifically pushed the frontier of algorithmic performance given their ability to capture highly valuable and previously unnoticed regularities in large datasets[77].

7.2.2 Relationships

7.2.2.1 Researchers <> State

The state – and particularly the DOD – was instrumental in progressing AI research in the early stages of its emergence. Indeed, without interest and investment from the state, it is unlikely that the first and second AI springs would have taken place, nor would the first and second AI winters be so directly caused by a pullback in state funding.

Prior to the creation of ARPA and the IPTO, state support of AI research was channelled through a fragmented set of efforts, mostly in the form of investing directly in individual researchers[78]. With the establishment of ARPA and the IPTO, the state's investments in AI

- In 2014 Ian Goodfellow introduced Generative Adversarial Networks, a neural net architecture that pits two neural nets against one another to enhance their performance. Goodfellow, I. J., Pouget-Abadie, J., Mirza, M., Xu, B., Warde-Farley, D., Ozair, S., … Bengio, Y. (2014). Generative Adversarial Networks. *ArXiv:1406.2661 [Cs, Stat]*. Retrieved from http://arxiv.org/abs/1406.2661

[75] Brynjolfsson, E., & Mitchell, T. (2017). What can machine learning do? Workforce implications. *Science*, *358*(6370), 1530–1534. https://doi.org/10.1126/science.aap8062

[76] Eckersley, P., & Nasser, Y. (2017). AI Progress Measurement. Retrieved from Electronic Frontiers Foundation (EFF) website: https://www.eff.org/ai/metrics

[77] Particularly impressive applications of deep neural networks include:

- *Image recognition*: deep neural networks have driven error rates in ImageNet (a large data-set of over 100,000 labelled images) down from over 30% in 2010 to less than 3% in 2017. The error rate of humans is approximately 5%.
- *Voice recognition*: deep neural networks have improved error rates from 8.4% to 4.9% between 2016 and 2017. The error rate of humans is approximately 5%.

[78] National Research Council. (1999). Developments in Artificial Intelligence. In *Funding a Revolution: Government Support for Computing Research*. https://doi.org/10.17226/6323

research became more streamlined and substantial, shifting from a collection of small projects to a large-scale high-profile domain of strategic interest on the part of the DOD. From the 1960s through to the 1990s, DARPA singlehandedly provided the bulk of the nation's support for AI research and propelled the creation and formalization of AI as an academic discipline.

They did so primarily through establishing and supporting hubs of leading AI research across the country, based at universities[79]. The relationship between DARPA and these academic institutions was initially very hands-off, enabling researchers to steer themselves as they saw fit and trusting that practical applications would follow. Allen Newell, a prominent AI researcher at the time, recalled the lack of accountability involved in receiving ARPA funding: 'They [ARPA] didn't have any control over the money they'd given us…We didn't tell people in ARPA in the '60s what we were going to do with the money…Once we got the money, we did what we thought was right with it.'[80] Allowing for this degree of academic freedom, in Newell's view, enabled DARPA to nurture a new scientific field by supporting university computer science research environments[81].

The onset of the first AI winter signalled a shift in DARPA's approach to supporting AI research towards a focus on immediate, and specifically defense applications of AI. Specifically, the Lighthill report triggered the DOD to establish a panel to assess DARPA's AI program. This investigation led to a shifting of DARPA funds towards what was termed mission-oriented direct research and away from basic undirected research[82]. This reflected

---

[79] The main hubs included: the Graduate School of Industrial Administration (GSIA) at Carnegie Institute of Technology, founded by Herbert Simon; the Artificial Intelligence Project at MIT, founded by John McCarthy and Marvin Minsky; and the Stanford Artificial Intelligence Lab (SAIL), following John McCarthy's move to Stanford.

[80] (Roland & Shiman, 2002)

[81] Newell, A. (1989). Reports on artificial intelligence from Carnegie-Mellon University: introduction to the COMTEX microfiche edition. *Readings from the AI Magazine*, 328–332. American Association for Artificial Intelligence.

[82] Fleck, J. (1982). Development and Establishment in Artificial Intelligence. In N. Elias (Ed.), *Scientific Establishments and Hierarchies* (pp. 169–217). Dordrecht, Holland: Reidel Publishing Company.

the increasing sentiment among U.S. regulatory bodies that defense funding should be spent on producing tangible military applications. The passing of the Mansfield Amendment as part of the Defense Authorization Act of 1970 enshrined this approach to defense research funding. The effect of the Mansfield Amendment was to restrict the DOD to supporting basic research that was of direct and apparent utility to specific military functions and operations[83]. In the years that followed the military's support for basic research declined substantially, including in emergent fields such as AI.

Notably, the lacuna in R&D funding was eventually filled by the entrance of AI firms. As momentum began to pick up again in the early 2000s, large private companies began to replace the state both as developers and funders of neural networks research. As Yoshua Bengio, one of the fathers of deep learning, reflects: 'The shift started…with companies like Google, IBM, and Microsoft, who were working on neural networks for speech recognition. By 2012, Google had these neural networks on their Android smartphones'[84].

7.2.2.2 Firms <> State

DARPA's shift of focus to applied AI research began to pay off during the emergence of the second AI spring, spurring private sector interest and investment. As of the mid-1980s, several start-up AI companies began to emerge with products largely based on expert systems, and existing corporations diverted substantial capital and human resources towards the development of such systems as well[85]. Many reported substantial returns on these investments – the Office for Technology Assessment of the U.S. government heralded

[83] U.S. Congress. Defense Authorization Act, Pub. L. No. 91–121 (1969).
[84] (Ford, 2018)
[85] (National Research Council, 1999)

expert systems as 'the first real commercial products of about 25 years of AI research'[86]. By 1992, over fifty expert system shell programs were available on the mainstream market.

The development of speech recognition technology is a clear case study of firm-state collaboration in fuelling AI commercialisation. Early support for research in this domain was supported by Bell Labs beginning in the 1950s. In the 1970s DARPA boosted support for this research by establishing the Speech Understanding Research Unit with the explicit aim of developing computer systems that could understand continuous speech. DARPA committed $3 million per year for five years, directed towards collaborators at industry labs, including the Systems Development Corporation and Bolt, Beranek and Newman (BBN) Technologies. A second wave of state funding in speech recognition began in 1984 and continued into the late 1990s[87]. Since, speech recognition technologies have been incorporated into the products of companies such as IBM, BBN Technologies, Nuance Communications, Dragon Systems, and Microsoft[88]. Thus, with substantial public funding and private sector engagement, speech recognition technology became one of the first domains of AI research to see successful commercialisation.

The SCI was also a demonstration of firm-state collaboration through the 60% of funds that were committed to industry. Firms such as AT&T, IBM, Texas Instruments, Intel, and Xerox Corporation engaged with the SCI. Further, the establishment of the SCI attracted large amounts of industry investment and venture capital in AI R&D[89].

---

[86] Office of Technology Assessment (OTA). (1985). *Information Technology R&D: Critical Trends and Issues, OTA-CIT-268*. Washington, D.C.: U.S. Government Printing Office.
[87] Defense Advanced Research Projects Agency (DARPA). (1997). *DARPA Technology Transition*. Arlington, VA: DARPA.
[88] McClain, D. (1998). Voice Technology Appears Ready to Recognize Bottom Line. *The New York Times*.
[89] Goldstein, N. (1992). Defense Advanced Research Project Agency's Role in Artificial Intelligence R&D: Case Study of the Military as the National Agent for Technological and Industrial Change. *Defense Analysis*, *8*(1), 61–80.

7.3 Phase 2: Commercialisation and proliferation [2013 – present]

By 2013, the theoretical progress in AI was being leveraged by evermore researchers and companies. The results have been remarkable – an onslaught of milestone achievements in AI across numerous domains. This has had significant ramifications on the perceived and actual economic value of AI. Indeed, the commercial AI sector has grown at an astounding rate, both in the volume of companies developing and deploying AI technologies as well as in the breadth of sectors that these companies span across[90].

Natural language processing (NLP) is a particular domain that has demonstrated rapid progress. From IBM Watson's victory in the game Jeopardy to the public debut of voice-responsive virtual personal assistants such as Apple's SIRI and Microsoft's Cortana, machines are increasingly capable of reading, comprehending, and utilising written prose in various forms[91]. Computer vision – specifically facial recognition technologies – have also progressed at an impressive rate: a number of systems developed by the likes of Google, Microsoft, and Facebook achieved identification rates superior to humans[92], and Microsoft's AI system proved capable of recognising human emotions[93]. Further, in recent years, evermore AI systems have met or exceeded human performance in a wide range of tasks, including speech transcription[94], language translation[95], navigating the London

[90] Zilis, S. (2016). The Current State of Machine Intelligence 3.0. Retrieved from Shivon Zilis website: http://www.shivonzilis.com//machineintelligence
[91] Hermann, K. M., Kočiský, T., Grefenstette, E., Espeholt, L., Kay, W., Suleyman, M., & Blunsom, P. (2015). Teaching Machines to Read and Comprehend. *ArXiv:1506.03340 [Cs]*. Retrieved from http://arxiv.org/abs/1506.03340
[92] (Shoham et al., 2018)
[93] Burgess, M. (2015). Microsoft's AI Can Detect Your Emotions (but Only If You're Angry). *Wired*. Retrieved from http://www.wired.co.uk/article/microsoft-predictemotions-artificial-intelligence
[94] Xiong, W., Droppo, J., Huang, X., Seide, F., Seltzer, M., Stolcke, A., … Zweig, G. (2016). Achieving Human Parity in Conversational Speech Recognition. *ArXiv:1610.05256 [Cs, Eess]*. Retrieved from http://arxiv.org/abs/1610.05256
[95] Lewis-Kraus, G. (2016). The Great A.I. Awakening. *The New York Times Magazine*. Retrieved from https://www.nytimes.com/2016/12/14/magazine/the-great-ai-awakening.html

underground[96], driving[97], detecting crop diseases[98], and even creative tasks such as writing recipes[99], screenplays[100], and songs[101].

At the cutting edge of research, AI systems are beginning to move beyond success at narrow task-based niches towards demonstrating increasingly general and abstract capabilities. DeepMind, a leading AI lab based in London, are at the forefront of developing self-teaching AI agents to play a range of games, from simple Atari games[102] through to complex games such as Go[103] and StarCraft[104]. Games have been used for decades as an important way to test and evaluate the performance of intelligent systems. Thus, defeating professional human players in games that demand substantial human intellect, long-term planning, and strategy capabilities is a feat that firmly signals that AI is progressing at a stunning pace.

---

[96] Gibney, E. (2016). Google's AI reasons its way around the London Underground. *Nature News*. https://doi.org/10.1038/nature.2016.20784

[97] Bryant, R. (2016). Google's AI Becomes First Non-Human to Qualify as a Driver. *Dezeen*. Retrieved from https://www.dezeen.com/2016/02/12/google-self-driving-car-artficial-intelligence-system-recognized-as-driver-usa

[98] Furness, D. (2016). AI in Agriculture? Algorithms Help Farmers Spot Crop Disease like Experts. *Digital Trends*. Retrieved from http://www.digitaltrends.com/computing/ai-crop-disease/

[99] Kleeman, A. (2016). Cooking with Chef Watson, I.B.M.'s Artificial-Intelligence App. *The New Yorker*. Retrieved from http://www.newyorker.com/magazine/2016/11/28/cooking-with-chef-watson-ibms-artificial-intelligence-app

[100] HAL 90210. (2016). This Is What Happens When an AI-Written Screenplay Is Made into a Film. *The Guardian*. Retrieved from https://www.theguardian.com/technology/2016/jun/10/artificial-intelligence-screenplay-sunspring-silicon-valley-thomas-middleditch-ai

[101] Marshall, A. (2017). From Jingles to Pop Hits, A.I. Is Music to Some Ears. *The New York Times*. Retrieved from https://www.nytimes.com/2017/01/22/arts/music/jukedeck-artificial-intelligence-songwriting.html

[102] Metz, C. (2015). Teaching AI to play Atari will help robots make sense of our world. *Wired*. Retrieved from https://www.wired.com/2015/12/teaching-ai-to-play-atari-will-help-robots-make-sense-of-our-world/

[103] DeepMind developed AlphaGo, which became the first computer program to defeat a professional human Go player and a Go world champion. AlphaGo is widely heralded as a landmark achievement by experts in the field, and a decade ahead of its time. AlphaGo Zero, the successor to the AlphaGo system, demonstrated even more impressive results by learning how to play the game without input of human data, but relying on playing games against itself instead. Go is an ancient Chinese game, known for its complexity and demands on human intellect and intuition. See: DeepMind. (2017). The story of AlphaGo so far. Retrieved from DeepMind Blog website: https://deepmind.com/research/alphago/

[104] StarCraft – considered to be one of the most challenging real time strategy games – has been considered a grand challenge for AI research. AlphaStar – DeepMind's AI system for playing StarCraft II – defeated a top professional player in December 2018, marking a landmark achievement for the field of AI. Succeeding in StarCraft requires capabilities such as: balancing short-term and long-term goals; adapting to unexpected information; operating with imperfect information; and controlling a large action space consisting of hundreds of different units and buildings in real-time. See: DeepMind. (2018)See: . AlphaStar: Mastering the Real-Time Strategy Game StarCraft II. Retrieved from DeepMind Blog website: https://deepmind.com/blog/alphastar-mastering-real-time-strategy-game-starcraft-ii/

As the economic and strategic value of AI becomes more evident, the stakes are raised in the competition to lead in the development of AI. Competition has become particularly heightened between the U.S. and China (section 7.3.1.1) which has in turn spurred a defense-oriented American national strategy on AI (section 7.3.1.2). Layered atop of this is the recent uptick in observable AI accidents caused by AI systems being deployed in the real world, and consequently causing public harm. The growing public fear and criticism, directed toward the behaviours of the companies that drives these accidents, has encouraged AI companies to begin to initiate self-governance efforts (section 7.3.1.3).

7.3.1 Notable events

7.3.1.1 The U.S.-China 'AI race'

In the spring of 2016, an AI system defeated a world champion Go player. The AI system – named AlphaGo – was developed by DeepMind, a London-based AI lab owned by Alphabet, the parent company of Google. In May 2017, AlphaGo beat a human player again – this time a Chinese Go master, Ke Jie, ranked top in the world.

Some analysts speculate that AlphaGo's triumphs triggered an uptick in the Chinese government's focus on AI as a matter of national strategic interest[105]. Indeed, a few months following Ke Jie's defeat, the Chinese government published the State Council's New Generation AI Development[106]. Further, on October 18, 2017, President Xi Jinping laid out his plan for the party's future during which AI was named as a core technology that would help transform China into an advanced industrial economy in the coming decades. These statements were followed by concerted and prompt action. Over $2 billion was committed

[105] Bremmer, N. T., Ian. (2018). The AI Cold War That Threatens Us All. *Wired*. Retrieved from https://www.wired.com/story/ai-cold-war-china-could-doom-us-all/

[106] Ding, J. (2018). *Deciphering China's AI Dream: The context, components, capabilities and consequences of China's strategy to lead the world in AI*. Future of Humanity Institute. Retrieved from https://www.fhi.ox.ac.uk/wp-content/uploads/Deciphering_Chinas_AI-Dream.pdf

to building an AI industrial park and the Chinese government identified several national champion Chinese companies to lead the widespread deployment of AI technologies[107]. The total spending on AI systems in China is estimated at $12 billion for the year 2017 with growth slated to reach $70 billion by 2020[108].

Looking to the East, the U.S. saw a looming threat to their technological dominance, and indeed their national security. The idea of an 'AI arms race' took swift hold. Before 2016, there were fewer than 300 Google results for 'AI arms race'; today, the term yields over 50,000 hits[109] and publications such as the Wall Street Journal[110] and the Guardian[111] explicitly warn of an impending AI arms race between the U.S. and China[112]. Well-respected technology leaders have stoked the fires with prescriptions of China's impending dominance in AI. Eric Schmidt, former CEO and Executive Chairman of Google, warned that 'by 2020, [the Chinese] will have caught up [to the United States]. By 2025, they will be better than us. And by 2030, they will dominate the industries of AI'[113]. Kai-Fu Lee, a well-known Chinese venture capitalist and AI expert, predicted China's rapid rise to global leadership in AI, likely surpassing the U.S. on the way[114].

---

[107] (Ding, 2018)
[108] Pawlyk, O. (2018). China Leaving US Behind on Artificial Intelligence: Air Force General. *Military.Com*. Retrieved from https://www.military.com/defensetech/2018/07/30/china-leaving-us-behind-artificial-intelligence-air-force-general.html
[109] Zwetsloot, R., Toner, H., & Ding, J. (2018). Beyond the AI Arms Race. *Foreign Affairs*. Retrieved from https://www.foreignaffairs.com/reviews/review-essay/2018-11-16/beyond-ai-arms-race
[110] Barnes, J. E., & Chin, J. (2018). The New Arms Race in AI. *Wall Street Journal*. Retrieved from https://www.wsj.com/articles/the-new-arms-race-in-ai-1520009261
[111] Busby, M. (2018). Killer robots: pressure builds for ban as governments meet. *The Guardian*. Retrieved from https://www.theguardian.com/technology/2018/apr/09/killer-robots-pressure-builds-for-ban-as-governments-meet
[112] A sincere thank you to Remco Zwetsloot and Jeffrey Ding for providing me with these references to arms race narratives.
[113] Schmidt, E. (2017). *Eric Schmidt Keynote Address at the Center for a New American Security Artificial Intelligence and Global Security Summit*. Retrieved from Center for a New American Security website: https://www.cnas.org/publications/transcript/eric-schmidt-keynote-address-at-the-center-for-a-new-american-security-artificial-intelligence-and-global-security-summit
[114] Lee, K.-F. (2018). AI Superpowers: China, Silicon Valley, and the New World Order. Houghton Mifflin Harcourt.

This has led to demands of the U.S. government to respond in kind – with speed, strategy, and an impetus to win the race against China. Prominent defense and security figures have been at the forefront of these clarion calls. Former Deputy Secretary of Defense Robert Work has argued that China's advances in AI should spark a 'Sputnik moment' for the U.S.'[115]; senior Air Force official Lieutenant General Jamieson invoked the threat from China to push for changes within the Air Force towards rapid integration of AI[116]. Washington D.C. thinktank analysts have advocated for the Pentagon to 'push ahead as quickly as possible on integrating well-proven AI technologies into [military] operational capabilities' lest the U.S. lose their 'slim edge over China in the AI arms race'[117]. Indeed, the rhetoric has gone so far as to warn of a Cold War where 'the world's most powerful nations are rapidly retreating into positions of competitive isolation'[118].

7.3.1.2 A defense-oriented American national strategy on AI

The launch of the Third Offset Strategy marked a turn of focus by the U.S. government to the development and deployment of autonomous technologies. The Third Offset Strategy was first announced in November 2014[119] and has remained the dominant military doctrine through to the current administration[120]. Central to the doctrine is the pursuit of AI

---

[115] Clark, C. (2017). Our Artificial Intelligence 'Sputnik Moment' Is Now: Eric Schmidt & Bob Work. *Breaking Defense*. Retrieved from https://breakingdefense.com/2017/11/our-artificial-intelligence-sputnik-moment-is-now-eric-schmidt-bob-work/

[116] (Pawlyk, 2018)

[117] Auslin, M. (2018). Can the Pentagon Win the AI Arms Race? *Foreign Affairs*. Retrieved from https://www.foreignaffairs.com/articles/united-states/2018-10-19/can-pentagon-win-ai-arms-race

[118] (Bremmer, 2018)

[119] Carter, A. (2016). *Keynote Address: The Path to the Innovative Future of Defense*. Presented at the Center for Strategic and International Studies: Assessing the Third Offset Strategy: Progress and Prospects for Defense Innovation, CSIS Headquarters, Washington, D.C. Retrieved from https://csis-prod.s3.amazonaws.com/s3fs-public/event/161028_Secretary_Ashton_Carter_Keynote_Address_The_Path_to_the_Innovative_Future_of_Defense.pdf; Martinage, R. (2014). *Toward a New Offset Strategy: Exploiting U.S. Long-Term Advantages to Restore U.S. Global Power Projection Capability*. Retrieved from Center for Strategic and Budgetary Assessments website: https://csbaonline.org/research/publications/toward-a-new-offset-strategy-exploiting-u-s-long-term-advantages-to-restore

[120] Johnson, T. R. (2016). Donald Trump's Pentagon and the Future of the Third Offset Strategy: Will the Department of Defense Invest in People or Technology? *The Atlantic*. Retrieved from https://www.theatlantic.com/politics/archive/2016/11/trump-military-third-offset-strategy/508964/

technologies – the stated aim is to 'exploit all advances in artificial intelligence and autonomy and to insert them into the Defense Department's battle networks'[121]. The five pillars identified for the future of the U.S. military reflect this focus, emphasising pursuit of autonomous deep learning machine systems, human-machine collaboration and combat teaming, and network-enabled semi-autonomous weapons[122]. The most evident areas of investment in this vein has been in unmanned aerial systems (UAS). U.S. spending on UAS grew tenfold from $283 million in 2000 to $2.9 billion in 2016; relatedly, the U.S. inventory of UAS increased by a 65-fold from 167 to 11,000 between 2002 and 2013. In 2013, the DOD published an 'Unmanned Systems Integration Roadmap' in an effort to formulate a streamlined strategy for further developing UAS between 2013 and 2038[123].

As the military utility of AI technologies became increasingly compelling, the U.S. defense and security communities began to divert substantial strategic attention and resources towards accelerating military applications of AI. In 2016 the DOD's Defense Science Board published a 'Summer Study on Autonomy' centred on the development of 'strategies to widen the use of autonomy' and 'accelerate the advancement of the technology for autonomous applications and capabilities'. The study recommended that the DOD 'take immediate action to accelerate its exploitation of autonomy while also preparing to counter autonomy employed by adversaries'[124]. Further, military uses of AI are mentioned in both

[121] Leung, J., & Fischer, S.-C. (2018). JAIC: Pentagon debuts artificial intelligence hub. *Bulletin of the Atomic Scientists*. Retrieved from https://thebulletin.org/2018/08/jaic-pentagon-debuts-artificial-intelligence-hub/
[122] Financial Times (FT). (2015). The Future Military-Artificial Intelligence Complex? *Financial Times*. Retrieved from https://ftalphaville.ft.com/2015/12/15/2147846/the-future-military-artificial-intelligence-complex/
[123] Department of Defense (DOD). (2014). *Unmanned Systems Integrated Roadmap: FY2013-2038*. Retrieved from Department of Defense website: https://apps.dtic.mil/dtic/tr/fulltext/u2/a592015.pdf
[124] Defense Science Board. (2016). *Summer Study on Autonomy*. Retrieved from United States Defense Science Board website: https://www.hsdl.org/?abstract&did=794641

the 2017 U.S. National Security Strategy[125] and the 2018 National Defense Strategy[126], following an announcement from the DOD of its intention to 'invest broadly in military application of autonomy, artificial intelligence, and machine learning'.

In view of the looming narrative of a U.S.-China AI race, the year 2018 saw the U.S. government pay more focused attention towards AI as a matter of national priority. In particular, Secretary of Defense Jim Mattis took it upon himself to address a memorandum to President Trump in May 2018, arguing that the U.S. needed a 'whole of country' national strategy for AI in order to remain competitive with China[127]. Mattis emphasized the importance of leading particularly in the realm of defense. Then, in August 2018, President Trump signed the National Defense Authorisation Act (NDAA) which solidified the role of AI technologies in delivering on U.S. defense priorities. Among other things, the NDAA established a National Security Commission for Artificial Intelligence whose role will be to assess how the DOD can leverage AI for national security[128]. The Pentagon also established the Joint Artificial Intelligence Center (JAIC) – a new institution intended to synchronise and accelerate AI activities and capabilities throughout the DOD, charged with overseeing and growing DOD's AI projects of which there are currently approximately six hundred[129].

7.3.1.3 The emergence of private-sector led self-governance

Phase 2 also saw the emergence of private sector led initiatives to self-govern the development and deployment of AI technologies. In the words of Google's CEO Sundar Pichai: 'How AI

---

[125] The United States Government. (2017). *National Security Strategy of the United States of America*. Retrieved from The White House website: https://partner-mco-archive.s3.amazonaws.com/client_files/1513628003.pdf

[126] Department of Defense (DOD). (2018). *Summary of the 2018 National Defense Strategy of the United States of America*. Retrieved from The White House website: https://dod.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf

[127] Metz, C. (2018). Artificial Intelligence Is Now a Pentagon Priority. Will Silicon Valley Help? *The New York Times*. Retrieved from https://www.nytimes.com/2018/08/26/technology/pentagon-artificial-intelligence.html

[128] McCain, J. S. National Defense Authorization Act for Fiscal Year 2019. , Pub. L. No. H.R.5515 (2018).

[129] (Leung & Fischer, 2018)

is developed and used will have a significant impact on society for many years to come' which, for Google, means 'we feel a deep responsibility to get this right'[130]. Microsoft's Satya Nadella has called for global cooperation on AI as a necessary and inevitable company investment[131]. Baidu's former Vice President and Chief Scientist, Andrew Ng, expects leaders in AI to acknowledge that "it is incumbent on all of us to make sure we are building a world in which every individual has an opportunity to thrive"[132]. DeepMind's CEO Demis Hassabis has emphasized the importance of focusing on coordination rather than competition in order 'to avoid this harmful race to the finish where corner-cutting starts happening, and safety gets cut'[133].

Beyond intention, some have begun to translate this into action. In June 2018, Google articulated a set of AI principles, resting on a commitment to have their AI systems 'be socially beneficial' and 'be built and tested for safety'. They have since followed this with publishing a set of Responsible AI Practices which are set to be updated quarterly, as well as initiating a number of other projects – including ethics training for their employees and putting in place a formal review structure to assess new projects, products and deals – to translate their AI principles into practice[134]. OpenAI, a San Francisco based AI lab, have similarly published a charter expressing their commitment to developing artificial general intelligence (AGI) in line with realising broadly distributed benefits to humanity, and have invested heavily in safety-oriented AI research[135]. DeepMind has established an Ethics and

---

[130] (Pichai, 2018)
[131] Hauteville, J.-M. (2017). Satya Nadella: Calling for Global Cooperation on Artificial Intelligence. *Handelsblatt TODAY*. Retrieved from https://www.handelsblatt.com/today/companies/satya-nadella-calling-for-global-cooperation-on-artificial-intelligence/23565430.html
[132] Ng, A. (2016). What Artificial Intelligence Can and Can't Do Right Now. *Harvard Business Review*. Retrieved from https://hbr.org/2016/11/what-artificial-intelligence-can-and-cant-do-right-now
[133] DeepMind Ethics & Society. (n.d.)). DeepMind Ethics & Society Principles. Retrieved from DeepMind website: https://deepmind.com/applied/deepmind-ethics-society/principles/
[134] Walker, K. (2018). Google AI Principles updates, six months in. Retrieved April 5, 2019, from Google Blog: The Keyword website: https://www.blog.google/technology/ai/google-ai-principles-updates-six-months/
[135] OpenAI. (2018). OpenAI Charter. Retrieved April 5, 2019, from OpenAI website: https://openai.com/charter/

Society team, reporting directly to one of their co-founders[136]; Microsoft have similarly set up their AI and Ethics in Engineering Research (AETHER) committee[137], and Facebook reportedly have a similar in-house ethics team[138].

[136] (DeepMind Ethics & Society, n.d.)
[137] Mulholland, M. (2018). Our shared responsibility for AI. Retrieved April 5, 2019, from Microsoft Partner Network website: https://blogs.partner.microsoft.com/mpn/shared-responsibility-ai-2/
[138] Shead, S. (2018). Facebook Reportedly Has A Dedicated AI Ethics Team. *Forbes*. Retrieved from https://www.forbes.com/sites/samshead/2018/05/03/facebook-reportedly-has-a-dedicated-ai-ethics-team/

7.4 Taking stock, looking ahead

Artificial intelligence is a case in motion – events on a daily and monthly basis continue to add texture to the political dynamics of AI. Nevertheless, observing the behaviours of states, firms, and the AI research community thus far reveals some sense of the direction in which we may expect these actors, and the relationships between them, to evolve. Section 7.4.1 and section 7.4.2 therefore take stock of what we know today – of the evolution of the actors' goals, resources, and constraints, and of the evolution of the strategic relationships at play between them. Then, section 7.4.3 looks ahead to what we may expect to see in the coming years as the politics of AI unfolds.

7.4.1 The evolution of actors

7.4.1.1 Actor goals

AI is a civilian-first strategic GPT[139]. The Dartmouth Summer Project of 1956 was envisioned as an intellectual endeavour; the second and third waves of AI breakthroughs were largely seeded by academic institutions first and foremost, followed by industry labs. While the DOD did express an interest in AI, this interest waxed and waned across phase 1.

As a civilian-first technology, in the main AI initially captured the state's interest for its potential economic value. The goal of pursuing AI for its military value emerged later, and only really became central with the onset of the Third Offset Strategy in 2014. Similarly, concerns over the risks posed by AI only became a central focus for the state in very recent years. This has taken two forms. Firstly, the emergence of China as a technological competitor has led to the perception of the proliferation of AI technologies and research as a national security risk. Secondly, the increased levels of public concern for the harm that

[139] As per the distinction drawn in Chapter 6 between defense-first and civilian-first technologies.

could be caused by the irresponsible deployment of AI technologies has encouraged the state to focus more on the social and economic risks from AI.

For firms, the goal to maximise profit remains consistent. Specifically, the emergence of expert systems spurred the first spike in private sector activity in AI, and the deep learning paradigm led to the rapid commercialisation of AI technologies from phase 2 onwards. The goal for AI researchers has also remained consistent across the technology life cycle.

7.4.1.2 Actor resources & constraints

The provision of AI *R&D funding* has shifted away from the state and towards firms. Certainly, the field of AI was very much born out of the U.S. government's initial investments, primarily channelled through DARPA and the IPTO. However, from the early 2000s onwards AI R&D funding began to pour in via private investments and industry expenditure. A total of over $17 billion was invested privately in AI technologies between 2009 and 2014[140]; as of 2016, the annual rate of investment was approximately $2.4 billion[141]. The trend continues to point steadfastly upwards: between 2013 and 2017, the amount of venture capital investment in AI companies increased by close to five-fold[142].

The world's largest technology companies account for a large portion of this private funding[143]. In 2017, Amazon and Alphabet invested $16.1 billion and $13.9 billion in total R&D, respectively, far outstripping the government's investments in autonomous and

[140] Faggella, D. (2019). Valuing the Artificial Intelligence Market, Graphs and Predictions | Emerj - Artificial Intelligence Research and Insight. *Emerj*. Retrieved from https://emerj.com/ai-sector-overviews/valuing-the-artificial-intelligence-market-graphs-and-predictions/

[141] Furman, J. (2016). Is This Time Different? The Opportunities and Challenges of Artificial Intelligence [Remarks at AI Now: The Social and economic Implications of Artificial Intelligence Technologies in the Near Term]. Retrieved from New York University website: https://obamawhitehouse.archives.gov/sites/default/files/page/files/20160707_cea_ai_furman.pdf

[142] Comparably, the amount of venture capital funding in general increased by 2.08x. See: (Shoham et al., 2018)

[143] For an overview of AI investments by sector, see: Bank of America Merrill Lynch. (2015). *Robot Revolution - Global Robot & AI Primer*. Retrieved from Bank of America Merrill Lynch website: http://www.bofaml.com/content/dam/boamlimages/documents/PDFs/robotics_and_ai_condensed_primer.pdf

unmanned systems which totalled to $5.3 billion in the 2019 budget[144]. Long-standing industries which have had a tradition of investing heavily in R&D have also entered into the AI fray. For example, leaders in the automotive industry such as Toyota[145], Ford[146], and Mercedes-Benz[147] have invested over $1 billion in AI research. Similarly, large players in the pharmaceutical industry have funded AI in drug discovery and healthcare services[148].

Innovation capacity in the AI field has consistently been the stronghold of firms and researchers; the state has never developed comparable in-house innovation capacity in AI. The innovation capacity of firms has scaled in recent years. As one metric of this, between January 2015 and January 2018 the number of active AI start-ups increased by over two times[149]. This is set to keep growing as the AI industry continues to scale. Andrew Ng, former Vice President and Chief Scientist at leading Chinese AI firm, Baidu, reflected the seemingly boundless commercial potential of AI: 'I have a hard time thinking of an industry we cannot transform with AI'[150].

Given the talent bottleneck facing the AI industry, the innovation capacity of AI researchers currently appears to be a valuable resource, as does their ability to hold political weight to pressure firms and the state (section 7.4.2.6). This may shift with time as the supply of AI

---

[144] This is the combined budget the National Sciences Foundation, DARPA, and the Department of Transport. See: United States Government. (2018). *United States Government Budget FY2019: Research and Development*. Retrieved from The White House website: https://www.whitehouse.gov/wp-content/uploads/2018/02/ap_18_research-fy2019.pdf

[145] Metz, R. (2015). Toyota Investing $50M for Autonomous-Car Research at Stanford and MIT. *MIT Technology Review*. Retrieved from https://www.technologyreview.com/s/541046/toyota-investing-50m-with-stanford-mit-for-autonomouscar-research/

[146] Isaac, M., & Boudette, N. E. (2017). Ford to Invest $1 Billion in Artificial Intelligence Start-Up. *The New York Times*. Retrieved from https://www.nytimes.com/2017/02/10/technology/ford-invests-billion-artificial-intelligence.html

[147] Bergen, M. (2015). Mercedes-Benz Wants to Beat Google, Uber to Our Driverless Future. *Recode*. Retrieved from http://www.recode.net/2015/11/26/11620962/mercedes-benz-wants-to-beat-google-uber-to-our-driverlessfuture

[148] CB Insights. (2017). From Virtual Nurses To Drug Discovery: 106 Artificial Intelligence Startups In Healthcare. Retrieved from CB Insights Research Briefs website: https://www.cbinsights.com/research/artificial-intelligence-startups-healthcare/

[149] Comparably, the number of active start-ups increased by 1.3x. See: (Shoham et al., 2018)

[150] Zhang, S. (2017). China's Artificial-Intelligence Boom. *The Atlantic*. Retrieved from https://www.theatlantic.com/technology/archive/2017/02/china-artificial-intelligence/516615/

researchers increases, as industry labs turn to more directly commercially focused R&D strategies, and/or as the state becomes more willing to constrain the activities of researchers and research institutions via legislation.

The *legislative environment* is poised to become more constraining on firms and researchers as the state more actively seeks to shape and bound the development and deployment of AI technologies. We already see indications of this being the case. For one, the topic of AI barely featured in the U.S. Congress before the year 2016[151]. Then, within months of one another, the House Energy and Commerce Committee held a hearing on Advanced Robotics and the Senate Joint Economic Committee held the first ever hearing focused solely on AI on November 30, 2016. Since, there have been a further seven hearings in the U.S. Congress centred on themes of artificial intelligence, the most recent of which recommended increased engagement by the U.S. Congress on AI[152]. Further, six AI related bills have been introduced in 2017 and 2018[153]. Four of these concerned AI more generally[154] while two relate specifically

[151] (Shoham et al., 2018)

[152] These have included:

- *The Dawn of Artificial Intelligence:* Senate, Commerce, Subcommittee on Space, Science and competitiveness, November 2016
- *Digital Decision Making: The Building Blocks of Machine Learning and Artificial Intelligence*: Senate, Commerce, Subcommittee on Communications, Technology, Innovation and the Internet, December 2017
- *China's pursuit of emerging and exponential technologies:* House, Armed Services, Subcommittee on Emerging Threats and Capabilities, January 2018
- *Game Changers: Artificial Intelligence:* House, Oversight and Government Reform, Subcommittee on Information Technology, February 2018 (Part I, II and III were held as three separate hearings)
- *Artificial Intelligence: With Great Power Comes Great Responsibility:* House, Science, Subcommittee on Energy and Research & Technology, June 2018

[153] A sincere thank you to Remco Zwetsloot for pointing me towards these bills.

[154] The four bills are as follows:

- *Future of AI Act (12/20187, H.R. 4625 / S. 2217) - Fundamentally Understanding the Usability and Realistic Evolution of Artificial Intelligence*: The primary goal of this bill is to address workforce changes caused by AI, and support the unbiased development and application of AI, and protect the privacy rights of individuals. See: https://www.congress.gov/bill/115th-congress/house-bill/4625/text
- *AI JOBS Act (1/2018, H.R. 4829) – Artificial Intelligence Job Opportunities and Background Summary Act:* See https://www.congress.gov/bill/115th-congress/house-bill/4829/text
- *National Security Commission on Artificial Intelligence Act (3/2018, H.R. 5356):* See https://www.congress.gov/bill/115th-congress/house-bill/5356/text. Note that this bill was folded into the 2019 National Defense Authorisation Act (NDAA); see https://www.congress.gov/bill/115th-congress/house-bill/5515/text/rh/
- *Artificial Intelligence in Government Act (9/2018, S. 3502):* See: https://www.congress.gov/bill/115th-congress/senate-bill/3502/text

to autonomous vehicles, aiming to regulate the deployment of these technologies on American roads[155].

Public concern over the societal consequences of AI has thus far largely centred on the actions of AI firms deploying these technologies. Indeed, a cynical perspective would explain the rise of private-sector led self-governance (section 7.3.1.3) as a hurried response from companies following the series of high profile, widely criticised chain of 'AI accidents' that characterised much of the coverage that these large firms received across 2018[156]. For example, Facebook was accused of inciting ethnic cleansing in Myanmar[157], hosting fake Russian accounts on its network[158], and breaching the privacy of millions of its users[159]. Uber faced the repercussions of causing the first fatality caused by a self-driving car[160]. IBM reportedly produced 'unsafe and incorrect' cancer treatment recommendations through their Watson system[161]. To a lesser extent, public concern has also increased as a constraint on the state insofar as it has generated demands on the state to regulate AI firms.

---

[155] The two bills are as follows:
- *SELF DRIVE Act (7/2017, H.R. 3388) – Safety Ensuring Lives Future Deployment in Research in Vehicle Evolution Act:* See https://www.congress.gov/bill/115th-congress/house-bill/3388
- *AV START Act (9/2018, S. 1885) – American Vision for Safer Transpiration through Advancement of Revolutionary Technologies Act:* See https://www.congress.gov/bill/115th-congress/senate-bill/1885/text

[156] For a thorough review of such events across the year 2018, see: AI Now Institute. (2018). AI in 2018: A Year in Review. Retrieved from AI Now Institute Blog website: https://medium.com/@AINowInstitute/ai-in-2018-a-year-in-review-8b161ead2b4e?_hsenc=p2ANqtz--C_ZUXgmw0DPz2_QDAM70a27Mzyxoc_Y70F6UtFHxYQCSLhZ8DubXSSw3X3nRA8pMD3vBgCHTBOm0d3ZlZ9VQhpqEAPg&_hsmi=68751142

[157] Bloomberg Opinion Editorial Board. (2017). Think the U.S. Has a Facebook Problem? Look to Asia. *Bloomberg Opinion*. Retrieved from https://www.bloomberg.com/opinion/articles/2017-10-22/facebook-has-a-bigger-problem-than-washington

[158] Weise, E. (2017). Russian fake accounts showed posts to 126 million Facebook users. *USA TODAY*. Retrieved from https://www.usatoday.com/story/tech/2017/10/30/russian-fake-accounts-showed-posts-126-million-facebook-users/815342001/

[159] Granville, K. (2018). Facebook and Cambridge Analytica: What You Need to Know as Fallout Widens. *The New York Times*. Retrieved from https://www.nytimes.com/2018/03/19/technology/facebook-cambridge-analytica-explained.html

[160] Etherington, D. (2018). An Uber self-driving car in autonomous mode hit and killed a pedestrian in Tempe, Arizona. *TechCrunch*. Retrieved from https://techcrunch.com/2018/03/19/uber-self-driving-test-car-involved-in-accident-resulting-in-pedestrian-death/

[161] Ross, C., & Swetlitz, I. (2018). IBM's Watson supercomputer recommended 'unsafe and incorrect' cancer treatments, internal documents show. *STAT+*. Retrieved from https://www.statnews.com/wp-content/uploads/2018/09/IBMs-Watson-recommended-unsafe-and-incorrect-cancer-treatments-STAT.pdf

Researchers have to some extent channelled this public concern as a political resource. As a case in point, when Google, Amazon, and Microsoft, among several others, were revealed to be engaged in government contracts that would make them complicit with the Trump administration's controversial family separation policy, this triggered a wave of dissent and protest by researchers employed at these firms[162]. As a workforce, researchers have also reflected public concerns with respect to the use of AI technologies for defense purposes (section 7.4.2.5). On the mitigation of AI risks more generally, notable examples of researcher-led advocacy initiatives include the AI Now Institute at New York University and the Association for the Advancement of Artificial Intelligence (AAAI).

Table 7.4-1: Summary of evolution of AI actors

		State	*Firms*	*Researchers*
Goals		Economic growth = Military leadership ↑ Risk mitigation ↑	Maximise profit =	Pursue research =
Resources and constraints	*R&D funding*	Resource ↓	Resource ↑	Constraint =
	Innovation capacity	Resource ↓	Resource ↑	Resource ↓
	Legislative environment	Resource ↑	Constraint ↑	Constraint ↑
	Public concern	Constraint ↑	Constraint ↑	Resource =

Notes:
↑ means that the goal / resource / constraint becomes more advantageous / constraining as the technology matures
↓ means that the goal / resource/constraint becomes less advantageous / constraining as the technology matures
= means that the goal / resource / constraint remains constant as the technology matures

7.4.2 The evolution of actor relationships

7.4.2.1 State depends on access to commercial technologies

In light of the shift away from public to private hubs of AI R&D, the U.S. government have realised the need for them to build closer relationships with U.S.-based technology

[162] Paulas, R. (2018). A New Kind of Labor Movement in Silicon Valley. *The Atlantic*. Retrieved from https://www.theatlantic.com/technology/archive/2018/09/tech-labor-movement/567808/

companies if they are to reap the fruits of the growing private AI industry. The state's dependence on firms to produce leading edge commercial technologies is therefore a synergy that has and will likely continue to strengthen, particularly as AI becomes more critical to the U.S. military technology base[163].

Indeed, the state has already taken steps to address this growing gap between Silicon Valley and Washington D.C. In 2016 the DOD created the Defense Innovation Board (DIB). The goal of the DIB is to advise the Secretary of Defense on matters of innovation and cooperation with the technology sector. A prominent recommendation from the DIB's first report was to 'catalyse innovation in artificial intelligence and machine learning' by 'expand[ing] exchange programs and collaborations with industry and academic experts in the field'[164]. The Defense Innovation Unit (DIU; formerly DIUx) was also established in 2015. Stationed in Silicon Valley, DIU was set up to help the U.S. military take advantage of emerging technologies, including AI. Further, in May 2018 President Trump hosted a Summit on Artificial Intelligence for American Industry at the White House. The goal of the event was to encourage firms to capitalise on the 'free market approach' of the Trump administration to 'develop their next generation inventions right here in the United States', emphasizing the importance of American AI companies to the nation's strategy to win against China[165].

7.4.2.2 State creates supportive R&D environment

While the U.S. government is currently a minor player in terms of supporting AI R&D, there are some indications that the state may become more focused on creating a supportive

[163] Segal, A. (2017). *Rebuilding Trust Between Silicon Valley and Washington*. Retrieved from Council on Foreign Relations website: https://www.cfr.org/report/rebuilding-trust-between-silicon-valley-and-washington
[164] Defense Innovation Board (DIB). (n.d.). Defense Innovation Board: Recommendations. Retrieved from Defense Innovation Board website: https://innovation.defense.gov/Recommendations/
[165] Office of Science and Technology Policy. (2018a). *Summary of the 2018 White House Summit on Artificial Intelligence for American Industry*. Retrieved from The White House website: https://www.whitehouse.gov/wp-content/uploads/2018/05/Summary-Report-of-White-House-AI-Summit.pdf

environment for AI researchers and industry. Following the Summit on Artificial Intelligence in May 2018, a Select Committee on AI was created to advise the White House on AI R&D priorities and to lead on a partnership strategy with academia and industry[166]. Further, a White House fact sheet issued in May 2018 titled 'Artificial Intelligence for the American People' placed funding AI R&D as the highest priority of six areas, and further flagged that President Trump's FY2019 Budget Request was the first to name AI as an R&D priority[167]. Then, in July, a memorandum to the Heads of Executive Departments and Agencies from the Trump Administration affirmed the importance of AI R&D as a priority in the FY2020 Research and Development budget[168].

The increase in support from the state has underscored AI as a defense and security priority, specifically. The National Defense Authorization Act (NDAA) for 2019, for example, increased funding for AI defense technologies from $16 million to $92.1 million – a 580% increase[169]. In September 2018, DARPA announced its own programme – the AI Next Campaign – which would commit $2 billion over the coming five years to advance state-of-the-art AI research[170]. More recently, in February 2019, President Trump signed an executive

---

166 Office of Science and Technology Policy (2018b). Readout from the Inaugural Meeting of the Select Committee on Artificial Intelligence. Retrieved from White House OSTP website: https://epic.org/privacy/ai/WH-AI-Select-Committee-First-Meeting.pdf

167 The White House. (2018). *Artificial Intelligence for the American People*. Retrieved from https://www.whitehouse.gov/briefings-statements/artificial-intelligence-american-people/

168 The memorandum was written by Mick Mulvaney, Director of the Office of Management and Budget, and Michael Kratsios, Deputy Assistant to the President in the Office of Science and Technology Policy. See: Mulvaney, M., & Kratsios, M. (2018). *Memorandum for the Heads of Executive Departments and Agencies: FY 2020 Administration Research and Development Budget Priorities*. Retrieved from https://www.whitehouse.gov/wp-content/uploads/2018/07/M-18-22.pdf

169 Cassano, J. (2018). Pentagon's Artificial Intelligence Programs Get Huge Boost in the NDAA. *Sludge*. Retrieved from https://readsludge.com/2018/08/15/pentagons-artificial-intelligence-programs-get-huge-boost-in-the-ndaa/

170 DARPA sees the next generation of AI as a third wave of technological advance, centred on contextual adaptation. Under the AI Next Campaign, key areas that will be explored will include: automating critical DOD business processes; improving the robustness and reliability of AI systems; enhancing the security and resiliency of machine learning and AI technologies; and pioneering next generation AI algorithms and applications. Over the first 12 months of the Campaign, DARPA plans to issue multiple Broad Agency Announcements for new programs, in addition to pursuing its current 20 programs exploring state-of-the-art AI and over 60 programs applying AI in some capacity. See: Defense Advanced Research Projects Agency (DARPA). (2018). DARPA Announces $2 Billion Campaign to Develop Next Wave of AI Technologies. Retrieved from DARPA website: https://www.darpa.mil/news-events/2018-09-07

order launching the American AI Initiative. The order elevated the development of AI as a prominent national priority which would herein receive concerted government support, in view of the security threat posed by China[171].

7.4.2.3 Firms create supportive R&D environment

As noted in section 7.4.1.2, AI R&D has become increasingly led by firms. Indicatively, in 2017 the proportion of AI papers that were published from corporate labs was double the proportion published from government-funded labs[172]. To create a supportive R&D environment for researchers, firms have pursued a range of strategies, including raising researcher salaries[173], mirroring the culture of academic research labs, and selecting which cities to open up headquarters in based on the presence of key researchers at local institutions[174]. One should expect firms to continue to create supportive R&D environments for AI researchers insofar as the commercial AI sector continues to grow.

7.4.2.4 State prevents firms and researchers from proliferating AI technologies

The perceived threat from China has, of late, provided a basis for the U.S. government to prevent the proliferation of American AI technologies and research beyond national borders.

---

[171] The initiative aims to achieve five key priorities:
- *Redirect funding*: The order directs federal funding agencies to prioritise investments in artificial intelligence;
- *Create resources:* It seeks to make federal data, computer models, and computing resources available to AI researchers;
- *Establish standards:* It directs the National Institute of Standards and Technology to create standards that foster the development of reliable, robust, trustworthy, secure, portable, and interoperable AI systems;
- *Retrain workers:* It asks agencies to prioritise preparing workers for the changes brought about by AI through apprenticeships, skills programs, and fellowships;
- *Engage internationally:* It calls for a strategy for international collaboration that ensures AI is developed in a way consistent with American values and interests.

See: The White House. *Executive Order on Maintaining American Leadership in Artificial Intelligence*., (2019).

[172] (Shoham et al., 2018)

[173] Paysa. (2017). U.S. Companies Raising $1 Billion or More to Fuel Artificial Intelligence (AI) Development Looking to Staff 10,000+ Openings, Cites New Paysa Research. *Global News Wire*. Retrieved from https://www.globenewswire.com/news-release/2017/04/18/961603/0/en/U-S-Companies-Raising-1-Billion-or-More-to-Fuel-Artificial-Intelligence-AI-Development-Looking-to-Staff-10-000-Openings-Cites-New-Paysa-Research.html

[174] (Goldfarb & Trefler, 2018)

Two particular areas of activity are of note here. Firstly, on the prevention of foreign direct investment from China into U.S. AI companies – the Committee on Foreign Direct Investment in the United States (CFIUS) has in recent years been used to block several attempts from Chinese buyers to invest in or acquire U.S. high-technology companies, notably those relevant to the AI software and hardware industries[175]. Then, on June 22, 2017, a bill was proposed to reform the authority and operation of CFIUS, nominally in response to a DOD report issued in early 2017 warning of China's strategies to circumvent CFIUS to gain access to critical technologies such as AI, robotics, and semiconductors[176]. The bill – known as the Foreign Investment Risk Review Modernization Act (FIRMA) – was written into law in August 2018[177].

Secondly, on the prevention of the export of AI technologies – on November 19, 2018, the Department of Commerce issued an Advanced Notice of Proposed Rulemaking (ANPRM) indicating an intention to revise U.S. export control rules to include 'emerging technologies' that are considered critical to U.S. national security. Among the technologies identified, the most extensive section is dedicated to AI[178]. While the outcomes of this process are still to be determined, it is clear that U.S. lawmakers are increasingly willing to exercise the legislative

---

[175] Roumeliotis, G., & Bartz, D. (2017). Exclusive: U.S. toughens stance on foreign deals in blow to China's buying spree. *Reuters*. Retrieved from https://www.reuters.com/article/us-usa-china-companies-idUSKBN1A532M

[176] The report in question was published by the Defense Innovation Unit Experimental (DIUx) – see Brown, M., & Singh, P. (2018). China's Technology Transfer Strategy: How Chinese Investments in Emerging Technology Enable A Strategic Competitor to Access the Crown Jewels of U.S. Innovation. Retrieved from Defense Innovation Unit Experimental (DIUx) website: https://admin.govexec.com/media/diux_chinatechnologytransferstudy_jan_2018_(1).pdf

[177] A sincere thank you to Sophie-Charlotte Fischer for lending me her expertise and sources on the CFIUS reforms.

[178] The AI technologies under review include: (i) Neural Networks and Deep Learning (e.g., brain modelling, time series prediction, classification); (ii) Evolution and genetic computation (e.g., genetic algorithms, genetic programming); (iii) Reinforcement learning; (iv) Computer vision (e.g., object recognition, image understanding); (v) Expert systems (e.g., decision support systems, teaching systems); (vi) Speech and audio processing (e.g., speech recognition and production); (vii) Natural language processing (e.g., machine translation); (viii) Planning (e.g., scheduling, game playing); (ix) Audio and video manipulation technologies (e.g., voice cloning, deep fakes); (x) AI cloud technologies; or (xi) AI chipsets. See: Bureau of Industry and Security, Commerce. (2018). *Review of Controls for Certain Emerging Technologies*. Retrieved from https://www.federalregister.gov/documents/2018/11/19/2018-25221/review-of-controls-for-certain-emerging-technologies

tools at their disposal to restrict the proliferation of AI technologies to China and their other adversaries, in the name of national security.

Thus far the main targets of these state efforts have been AI products and firms. It remains unclear as to whether the state will begin to extend restrictions to apply to research, both in the form of knowledge as well as talent.

7.4.2.5 Firms face public backlash for selling technologies to the state

Phase 2 sees several trends converging to raise the stakes of firm-state collaboration. Namely, the state's interest in integrating AI technologies into their defense and security arsenals, particularly in the face of escalating strategic competition with China, means that the U.S. government is increasingly turning to private AI companies for their technologies and talent (section 7.4.2.1). Simultaneously, the heightened levels of scrutiny on AI companies, both from the public as well as from the researchers employed at these companies, has meant that firms are more likely to be disincentivised from engaging with the state on defense projects, given the ethics concerns that arise from doing so (section 7.4.1.2).

Across the year 2018, significant events brought these conflicting dynamics to the forefront[179]. Of note was the case of Project Maven. In April 2017, the Pentagon announced the Algorithmic Warfare Cross-Functional Team, otherwise known as 'Project Maven'. The goal of Project Maven was to 'accelerate the DOD's integration of big data and machine learning'[180]. One of the first projects was to augment and automate the processing of drone video footage to increase actionable intelligence. Project Maven was to be delivered in

[179] A sincere thank you to Nathan Calvin for digging up a lot of the relevant facts of these cases.
[180] Work, R. (2017). *Establishment of an Algorithmic Warfare Cross-Functional Team (Project Maven)*. Retrieved from http://dodcio.defense.gov/Portals/0/Documents/Project%20Maven%20DSD%20Memo%2020170425.pdf

partnership with several technology companies as contractors. On March 6, 2018, it was revealed that Google was one such company[181].

As soon as the story broke, Google employees mobilised to object to their employer being engaged in 'the business of war'[182]. Over 4,000 employees signed a letter to Google's CEO Sundar Pichai urging Google to cancel Project Maven and demanding that 'Google draft, publicise, and enforce a clear policy stating that neither Google nor its contractors will ever build warfare technology'[183]. A dozen or so employees resigned in protest[184]. Following continued friction between Google management and their employees, in June 2018 Google announced that it would not renew its Project Maven contract[185]. Several days later, Sundar Pichai released a set of AI principles ostensibly to guide the company's future work on AI; the principles included a commitment to not pursue AI weapons or other applications that are likely to cause harm or injury[186]. Further, in October 2018 Google withdrew from bidding for a large government cloud computing contract, citing their AI principles[187].

---

[181] Conger, K., & Cameron, D. (2018). Google is helping the Pentagon build AI drones. *Gizmodo*. Retrieved from https://gizmodo.com/google-is-helping-the-pentagon-build-ai-for-drones-1823464533

[182] Shane, S., & Wakabayashi, D. (2018). "The Business of War": Google employees Protest Work for the Pentagon. *The New York Times Magazine*. Retrieved from https://www.nytimes.com/2018/04/04/technology/google-letter-ceo-pentagon-project.html

[183] Menegus, B. (2018). Thousands of Google Employees Protest Company's Involvement in Pentagon AI Drone Program. *Gizmodo*. Retrieved from https://gizmodo.com/thousands-of-google-employees-protest-companys-involvem-1824988565

[184] Conger, K. (2018a). Google Employees Resign in Protest Against Pentagon Contract. *Gizmodo*. Retrieved from https://gizmodo.com/google-employees-resign-in-protest-against-pentagon-con-1825729300

[185] Conger, K. (2018b). Google Plans Not to Renew Its Contract for Project Maven, a Controversial Pentagon Drone AI Imaging Program. *Gizmodo*. Retrieved from https://gizmodo.com/google-plans-not-to-renew-its-contract-for-project-mave-1826488620

[186] Pichai, S. (2018). AI at Google: our principles. Retrieved from Google Blog: The Keyword website: https://www.blog.google/technology/ai/ai-principles/

[187] Pichai also cited that 'there were portions of the contract that were out of scope with our current government certifications', and repeated a complaint lodged by all non-Amazon companies bidding on JEDI that it would be more prudent for the DOD to pursue a multi-vendor approach. See Nix, N. (2018). Google Drops Out of Pentagon's $10 Billion Cloud Competition. *Bloomberg*. Retrieved from https://www.bloomberg.com/news/articles/2018-10-08/google-drops-out-of-pentagon-s-10-billion-cloud-competition

7.4.2.6 Researchers clash with firms on issues of ethics and societal consequences

Instances of AI firms facing public backlash for selling technologies to the state have often been in part caused by related conflicts between researchers and firms. As a 2018 report from the U.S. Department of Homeland Security flags, the importance of private sector cooperation for the achievement of national priorities is overshadowed with the concern that employees of these companies are increasingly prone to disputing the use of these technologies for defense and security purposes[188].

Such concerns have been raised by AI researchers since the days of the Strategic Computing Initiative (SCI)[189]. Indeed, the more that the DOD constrained AI researchers and labs to working on projects of military relevance across the 1970s and 1980s, the more controversy that this raised within the AI research community. The main group at the forefront of these debates was Computer Professionals for Social Responsibility (CPSR), who primarily raised concerns with respect to the SCI and its efforts to militarise advanced technologies such as AI. An excerpt from the organisation's statement regarding its campaign against the SCI reads as follows[190]:

> The SCI promotes the use of machine "intelligence", to control the operation of complex military under unpredictable circumstances. Our concern is that, particularly when the stakes are high, situations with extreme uncertainty are precisely the wrong environment for the application of artificial intelligence… Rather than increasing our security,

[188] 2018 Public-Private Analytic Exchange Program. (2018). *Emerging Technology and National Security*. Retrieved from Department of Homeland Security (DHS) website: https://www.dhs.gov/sites/default/files/publications/2018_AEP_Emerging_Technology_and_National_Security.pdf

[189] A sincere thank you to Nathan Calvin for finding this reference.

[190] Suchman, L. (1984). DARPA Strategic Computing Initiative: A progress report on the CPSR response. Retrieved from The Computer Professinoals for Social Responsibility Newsletter website: http://cpsr.org/prevsite/publications/newsletters/old/1980s/Spring1984.txt/

> past attempts to achieve superiority in new weapons technology have fuelled an arms race that has no foreseeable end.

Fast forward to August 2018, a controversial Google initiative known as 'Project Dragonfly' brought this firm-researcher conflict into sharp relief. Project Dragonfly was the name for Google's new effort to release a censored search engine in China[191]. The platform would remove results around human rights, democracy, peaceful protests, and other topics mandated for censorship by the Chinese Communist Party. It would also require users to link their accounts with verified cell phone numbers, enabling ease of user identification by the Chinese government[192].

As soon as the story broke of Project Dragonfly, Google came under sharp criticism from several sources, including the U.S. government[193], Google employees[194], and Amnesty International[195]. Members of the Google security and privacy team notably raised objections at several points but were reportedly ignored[196]. Then, in December 2018 it was reported that Google had lost access to data from 265.com, a Chinese website which Google acquired in 2008 and from which Google was storing searches in order to train Project Dragonfly on

---

[191] Notably, this marks Google's second attempt at launching such an effort; between 2006 and 2010, Google had operated a censored version of its search engine in China until a state-sponsored cyberattack in January 2010 targeting the Gmail accounts of Chinese human rights activists led Google to exit mainland China., See Google. (2010a). A new approach to China. Retrieved from Google Official Blog website: https://googleblog.blogspot.com/2010/01/new-approach-to-china.html; Google. (2010b). A new approach to China: an update. Retrieved from Google Official Blog website: https://googleblog.blogspot.com/2010/03/new-approach-to-china-update.html

[192] Gallagher, R. (2018a). Google Shut Out Privacy and Security Teams from Secret China Project. *The Intercept*. Retrieved from https://theintercept.com/2018/11/29/google-china-censored-search/

[193] Ashkenas, J. (2018). Sundar Pichai's Congressional Testimony on Google's Project Dragonfly. Retrieved from Observable website: https://observablehq.com/@jashkenas/sundar-pichais-congressional-testimony-on-googles-projec

[194] Google Employees Against Dragonfly. (2018). We are Google employees. Google must drop Dragonfly. Retrieved from Medium website: https://medium.com/@googlersagainstdragonfly/we-are-google-employees-google-must-drop-dragonfly-4c8a30c5e5eb

[195] Fang, L. (2018). Amnesty International to Stage Worldwide Protests Against Google's "Dystopian" Censored Search for China. *The Intercept*. Retrieved from https://theintercept.com/2018/11/26/google-dragonfly-project-china-amnesty-international/

[196] (Gallagher, 2018a)

Chinese users' search preferences[197]. The internal privacy team had not been alerted to the fact that Google was storing these searches; they confronted Google management on the grounds that such practices were likely in violation of Chinese law[198]. To resolve this internal disagreement, Google management subsequently moved several groups of engineers off Project Dragonfly, and the search engine has been restricted to training on data from Chinese immigrants outside of mainland China. Progress on Dragonfly was therefore substantially slowed, if not 'effectively ended'[199].

In this vein, AI researchers have led a series of public-facing efforts to cohere their views on what they consider ethical behaviour by the AI industry. The Asilomar AI Principles is the first notable effort to articulate a set of principles to promote the safe and beneficial development of AI. Published in January 2017, the principles emphasize themes such as safety, responsibility, preventing an AI arms race, and developing AI for the common good. To date they have been signed by 1,273 AI researchers, including Demis Hassabis of DeepMind, Yann LeCun of Facebook, Jeff Dean of Google, and Ilya Sutskever of OpenAI[200]. Leading AI researchers at Google, Apple, Amazon, DeepMind, Facebook, IBM, and Microsoft also banded together in 2016 to create the Partnership on AI (PAI), a multi-stakeholder organisation with the mandate to 'develop and share best practices', 'provide an open and inclusive platform for discussion and engagement', and 'identify and foster aspirational efforts in AI for socially beneficial purposes'[201].

---

[197] Gallagher, R. (2018b). Google's Secret China Project "Effectively Ended" After Internal Confrontation. *The Intercept*. Retrieved from https://theintercept.com/2018/12/17/google-china-censored-search-engine-2/
[198] Horwitz, J. (2017). A key question is at the heart of China's new cybersecurity law: Where should data live? *Quartz*. Retrieved from https://qz.com/999613/a-key-question-at-the-heart-of-chinas-cybersecurity-law-where-should-data-live/
[199] (Gallagher, 2018b)
[200] Future of Life Institute. (2017). Asilomar AI Principles. Retrieved from https://futureoflife.org/ai-principles/?cn-reloaded=1
[201] Partnership on AI (PAI). (n.d.). About - The Partnership on AI. Retrieved April 5, 2019, from https://www.partnershiponai.org/about/

7.4.3 Predicting the politics of AI

In glimpsing the transformative potential of AI, we may all too easily fall into narratives of novelty and exceptionalism – narratives which claim that AI could cause an unprecedented redistribution of global power and wealth, and thus the politics of AI could unfold in entirely unprecedented ways. Indeed, current discourse surrounding AI can tend to move towards the extremes, hypothesizing that this time, things may be distinctly different from what we've ever seen before[202].

In response, looking to history encourages us to posit the opposite – that this time is unlikely to be different, or at least, not *that* different. In this section, we make predictions in this vein. These predictions are conservative by design. They do not propose anomalous events or outcomes, but rather extrapolate from observed trends in the nature of the actors, and the nature of their relationships. They do not feed prominent narratives of, for example, AI firms being too big to regulate[203] or AI researchers being a powerful political force against unethical companies[204]; rather, they extend historical narratives of states being capable of constraining

---

[202] A recent example of this type of rhetoric can be found in Schmidt, E., Kissinger, H., & Huttenlocher, D. (2019). The Metamorphosis. *The Atlantic*. Retrieved from https://www.theatlantic.com/magazine/archive/2019/08/henry-kissinger-the-metamorphosis-ai/592771/

[203] Examples of commentary in this vein include articles such as: Kaminska, I. (2017). When AI becomes too big to fail. *Financial Times*. Retrieved from http://ftalphaville.ft.com/2017/11/01/2195451/when-ai-becomes-too-big-to-fail/; Thomson, J. (2018). Are Amazon, Alphabet too big to regulate? *Australian Financial Review*. Retrieved from https://www.afr.com/chanticleer/tech-giant-numbers-amazon-alphabet-revenue-jump-revives-competition-debate-20180726-h13775; Wu, T. (2018). How Google and Amazon Got So Big Without Being Regulated. *Wired*. Retrieved from https://www.wired.com/story/book-excerpt-curse-of-bigness/. Notably this debate has been recently reinvigorated in the wake of antitrust investigations by the Department of Justice and the Federal Trade Commission targeted at Google, Amazon, Facebook, and Apple; see Chen, A. (2019). Regulating or breaking up Big Tech: an antitrust explainer. *MIT Technology Review*. Retrieved from https://www.technologyreview.com/s/613628/big-tech-breakup-regulation-antitrust-apple-amazon-google-facebook-doj-ftc-policy/; Schleifer, T. (2019). Why does Washington suddenly seem ready to regulate Big Tech? Look at the polls. *Vox*. Retrieved from https://www.vox.com/2019/6/4/18652469/washington-antitrust-regulate-amazon-google-facebook-look-at-polls

[204] Events such as those described in section 7.4.2.5 and 7.4.2.6 are often used to support this broader narrative of AI researcher influence. Several other events have also been framed in this vein, including the boycott by AI researchers of South Korean university KAIST due to a recent opening of an AI weapons lab - Forrest, C. (2018). South Korea university faces major backlash after opening AI weapons lab. *TechRepublic*. Retrieved from https://www.techrepublic.com/article/south-korea-university-faces-major-backlash-after-opening-ai-weapons-lab/; Google's failed attempt to establish an AI ethics board due to employee push back - Jee, C. (2019). Google has now cancelled its AI ethics board after a backlash from staff. *MIT Technology Review*. Retrieved from https://www.technologyreview.com/f/613271/google-has-now-cancelled-its-ai-

the actions of firms and researchers, and private actors being more heterogeneous than the cosmopolitan Silicon Valley story would have one assume. Sections 7.4.3.1 to 7.4.3.3 highlight three predictions which are particularly surprising given the current narratives around AI. Section 7.4.4 offers some caveats to these predictions.

7.4.3.1 The state will use tools such as export controls to constrain the actions of AI firms and researchers

The rise of China as a technological and economic leader has and continues to fuel the narrative of an escalating strategic competition between the U.S. and China. AI has become one of the focal points in this narrative. Thus, we should expect the state to increasingly frame AI as a matter of national priority and security and be increasingly willing to exercise their legislative capacity as a resource to pursue these goals with some success.

A specific goal that the state is likely to pursue in this vein is to halt the proliferation of AI technologies, knowledge, and talent to American adversaries. Given the prominence of the use of export controls across the historical case studies, we should particularly expect the state to turn to export controls as a tool for this task. Indeed, the advanced notice for proposed rulemaking on export controls for AI technologies (section 7.4.2.4) is a first step in this direction.

In their attempts to apply export controls to AI technologies, the state will face familiar challenges[205]. For one, given how ineffective export controls were at halting the proliferation of cryptography products and research, we should expect export controls to be of limited effectiveness particularly when applied to software-based AI technologies. Further, the track

ethics-board-after-a-backlash-from-staff/ - and growing researcher backlash within Amazon, Microsoft, and Apple on the use of facial recognition technologies - Samuel, S. (2019). The growing backlash against facial recognition tech. *Vox*. Retrieved from https://www.vox.com/future-perfect/2019/4/27/18518598/ai-facial-recognition-ban-apple-amazon-microsoft. Some frame these events within the broader umbrella of a 'tech backlash' against big technology companies – for example, Sacasas, L. C. (2018). The Tech Backlash We Really Need. The New Atlantis, 55(Spring 2018). Retrieved from https://www.thenewatlantis.com/publications/the-tech-backlash-we-really-need

[205] A sincere thank you to Allan Dafoe and Sophie-Charlotte Fischer with whom I developed a lot of this thinking on the application of export controls to AI in the process of co-authoring our article on this topic.

record of export control restrictions being costly for firms and unpopular with the global scientific community at large means that we should expect AI export controls to face substantial backlash from AI firms as well as the transnational AI research community. Thus, in order for AI export controls to be effective, the state faces the tasks of weighing the national security benefits of such a tool with its economic and political costs, and balancing the varied interests of AI firms operating in international markets and AI researchers embedded in an international scientific community[206].

7.4.3.2 AI firms will bifurcate into those who are willing versus unwilling to cooperate with the state

As the state pursues strategies to gain access to commercial AI technologies, AI firms face the thorny decision of whether they will choose to cooperate with the state or not – specifically, whether they will sell their products and services to the state in service of the nation's defense and security interests. The tensions between Silicon Valley and Washington DC, as described in Chapter 1, are often cited as reason to believe that AI firms will continue to refuse to work with the state on publicly pronounced ethical grounds.

However, history would suggest otherwise. Instead of a coherent industry stance against cooperating with the U.S. government for defense purposes, we should instead expect a subset of AI firms to willingly sell technologies to the state. Indeed, there are already several examples of this happening[207]. For example, in October 2018 BAE Systems Inc. was awarded a DOD contract to 'leverage innovations in artificial intelligence, machine learning…to enhance the security and effectiveness of our war-fighters across physical and digital domains'[208]. Booz Allen Hamilton was awarded a $886 million contract to provide machine

[206] Leung, J., Fischer, S.-C., & Dafoe, A. (2019). Export Controls in the Age of AI. *War on the Rocks*. Retrieved from https://warontherocks.com/2019/08/export-controls-in-the-age-of-ai/

[207] A sincere thank you to Nathan Calvin for finding the sources for many of these cases.

[208] Ratzer, C. (2018). The U.S. Department of Defense selects BAE Systems to help develop and deliver next generation mission technologies. Retrieved from BAE Systems Newsroom website: https://www.baesystems.com/en-us/article/the-u-s--department-of-defense-selects-bae-systems-to-help-develop-and-deliver-next-generation-mission-technologies

learning support to the U.S. Government Program Office in order to 'unlock the value of AI and analytics[209]. Cisco Systems are working with the DOD to 'expedite the integration of increased computer automation'[210], and Raytheon are providing AI expertise to the U.S. military to 'develop advanced data automation, analytics and artificial intelligence capabilities'[211].

Several of the firms listed fall into the category of traditional defense contractors. Thus, we should expect firms that are less visible and/or less sensitive to public opinion to facilitate the state's access to commercial AI technologies, even if a handful of very visible and vocal firms refuse to do so on ethical or principled grounds. As a case in point of this, Anduril, a government contractor specialising in artificial intelligence and 'lattice vision', began to work on Project Maven, plausibly to replace the role that Google was slated to play[212].

7.4.3.3 AI researchers will become less influential over time

Of late, AI researchers seem to hold substantial influence in swaying the behaviour of their employers – largely AI firms – in the vein of compelling said firms to refrain from selling their technologies to the state (section 7.4.2.5) and to invest in self-governance mechanisms (section 7.4.2.6). However, as per the model and as corroborated by the historical case studies, the influence of researchers tends to become diluted over time as the technology matures. Specifically, as the innovation capacity of firms increases, and as firms step up the

[209] Booz Allen Hamilton. (2018). U.S. Government & GSA FEDSIM Select Booz Allen to Help Apply Artificial Intelligence. Retrieved from Booz Allen Hamilton website: https://www.boozallen.com/e/media/press-release/booz-allen-selected-to-help-apply-artificial-intelligence.html
[210] Osborn, K. (2017). Cisco, DOD move JRSS to cloud tech and greater automation. *Defense Systems*. Retrieved from https://defensesystems.com/articles/2017/06/01/cisco.aspx
[211] PR Newswire. (2018). Raytheon wins two National Geospatial Agency contracts valued at up to $600M. *Seeking Alpha*. Retrieved from https://seekingalpha.com/pr/17325208-raytheon-wins-two-national-geospatial-agency-contracts-valued-600m
[212] Fang, L. (2019). Defense Tech Startup Founded by Trump's Most Prominent Silicon Valley Supporters Wins Secretive Military AI Contract. *The Intercept*. Retrieved from https://theintercept.com/2019/03/09/anduril-industries-project-maven-palmer-luckey/

levels of private investment in R&D, the resources that firms can leverage over researchers tends to constrain the independence of the research community.

As such, we predict that the influence of AI researchers will decrease with time. Additionally, we should expect the movement of AI researchers and the exchange of AI research to become increasingly constrained by legislation passed in the name of national security, whether that be in the form of 'hard' mechanism such as visa restrictions and deemed export controls, or 'softer' mechanisms such as pre-publication review schemes.

In this view, while both Project Maven and Dragonfly are examples of successful researcher-led push back against a firm's actions, they may prove to be anomalies moving forward. Indeed, across 2018 there were a handful of events whose outcomes would suggest that the synergistic business relationship between firms and the state tends to outweigh protests from a firm's researchers. For example, in 2017 Amazon announced that its facial recognition technology, Rekognition, had been provided to the U.S. military and law enforcement agencies. In response, the American Civil Liberties Union (ACLU)[213] and Amazon employees[214] wrote letters to Amazon's CEO, Jeff Bezos, requesting that Amazon cease providing Rekognition to the government specifically in relation to its use in Immigration and Customs Enforcement (ICE). Nevertheless, in November 2018 Amazon leadership announced that it would continue to sell Rekognition to government customers[215].

Microsoft was similarly embroiled in the controversy surrounding ICE. Microsoft has a track record of being a frequent government and military contractor, providing its cloud

---

[213] ACLU. (2018). *Amazon Rekognition Coalition Letter to Jeffrey P. Bezos*. Retrieved from https://www.aclunc.org/docs/20180522_AR_Coalition_Letter.pdf

[214] Amazonians. (2018). *Letter to Jeff Bezos*. Retrieved from https://www.scribd.com/document/382334740/Dear-Jeff?campaign=SkimbitLtd&ad_group=44681X1458326X9354476c7cb92ebbd7a6950bd5ad7b80&keyword=660149026&source=hp_affiliate&medium=affiliate

[215] Statt, N. (2018). Amazon told employees it would continue to sell facial recognition software to law enforcement. *The Verge*. Retrieved from https://www.theverge.com/2018/11/8/18077292/amazon-rekognition-jeff-bezos-andrew-jassy-facial-recognition-ice-rights-violations

computing platform Microsoft Azure to the U.S. Air Force and the Department of Homeland Security. In the wake of controversial changes to Homeland Security policy that would result in family separations at the U.S. border, Microsoft employees wrote an open letter to the CEO requesting that Microsoft cease their work with ICE[216]. Further, when Google announced that it would be pulling out of Project Maven and bidding for the JEDI cloud computing contract, Microsoft employees demanded that Microsoft similarly withdraw from the JEDI process[217]. Neither of these efforts succeeded: in June 2018, Microsoft released a statement condemning the family separation policy but did not follow with any changes in their contractual arrangements with the government[218].

7.4.4 The limits of looking ahead

By using the proposed model to motivate these predictions, one is intentionally constraining the space of possible predictions to those which can be derived from common historical patterns. This, by design, does not leave room for predicting exceptional events. Nevertheless, exceptions are difficult to predict yet important to acknowledge – for oftentimes, exceptions become consequential events which shape history.

In the case of AI, then, we should acknowledge that it could be an exceptional case of a strategic GPT, and therefore could buck predicted trends and outcomes. For example, it could be that we are in an exceptional period of private sector dominance, and that AI firms are or could become unprecedentedly powerful given the vast wealth that a single company could accrue with sufficiently advanced AI.

---

[216] The Seattle Times. (2018). Microsoft employees protest company's work with ICE. *The Seattle Times*. Retrieved from https://www.seattletimes.com/business/microsoft-employees-protest-companys-work-with-ice/

[217] Microsoft employees. (2018). An Open Letter to Microsoft: Don't Bid on the US Military's Project JEDI. Retrieved from Medium website: https://medium.com/s/story/an-open-letter-to-microsoft-dont-bid-on-the-us-military-s-project-jedi-7279338b7132

[218] Novet, J., & Pramuk, J. (2018). Microsoft condemns "forcible separation" of children from families after criticism over work with ICE. *CNBC*. Retrieved from https://www.cnbc.com/2018/06/18/microsoft-condemns-forcible-separation-of-families-after-ice-flap.html

Conversely, the plausibly exceptional tensions between the U.S. and China could in turn mean that AI firms become embroiled in the global politics of great power competition and face far more constraints on their activities. The state could, in turn, marshal domestic industry actors in a far more coordinated and successful manner than predicted.

We may also be witnessing an exceptionally transnational and mission-oriented AI research community. Instead of the predicted decline of researcher influence, we could perhaps see researchers growing into a coordinated, politically influential actor positioned to express concerns about the social consequences of AI, and thus shape the actions of larger actors in beneficial directions.

Yet, exceptions are difficult to predict – so as we look ahead, the challenge of predicting what is to come in AI should be assumed to be a difficult task. Nevertheless, at the very least, artificial intelligence is poised to shape history as history has been shaped before by the pursuit and politics of strategic general purpose technologies. The development and deployment of AI, then, is – at the very least – a predictably consequential event which warrants our focused attention and intervention.

8 Conclusion

Strategic general purpose technologies have transformed our economy, our security, and our politics. They have expanded our civilization to the reaches of outer space; empowered communication and economic transactions at a transnational scale; enabled us to understand and manipulate the fundamental building blocks of biological life; and inspired us to create increasingly powerful semblances of human intelligence. However, they have also threatened our security – individually, nationally, and internationally. Inevitably, strategic general purpose technologies have shaped the dynamics and consequences of politics as powerful actors seek to reap their benefits while mitigating their risks.

States, firms, and researchers are the main political actors invested in strategic general purpose technologies. The development and deployment of these technologies causes the goals of these actors to collide, pitting their capabilities against one another. These capabilities are underpinned by resources such as R&D funding and innovation capacity; conversely, they are moderated by constraints such as the legislative environment and public opinion. The provision of R&D funding and the possession of innovation capacity allows an actor to maintain leadership at the frontier of technological progress. Conversely, a lack of these resources translates into a lack of influence over the technology trajectory, and a dependence on the resourced actors. The legislative environment serves as the rule book for how these technologies interact with society and proliferates to one's friends or enemies. Therefore, the ability to shape this environment is a critical resource; being subject to its rules is a critical constraint. The level and nature of public concern regarding the technology further shapes the actors' environment by acting as a proxy for voter concern and as an expression of customer preferences.

The behavior of states, firms, and researchers are therefore shaping and being shaped by the politics of strategic general purpose technologies. Specifically, these actors find themselves simultaneously dependent upon and in conflict with one another. This manifests as synergies and conflicts between pairs of actors, which evolve across the technology life cycle.

The life cycle tends to begin with researchers – specifically, with them breaking new ground with a series of fundamental insights which lay the foundations for the technology to emerge. Often, the state is alongside as enabling partners, demonstrating an investment appetite for early-stage risk which escapes firms. However, as theoretical breakthroughs spur applied research, and as fundamental insights generate business opportunities, firms are quick to enter the fray, wielding innovation capacity particularly suited to commercialization and proliferation. The entrance of private firms causes the technology industry to scale rapidly. The state retreats into the position of being a customer of these technologies, no longer the primary funders nor controllers of the technology.

The actors thus settle into an uneasy equilibrium. Firms are in control over much of the R&D pipeline – as funders of research, employers of researchers, and owners of the infrastructure to bring products and applications to international markets. The state supports the growth of the technology industry, often with limited routes to influence its development and deployment. However, the equilibrium proves fragile to shifts in the external environment. Such shifts can take the form of escalating strategic competition between states, for example, or an increasingly engaged public concerned about the potential harms caused by these technologies. These shifts create the impetus for the state to seek to regain influence over the technology; they thus begin to draw on their legislative authority to do so. They specifically pursue routes to control the movements of technology products and knowledge across national borders, and to increase their access to commercial technologies. In turn, firms find themselves in a precarious position of balancing competing interests and

stakeholders. On the one hand, they are being pulled to sell their technologies to the state in service of national defense and security goals. On the other hand, the public and the research community become critical of the choices that firms make with respect to serving such goals. Fading into the backdrop are researchers – constrained by their dependence on R&D funding and by their legislative environment, their influence as an actor wanes.

*This model of the politics of strategic general purpose technologies fares well when held up to history***.** In tracing the technology life cycles of aerospace technology, biotechnology, and cryptography as developed in the U.S., one finds that the politics surrounding their development and deployment are broadly captured by the proposed model. With that said, history predictably proved to be more complex. For one, it emerged as important to distinguish between a defense-first versus civilian-first technology, for that informs the goals that the state prioritizes across the technology life cycle. Namely, for defense-first technologies, the goals of military leadership and risk mitigation feature earlier and more prominently than for civilian-first technologies. It also appeared that the state's ability to retain control and exercise influence over the technology trajectory was heavily influenced by its importance as a technology customer. The more that the commercial industry relied on government demand for the technologies, the more that the state proved capable of wielding its resources and ignoring its constraints. Thirdly, firms were less homogenous an actor than modelled. Some were less sensitive to the constraints of public concern and researcher push back than others, and thus became those more likely to sell their technologies to the state.

Artificial intelligence is a contemporary case of a strategic general purpose technology. The model does well to capture the political dynamics of AI to date. More importantly, by drawing on the wealth of historical insights captured in the model, we posit predictions about what is to come. In particular, we predict that what is to come may be different to the narrative of AI exceptionalism that dominates current discourse around AI.

For example, I predict that AI firms are not beyond the tools of the state, contra to some who frame AI firms as 'too big to regulate'. Instead, as external pressures escalate – in the form of China's rise in AI and increasing public concern over AI risks – I posit that firms will find themselves increasingly constrained by the legislative environment, and more pressured to serve national defense and security interests. Some will be caught in the cross-hairs of public critique and researcher push back, and thus refuse to work with the state on ethical grounds. Others, however, will willingly sell AI technologies to the state – these are likely to be the less publicly visible firms with a track record of defense contracting with the U.S. government. Further, I predict that the political influence of researchers will likely shrink; this would go against what some may view as a rise in researcher influence given recent events of employee backlash in AI firms. In turn, the inclination and capacity for the state to exert control over AI's development and proliferation will likely grow, exercised via tools such as export controls.

The politics of strategic general purpose technologies is not comprehensively captured in this model. There remain a host of open questions which, if answered, would certainly add granularity to the model and plausibly challenge the conclusions from this work. For example, one should query what elements are missing from this model which could be informative for understanding the politics of strategic general purpose technology pursuit. Would the modelling of other actors – for example, civil society – or other focal points of conflict – for example, on technology patenting – provide enough analytical value to warrant inclusion? Further, if the model took the natural extension of linking domestic political interactions to the international arena, what would we then describe and understand about political dynamics at that level, particularly vis a vis inter-state interaction in domains such as international arms control and trade? What could we then say about the shape of the global governance regime that emerges downstream of domestic and international politics between

powerful actors? Would conflicts between actors resolve in a predictable manner? Would certain governance solutions be off the table or be consistently undermined by ongoing politics between these powerful actors?

The model could also gesture towards critical junctures in the technology life cycle; these could be leveraged by actors today trying to steer the trajectory of AI. One could use the descriptive nature of this model to support further normative analysis. Indeed, the model currently portrays this pattern of politics as deterministic. This may not need to be the case. Are there interventions that actors can take – at specific moments within this pattern of politics, and in specific forms – that could result in the avoidance of costly conflicts? How would this inform the actions of those intent on or inevitably steering the trajectory of artificial intelligence? Addressing such questions are important, particularly for those inclined to believe that the governance of critical technologies is a complex challenge for which we have an abysmal track record.

This is a challenge that demands our attention. The emergence, proliferation, and contestation over strategic general purpose technologies are political events that matter. These are moments that shape the contours of power and prestige as distributed across important actors; these are technologies that shape central pillars of our civilization, from warfare to economic production and social progress. Artificial intelligence is going to matter greatly, and indeed, already does. It matters, then, that we understand the politics that surrounds it, that we examine the prospective conflicts ahead, and that we ultimately lay the groundwork for the governance of a technology that is poised to be transformative.

Appendix A: Acronyms

Chapter 3: Aerospace technology

ARPA	Advanced Research Projects Agency
ASAT	Anti-satellite weapon
CCL	Commerce Control List
COMSAT	Communications Satellite Corporation
COPUOS	Committee on the Peaceful Uses of Outer Space
EAR	Export Administration Regulations
ELV	Expendable launch vehicle
ESA	European Space Agency
GIS	Geographic information system
GNSS	Global Satellite Navigation Systems
GPS	Global Positioning System
IADCC	Inter-Agency Space Debris Coordination Committee
ICBM	Intercontinental ballistic missile
IGY	International Geophysical Year
INMARSAT	International Maritime Satellite Organization
INTELSAT	International Telecommunications Satellite Organization
ISS	International Space Station
ITAR	International Traffic in Arms Regulations
LEO	Low earth orbit
NASA	National Aeronautics and Space Administration
NDAA	National Defense Authorisation Act
NGA	National Geospatial-Intelligence Agency
NRO	National Reconnaissance Office
OSTP	Office of Science and Technology Policy
PLA	People's Liberation Army
PRC	People's Republic of China
RLV	Reusable launch vehicle
UNGA	United Nations General Assembly
USAF	U.S. Air Force
USML	United States Munitions List
USSR	Union of Soviet Socialist Republic

AAAS	American Association for the Advancement of Science
Amerithrax	FBI case name for anthrax attacks, September 2001
ASM	American Society for Microbiology
BIO	Biotechnology Innovation Organisation (known as Biotechnology Industry Organisation until 2016)
BWC	The Convention on the Prohibition of the Development, Production and Stockpiling of Bacteriological (Biological) and Toxin Weapons and on their Destruction; known as the Biological Weapons Convention
CCD	Conference on the Committee on Disarmament
CDC	Centre for Disease Control
DTRA	Defense Threat Reduction Agency
DURC	Dual Use Research of Concern
GOF	Gain of Function
iGEM	International Genetically Engineered Machine
IBC	Institutional Biosafety Committee
IRB	Institutional Review Board
NIH	National Institutes of Health
NSABB	National Science Advisory Board for Biosecurity
RAC	Recombinant DNA Advisory Committee
RBSP	Registry of Biological Standard Parts
rDNA	Recombinant DNA
USPTO	United States Patent and Trademark Office

AES	Advanced Encryption Standard
CCL	Commerce Control List
COCOM	Coordinating Committee for Multilateral Export Controls
COTS	Commercial Off the Shelf Technology
CSA	Computer Security Act
DES	Data Encryption Standard
DHS	Department of Homeland Security
DOC	Department of Commerce
DOJ	Department of Justice
EAR	Export Administration Regulations
EES	Escrowed Encryption Standard
FIPS	Federal Information Processing Standard
FISC	Foreign Intelligence Surveillance Act
GAO	Government Accountability Office
GCHQ	Government Communications Headquarters
ITAR	International Traffic in Arms Regulations
NBS	National Bureau of Standards
NIST	National Institute of Standards and Technology
NSA	National Security Agency
NSD	National Security Directive
NSDD	National Security Decision Directive
PGP	Pretty Good Privacy
SSL	Secure Sockets Layer
TLS	Transport Layer Security
USML	United States Munitions List
WA	Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies

ARPA	Advanced Research Projects Agency
CFIUS	Committee on Foreign Direct Investment in the United States
DIB	Defense Innovation Board
DIU	Defense Innovation Unit, formerly Defense Innovation Unit Experimental (DIUx)
FIRMA	Foreign Investment Risk Review Modernization Act
ICE	Immigration and Customs Enforcement
IPTO	Information Processing Techniques Office
JAIC	Joint Artificial Intelligence Center
LISP	LISt Processor, an early AI programming language
ML	Machine learning
NDAA	National Defense Authorisation Act
R&D	Research and development
SCI	Strategic Computing Initiative
UAS	Unmanned aerial system
UAV	Unmanned aerial vehicle

Appendix B: Bibliography

The following bibliography includes a comprehensive list of all of the works cited in the thesis, segmented by chapter.

Chapter 1: Introduction

Abbott, K. W., & Snidal, D. (2000). Hard and Soft Law in International Governance. *International Organization*, *54*(3), 421–456. https://doi.org/DOI: 10.1162/002081800551280

Abbott, K. W., & Snidal, D. (2010). International regulation without international government: Improving IO performance through orchestration. *The Review of International Organizations*, *5*(3), 315–344. https://doi.org/10.1007/s11558-010-9092-3

Abrahamsen, R., & Williams, M. C. (2009). Security Beyond the State: Global Security Assemblages in International Politics. *International Political Sociology*, *3*(1), 1–17. https://doi.org/10.1111/j.1749-5687.2008.00060.x

Abrahamsen, R., & Williams, M. C. (2011). *Security beyond the state: private security in international politics*. Cambridge: Cambridge University Press.

Acharya, A. (2016). The Future of Global Governance: Fragmentation May Be Inevitable and Creative. *Global Governance*, *22*(4), 453–460.

Adler, E. (1992). The emergence of cooperation: national epistemic communities and the international evolution of the idea of nuclear arms control. *International Organization*, *46*(1), 101–145. https://doi.org/DOI: 10.1017/S0020818300001466

Alberts, D. S., Garstka, J. J., & Stein, F. P. (2000). *Network Centric Warfare: Developing and Leveraging Information Superiority*. Retrieved from United States Department of Defense website: https://www.hsdl.org/?abstract&did=805186

Alic, J. A. (1994). The dual use of technology: Concepts and policies. *Technology in Society*, *16*(2), 155–172. https://doi.org/10.1016/0160-791X(94)90027-2

Alic, J. A., Branscomb, L. M., Brooks, H., Epstein, G. L., & Carter, A. B. (1992). *Beyond spinoff: Military and commercial technologies in a changing world*. Harvard Business Press.

Arnold, D. C., & McCartney, F. S. (2005). *Spying from space : constructing America's satellite command and control systems* (1st ed.). College Station: Texas A&M University Press.

Avant, D. D., Finnemore, M., & Sell, S. K. (2010). *Who governs the globe?* New York: Cambridge University Press.

Barnet, R. J. (1975). *Global reach: the power of the multinational corporations*. London: Jonathan Cape.

Barnett, M., & Duvall, R. (2005). Power in International Politics. *International Organization*, *59*(1), 39–75. https://doi.org/DOI: 10.1017/S0020818305050010

Barnett, M. N., & Duvall, R. (2005). *Power in Global Governance*. Retrieved from http://search.ebscohost.com/login.aspx?direct=true&db=nlebk&AN=129339&site=ehost-live&authtype=ip,uid

Barnett, M., Pevehouse, J., & Raustiala, K. (2017). *The Future of Global Governance*. Geneva, Switzerland: Graduate Institute of International Development Studies and Social Trends Institute.

Barth, K.-H. (2003). The Politics of Seismology: Nuclear Testing, Arms Control, and the Transformation of a Discipline. *Social Studies of Science*, *33*(5), 743–781. https://doi.org/10.1177/0306312703335005

Beck, U. (2000). *What is globalization?* Cambridge: Polity Press.

Beck, U. (2005). *Power in the global age: a new global political economy*. Cambridge: Polity.

Bell, S. (2009). *Rethinking governance: the centrality of the state in modern society*. Cambridge: Cambridge University Press.

Bieler, A., Higgott, R., & Underhill, G. (1999). *Non-State Actors and Authority in the Global System*. Retrieved from http://ebookcentral.proquest.com/lib/oxford/detail.action?docID=165773

Biermann, F., Pattberg, P., van Asselt, H., & Zelli, F. (2009). The Fragmentation of Global Governance Architectures: A Framework for Analysis. *Global Environmental Politics*, *9*(4), 14–40. https://doi.org/10.1162/glep.2009.9.4.14

Blumenthal, D., Gluck, M., Louis, K. S., Stoto, M. A., & Wise, D. (1986). University-Industry Research Relationships in Biotechnology: Implications for the University. *Science*, *232*(4756), 1361–1366. Retrieved from JSTOR.

Bottomley, S. (2007). *The constitutional corporation: rethinking corporate governance*. Aldershot: Ashgate.

Braithwaite, J. (2000). *Global business regulation*. Cambridge: Cambridge University Press.

Braithwaite, J. (2008). *Regulatory capitalism: how it works, ideas for making it work better*. Cheltenham, UK ; Northampton, MA: Edward Elgar.

Branscomb, L. M. (1992a). America's emerging technology policy. *Minerva*, *30*(3), 317–336. https://doi.org/10.1007/BF01097642

Branscomb, L. M. (1992b). U.S. scientific and technical information policy in the context of a diffusion-oriented national technology policy. *Government Publications Review*, *19*(5), 469–482. https://doi.org/10.1016/0277-9390(92)90050-L

Bresnahan, T. F., & Trajtenberg, M. (1992). General Purpose Technologies "Engines of Growth?" *National Bureau of Economic Research Working Paper Series*, *No. 4148*. https://doi.org/10.3386/w4148

Brint, S. G. (2002). *The future of the city of intellect : the changing American university*. Stanford, Calif.: Stanford University Press.

Büthe, T., & Mattli, W. (2011). *The new global rulers: the privatization of regulation in the world economy*. Princeton, NJ: Princeton University Press.

Carroll, A. B. (1991). The pyramid of corporate social responsibility: Toward the moral management of organizational stakeholders. *Business Horizons*, *34*(4), 39–48. https://doi.org/10.1016/0007-6813(91)90005-G

Carter, A. (2016, October). *Keynote Address: The Path to the Innovative Future of Defense*. Presented at the Center for Strategic and International Studies: Assessing the Third Offset Strategy: Progress and Prospects for Defense Innovation, CSIS Headquarters, Washington, D.C. Retrieved from https://csis-prod.s3.amazonaws.com/s3fs-public/event/161028_Secretary_Ashton_Carter_Keynote_Address_The_Path_to_the_Innovative_Future_of_Defense.pdf

Cassano, J. (2018, August 15). Pentagon's Artificial Intelligence Programs Get Huge Boost in the NDAA. *Sludge*. Retrieved from https://readsludge.com/2018/08/15/pentagons-artificial-intelligence-programs-get-huge-boost-in-the-ndaa/

Cavanagh, G. F. (2004). Global Business Ethics: Regulation, Code, or Self-Restraint. *Business Ethics Quarterly*, *14*(4), 625–642. https://doi.org/10.5840/beq200414436

Cerny, P. G. (1995). Globalization and the changing logic of collective action. *International Organisation*, *49*(4), 595–625. https://doi.org/10.1017/S0020818300028459

Chandler, A. D., & Mazlish, B. (2005). *Leviathans: multinational corporations and the new global history*. Cambridge: Cambridge.

Clark, I. (1999). *Globalization and international relations theory*. Oxford: Oxford University Press.

Clifford, C. (2017, September 12). Top Silicon Valley exec on why Mark Zuckerberg and Elon Musk are both right about A.I. *CNBC*. Retrieved from https://www.cnbc.com/2017/09/11/y-combinators-sam-altman-zuckerberg-and-musk-both-right-on-a-i.html

Clifford, C. (2018, February 1). Google CEO: A.I. is more important than fire or electricity. *CNBC*. Retrieved from https://www.cnbc.com/2018/02/01/google-ceo-sundar-pichai-ai-is-more-important-than-fire-electricity.html

Cooper, R. N. (1968). *The economics of interdependence: economic policy in the Atlantic community* (1st ed.). New York: Published for the Council on Foreign Relations by McGraw-Hill.

Crane, A. (2008). *Corporations and citizenship*. Retrieved from http://www.loc.gov/catdir/enhancements/fy0834/2008019385-t.html

Cross, M. K. D. (2013). Rethinking epistemic communities twenty years later. *Review of International Studies*, *39*(1), 137–160. https://doi.org/10.1017/S0260210512000034

Cutler, A. C., Haufler, V., & Porter, T. (1999a). *Private authority and international affairs*. Albany: State University of New York Press.

Cutler, A. C., Haufler, V., & Porter, T. (1999b). *Private authority and international affairs*. Albany: State University of New York Press.

Dahl, R. A. (1957). The concept of power. *Behavioral Science*, *2*(3), 201–215. https://doi.org/10.1002/bs.3830020303

Dasgupta, R. (2018, April 5). The demise of the nation state. *The Guardian*. Retrieved from https://www.theguardian.com/news/2018/apr/05/demise-of-the-nation-state-rana-dasgupta

David, P. A., & Wright, G. (1999). *General purpose technologies and surges in productivity : historical reflections on the future of the ICT revolution*. Oxford: University of Oxford.

DeNardis, L. (2009). *Protocol politics: the globalization of Internet governance*. Cambridge, Mass.: MIT Press.

Dicken, P. (1998). *Global shift: transforming the world economy* (3rd ed.). London: Paul Chapman.

DiMaggio, P. J., & Powell, W. W. (1983). The Iron Cage Revisited: Institutional Isomorphism and Collective Rationality in Organizational Fields. *American Sociological Review*, *48*(2), 147–160. https://doi.org/10.2307/2095101

Ding, J. (2018). *Deciphering China's AI Dream: The context, components, capabilities and consequences of China's strategy to lead the world in AI*. Retrieved from Future of Humanity Institute website: https://www.fhi.ox.ac.uk/wp-content/uploads/Deciphering_Chinas_AI-Dream.pdf

Djelic, M.-L., & Quack, S. (2010). *Transnational communities : shaping global economic governance*. Cambridge: Cambridge University Press.

Drezner, D. W. (2004a). The Global Governance of the Internet: Bringing the State Back In. *Political Science Quarterly*, *119*(3), 477–498. https://doi.org/10.2307/20202392

Drezner, D. W. (2004b). The Global Governance of the Internet: Bringing the State Back In. *Political Science Quarterly*, *119*(3), 477–498. https://doi.org/10.2307/20202392

Drezner, D. W. (2007). *All politics is global: explaining international regulatory regimes*. Princeton, N.J.: Princeton University Press.

Dunfee, T. W., & Fort, T. L. (2003). Corporate hypergoals, sustainable peace, and the adapted firm. *Vand. J. Transnat'l L.*, *36*, 563.

Dunlop, C. (2000). Epistemic Communities: A Reply to Toke. *Politics*, *20*(3), 137–144. https://doi.org/10.1111/1467-9256.00123

Empson, L., Cleaver, I., & Allen, J. (2013). Managing Partners and Management Professionals: Institutional Work Dyads in Professional Partnerships. *Journal of Management Studies*, *50*(5), 808–844. https://doi.org/10.1111/joms.12025

Evans, P. (1997). The Eclipse of the State? Reflections on Stateness in an Era of Globalization. *World Politics*, *50*(1), 62–87.

Falkner, R. (2003). Private Environmental Governance and International Relations: Exploring the Links. *Global Environmental Politics*, *3*(2), 72–87. https://doi.org/10.1162/152638003322068227

Fitzgerald, B., & Parziale, J. (2017). As technology goes democratic, nations lose military control. *Bulletin of the Atomic Scientists*. Retrieved from https://thebulletin.org/2017/03/as-technology-goes-democratic-nations-lose-military-control/

Forge, J. (2010). A Note on the Definition of "Dual Use." *Science and Engineering Ethics*, *16*(1), 111–118. https://doi.org/10.1007/s11948-009-9159-9

Fort, T. L., & Schipani, C. A. (2002). The role of the corporation in fostering sustainable peace. *Vand. J. Transnat'l L.*, *35*, 389.

Friedman, T. L. (1999). *The Lexus and the olive tree*. London: HarperCollins.

Fuchs, D. (2013). Theorizing the Power of Global Companies. In J. Mikler (Ed.), *The Handbook of Global Companies*. Chichester: John Wiley & Sons Inc.

Fuchs, D. A. (2007). *Business power in global governance*. Lynne Rienner Boulder, CO.

Fukuyama, F. (1992). *The end of history and the last man*. London: Hamish Hamilton.

Future of Life Institute. (n.d.). National and International AI Strategies. Retrieved December 11, 2018, from https://futureoflife.org/national-international-ai-strategies/

Gansler, J. S., Greenwalt, W. C., & Lucyshyn, W. (2013). *Non-traditional Commercial Defense Contractors*. Retrieved from Center for Public Policy and Private Enterprise website: file:///C:/Users/Jade/Downloads/UMD_12010_Non-Traditional%20Commercial%20Defense%20Contractors_November%202013.pdf

GAO. (2017). *Military Acquisitions: DOD Is Taking Steps to Address Challenges Faced by Certain Companies*. Retrieved from United States Governmance Accountability Office website: https://www.gao.gov/assets/690/686012.pdf

Garton Ash, T. (2016). *Free speech: ten principles for a connected world*. London: Atlantic Books.

Gasser, U., Gertner, N., Goldsmith, J., Landau, S., Nye, J., O'Brien, D. R., … Zittrain, J. (2016). *Don't Panic: Making Progress on the "Going Dark" Debate*. The Berkman Center for Internet & Society.

Gessner, V. (2012). Enabling global business transactions: Relational and legal mechanisms. In G. Morgan & R. Whitley (Eds.), *Capitalisms and Capitalism in the Twenty-first Century*. Oxford University Press.

Gilpin, R. (1976). *U.S. power and the multinational corporation: the political economy of foreign direct investment*. London: Macmillan.

Glaser, C. L., & Kaufmann, C. (1998). What is the Offense-Defense Balance and Can We Measure it? *International Security*, *22*(4), 44–82. https://doi.org/10.2307/2539240

Good, I. J. (1966). Speculations Concerning the First Ultraintelligent Machine. In F. L. Alt & M. Rubinoff (Eds.), *Advances in Computers* (Vol. 6, pp. 31–88). https://doi.org/10.1016/S0065-2458(08)60418-0

Graz, J.-C., & Nölke, A. (2008). *Transnational private governance and its limits*. London: Routledge.

Greene, B. P. (2015). "Captive of a Scientific-Technological Elite": Eisenhower and the Nuclear Test Ban. *Presidential Studies Quarterly*, *45*(1), 29–45. https://doi.org/10.1111/psq.12169

Haas, E. B. (1964). *Beyond the nation-state: functionalism and international organization*. Stanford, Calif: Stanford University Press.

Haas, E. B. (1980). Why Collaborate? Issue-Linkage and International Regimes. *World Politics*, *32*(3), 357–405. https://doi.org/10.2307/2010109

Haas, P. (2008). Epistemic Communities. In *The Oxford Handbook of International Environmental Law*. https://doi.org/10.1093/oxfordhb/9780199552153.013.0034

Haas, P. M. (1992a). Epistemic communities and international policy coordination. *International Organization*, *46*(1), 1–35. https://doi.org/DOI: 10.1017/S0020818300001442

Haas, P. M. (1992b). Introduction: Epistemic Communities and International Policy Coordination. *International Organization*, *46*(1), 1–35.

Hall, R. B., & Biersteker, T. J. (2002). *The emergence of private authority in global governance*. Cambridge, UK: Cambridge University Press.

Harris, E. D. (2016). *Governance of Dual-Use Technologies: Theory and Practice*. Cambridge, MA: American Academy of Arts and Sciences.

Harwell, D. (2018, September 7). Defense Department pledges billions toward artificial intelligence research. *The Washington Post*. Retrieved from https://www.washingtonpost.com/technology/2018/09/07/defense-department-pledges-billions-toward-artificial-intelligence-research/?utm_term=.1e1dfd2c7c61

Hasenclever, A., Mayer, P., & Rittberger, V. (1997). *Theories of international regimes*. Cambridge: Cambridge University Press.

Haufler, V. (2001). *A public role for the private sector: industry self-regulation in a global economy*. Washington, D.C.: Carnegie Endowment for International Peace.

Hecht, D. (2016). Scientists at War: The Ethics of Cold War Weapons Research. *Journal of American History*, *102*(4), 1255.2-1256. https://doi.org/10.1093/jahist/jav717

Held, D. (1999). *Global transformations: politics, economics and culture*. Cambridge: Polity Press.

Held, D. (2016). Elements of a theory of global governance. *Philosophy & Social Criticism*, *42*(9), 837–846. https://doi.org/10.1177/0191453716659520

Hinchliffe, E. (2016, December 14). IBM's Watson supercomputer discovers 5 new genes linked to ALS. *Mashable UK*. Retrieved from https://mashable.com/2016/12/14/ibm-watson-als-research/#c6wvytOVaGqK

Huntington, S. P. (1973). Transnational Organizations in World Politics. *World Politics*, *25*(3), 333–368. https://doi.org/10.2307/2010115

Hymans, J. E. C. (2012). *Achieving nuclear ambitions : scientists, politicians and proliferation*. Cambridge: Cambridge University Press.

Hymer, S. (1972). The Multinational Corporation and the Law of Uneven Development. In J. Bhagwati, *Economics and the World Order - From the Nineteen Seventies to the Nineteen Nineties*. New York: Macmillan.

Jordana, J., Levi-Faur, D., & University of Manchester. Centre on Regulation and Competition. (2004). *The politics of regulation: institutions and regulatory reforms for the age of governance*. Cheltenham: Edward Elgar.

Jovanovic, B., & Rousseau, P. L. (2005). General purpose technologies. In P. Aghion & S. Durlauf (Eds.), *Handbook of Economic Growth* (pp. 1182–1224). Elsevier.

Julius, D. (1990). *Global companies and public policy: the growing challenge of foreign direct investment*. London: Pinter.

Kaul, I., & United Nations Development Programme. (2003). *Providing global public goods: managing globalization*. Oxford: Oxford University Press.

Keohane, R. O., & Nye, J. S. (1977). *Power and interdependence: world politics in transition*. Boston: Little, Brown.

Keohane, R. O., & Nye, J. S. (1989). *Power and interdependence* (2nd ed.). New York: Longman.

Kindleberger, C. P. (1970). *The international corporation: a symposium*. Cambridge, Mass: MIT Press.

King, R. D., Rowland, J., Oliver, S. G., Young, M., Aubrey, W., Byrne, E., … Clare, A. (2009). The Automation of Science. *Science*, *324*(5923), 85. https://doi.org/10.1126/science.1165620

Kinley, D., & Tadaki, J. (2003). From talk to walk: The emergence of human rights responsibilities for corporations at international law. *Va. J. Int'l L.*, *44*, 931.

Koenig-Archibugi, M. (2010). Understanding the Global Dimensions of Policy. *Global Policy*, *1*(1), 16–28. https://doi.org/10.1111/j.1758-5899.2009.00009.x

Krahmann, E. (2003). National, Regional, and Global Governance: One Phenomenon or Many? *Global Governance*, *9*(3), 323.

Krasner, S. (1976). State Power and the Structure of International Trade. *World Politics*, *28*(3), 317. https://doi.org/10.2307/2009974

Krasner, S. D. (1983). *International regimes*. Ithaca: Cornell University Press.

Krebs, R. R. (2001). The Limits of Alliance: Conflict, Cooperation, and Collective Identity. In A. Lake & D. A. Ochmanek (Eds.), *The real and the ideal : essays on international relations in honor of Richard H. Ullman*. Lanham, Md.: Rowman & Littlefield Publishers.

Lake, D. A. (2010). Rightful Rules: Authority, Order, and the Foundations of Global Governance. *International Studies Quarterly*, *54*(3), 587–613. https://doi.org/10.1111/j.1468-2478.2010.00601.x

Lake, D. A., & Powell, R. (1999). *Strategic choice and international relations*. Princeton, N.J.: Princeton University Press.

Leung, J., & Fischer, S.-C. (2018, August 8). JAIC: Pentagon debuts artificial intelligence hub. *Bulletin of the Atomic Scientists*. Retrieved from https://thebulletin.org/2018/08/jaic-pentagon-debuts-artificial-intelligence-hub/

Löblová, O. (2018). When Epistemic Communities Fail: Exploring the Mechanism of Policy Influence. *Policy Studies Journal*, *46*(1), 160–189. https://doi.org/10.1111/psj.12213

Lukes, S. (2005). *Power: A Radical View* (Second edition). Retrieved from http://search.ebscohost.com/login.aspx?direct=true&db=nlebk&AN=197447&site=ehost-live&authtype=ip,uid

Lynn, W. J. (2014). The End of the Military-Industrial Complex. *Foreign Affairs*, (November / December 2014). Retrieved from https://www.foreignaffairs.com/articles/united-states/end-military-industrial-complex

Macdonald, K. M. (1995). *The sociology of the professions*. London: Sage.

Mandel, E. (1967). International Capitalism and Supra Nationality. In R. Miliband & J. Saville, *The Socialist Register*. London: Merlin Press.

Martell, L. (2007). The Third Wave in Globalization Theory. *International Studies Review*, *9*(2), 173–196. https://doi.org/10.1111/j.1468-2486.2007.00670.x

Matten, D., & Crane, A. (2005). Corporate Citizenship: Toward an Extended Theoretical Conceptualization. *Academy of Management Review*, *30*(1), 166–179. Retrieved from bth.

May, C. (2015a). *Global corporations in global governance*. Routledge.

May, C. (2015b). Who's in charge? Corporations as institutions of global governance. *Palgrave Communications*, *1*, 15042.

Mazzucato, M. (2011). *The entrepreneurial state*. London: Demos.

McCain, J. S. *National Defense Authorization Act for Fiscal Year 2019*. , Pub. L. No. H.R.5515 (2018).

Metz, C. (2018, August 26). Artificial Intelligence Is Now a Pentagon Priority. Will Silicon Valley Help? *The New York Times*. Retrieved from https://www.nytimes.com/2018/08/26/technology/pentagon-artificial-intelligence.html

Mikler, J. (2011). The Illusion of the "Power of Markets." *The Journal of Australian Political Economy*, (68), 41–61.

Mikler, J. (2018). *The political power of global corporations*. Cambridge, UK: Polity Press.

Moore, M., & Tambini, D. (2018). *Digital dominance: the power of Google, Amazon, Facebook, and Apple*. New York: Oxford University Press.

Morisse-Schilbach, M. (2015). "Changing the world": epistemic communities, and the democratizing power of science. *Innovation: The European Journal of Social Science Research*, *28*(1), 18–26. https://doi.org/10.1080/13511610.2014.943163

Mörth, U. (2004). *Soft law in governance and regulation: an interdisciplinary analysis*. Cheltenham: Edward Elgar.

Most, B. A., & Starr, H. (1984). International Relations Theory, Foreign Policy Substitutability, and "Nice" Laws. *World Politics*, *36*(3), 383–406. https://doi.org/10.2307/2010380

Noble, S. U. (2018). *Algorithms of oppression: how search engines reinforce racism*. New York: New York University Press.

O'Brien, R. (2000). *Contesting global governance: multilateral economic institutions and global social movements*. Cambridge: Cambridge University Press.

Ōmae, K. (1995). *The end of the nation state: the rise of regional economies*. London: HarperCollins.

Orsini, A., Morin, J.-F., & Young, O. (2013). Regime Complexes: A Buzz, a Boom, or a Boost for Global Governance? *Global Governance*, *19*(1), 27–39.

Ouagrham-Gormley, S. B. (2014). *Barriers to Bioweapons: The Challenges of Expertise and Organization for Weapons Development*. Cornell University Press.

Parker, C. (2002). *The open corporation: Effective self-regulation and democracy*. Cambridge University Press.

Pattberg, P. (2005). The Institutionalization of Private Governance: How Business and Nonprofit Organizations Agree on Transnational Rules. *Governance*, *18*(4), 589–610. https://doi.org/10.1111/j.1468-0491.2005.00293.x

Porter, M. E., & Kramer, M. R. (2002). The competitive advantage of corporate philanthropy. *Harvard Business Review*, *80*(12), 56–68.

Powell, W. W., & Owen-Smith, J. (1998). Universities and the Market for Intellectual Property in the Life Sciences. *Journal of Policy Analysis and Management*, *17*(2), 253–277. Retrieved from JSTOR.

Rappert, B., & Selgelid, M. J. (2013). *On the dual uses of science and ethics: principles, practices, and prospects*. Canberra: ANU E Press.

Reinicke, W. H., & Witte, J. M. (2000). Interdependence, Globalization and Sovereignty: The Role of non-binding International Legal Accords. In D. Shelton (Ed.), *Commitment and compliance: The role of non-binding norms in the international legal system*. Oxford University Press on Demand.

Rittberger, V., & Mayer, P. (1993). *Regime theory and international relations*. Oxford: Clarendon Press.

Rodrik, D. (1997). *Has globalization gone too far?* Washington, D.C.: Institute for International Economics.

Ronit, K., & Schneider, V. (1999). Global Governance through Private Organizations. *Governance*, *12*(3), 243–266. https://doi.org/10.1111/0952-1895.00102

Ronit, K., & Schneider, V. (2000). *Private organisations in global politics*. London: Routledge.

Rosecrance, R. N. (1999). *The rise of the virtual state: wealth and power in the coming century*. New York: Basic Books.

Rosenau, J. N. (1995). Governance in the Twenty-first Century. *Global Governance*, *1*(1), 13–43.

Rosenau, J. N., & Czempiel, E. O. (1992a). *Governance without government: order and change in world politics*. Cambridge: Cambridge University Press.

Rosenau, J. N., & Czempiel, E. O. (1992b). *Governance without government : order and change in world politics*. Cambridge: Cambridge University Press.

Ruggie, J. (2014). Global Governance and "New Governance Theory": Lessons from Business and Human Rights. *Global Governance*, *20*(1), 5–17.

Ruttan, V. (2006). Will Government Programs Spur the Next Breakthrough? *Issues in Science and Technology*, *22*(2), 55–61.

Ruttan, V. W. (2001). *The Role of the Public Sector in Technology Development: Generalizations from General Purpose Technologies* (Science, Technology, and Innovation Discussion Paper No. 11). Retrieved from Harvard University Center for International Development website: http://ageconsearch.umn.edu/record/13563/files/p01-11.pdf

Saxenian, A. (1994). *Regional advantage : culture and competition in Silicon Valley and Route 128*. Cambridge, Mass: Harvard University Press.

Scherer, A. G., Palazzo, G., & Baumann, D. (2006). Global Rules and Private Actors: Toward a New Role of the Transnational Corporation in Global Governance. *Business Ethics Quarterly*, *16*(4), 505–532. Retrieved from JSTOR.

Scherer, A. G., & Smid, M. (2000). The downward spiral and the US model business principles-Why MNEs should take responsibility for the improvement of world-wide social and environmental conditions. *MIR: Management International Review*, *40*, 351–371.

Schmidt, V. A. (1995). The New World Order, Incorporated: The Rise of Business and the Decline of the Nation-State. *Daedalus*, *124*(2), 75–106.

Schmitter, P. C., & Streeck, W. (1985). *Private interest government : beyond market and state*. London: Sage.

Schwarz, J. A. (2017). Platform Logic: An Interdisciplinary Approach to the Platform-Based Economy. *Policy & Internet*, *9*(4), 374–394. https://doi.org/10.1002/poi3.159

Sharma, S., & Starik, M. (2002). *Research in corporate sustainability: The evolving theory and practice of organizations in the natural environment*. Edward Elgar Publishing.

Shelton, D. (2003). *Commitment and compliance: the role of non-binding norms in the international legal system*. Oxford: Oxford University Press.

Slaughter, S., & Leslie, L. L. (1997). *Academic capitalism : politics, policies, and the entrepreneurial university*. Baltimore: Johns Hopkins University Press.

Slaughter, S., & Rhoades, G. (2004). *Academic capitalism and the new economy : markets, state, and higher education*. Baltimore: Johns Hopkins University Press.

Srnicek, N. (2017). *Platform capitalism*. Cambridge, UK ; Malden, MA: Polity Press.

Stanford Graduate School of Business. (2017). *Andrew Ng: Artificial Intelligence is the New Electricity*. Retrieved from https://www.youtube.com/watch?v=21EiKfQYZXc

Stoker, G. (1998). Governance as theory: five propositions. *International Social Science Journal*, *50*(155), 17–28. https://doi.org/10.1111/1468-2451.00106

Stopford, J. M. (1991). *Rival states, rival firms: competition for world market shares*. Cambridge: Cambridge University Press.

Strange, S. (1988). *States and markets*. London: Pinter.

Strange, S. (1991). Big Business and the State. *Millennium - Journal of International Studies*, *20*(2). Retrieved from https://ezproxy-prd.bodleian.ox.ac.uk:7218/doi/abs/10.1177/03058298910200021501#articleCitationDownloadContainer

Strange, S. (1997). The Future of Global Capitalism; or Will Divergence Persist Forever? In C. Crouch & W. Streeck (Eds.), *Political Economy of Modern Capitalism: Mapping Convergence and Diversity*. Retrieved from http://ebookcentral.proquest.com/lib/oxford/detail.action?docID=537777

Strange, S. (2000). *The retreat of the state: the diffusion of power in the world economy*. Cambridge: Cambridge University Press.

Suddaby, R., & Viale, T. (2011). Professionals and field-level change: Institutional work and the professional project. *Current Sociology*, *59*(4), 423–442. https://doi.org/10.1177/0011392111402586

Tayarani-N., M. H., Yao, X., & Xu, H. (2015). Meta-Heuristic Algorithms in Car Engine Design: A Literature Survey. *IEEE Transactions on Evolutionary Computation*, *19*(5), 609–629. https://doi.org/10.1109/TEVC.2014.2355174

Thatcher, M. (2007). *Internationalisation and economic institutions: comparing European experiences*. Retrieved from http://www.loc.gov/catdir/toc/ecip077/2006102400.html

The Long Term Strategy Group. (2017). *Testimony before the U.S.-China Economic and Security Review Commission: Chinese Advances in Unmanned Systems and the Military Applications of Artificial Intelligence - the PLA's Trajectory towards Unmanned, "Intelligentized" Warfare*. Retrieved from https://www.uscc.gov/sites/default/files/Kania_Testimony.pdf

Tiberghien, Y. (2007). *Entrepreneurial states: reforming corporate governance in France, Japan, and Korea*. Retrieved from http://www.loc.gov/catdir/toc/ecip0713/2007011004.html

Tucker, J. B. (2012). *Innovation, dual use, and security: managing the risks of emerging biological and chemical technologies*. Cambridge, Mass.: MIT Press.

Vallas, S. P., & Kleinman, D. L. (2008). Contradiction, convergence and the knowledge economy: the confluence of academic and commercial biotechnology. *Socio-Economic Review*, *6*(2), 283–311. https://doi.org/10.1093/ser/mwl035

Vernon, R. (1968). Economic Sovereignty at Bay. *Foreign Affairs*, *47*(1), 110–122. https://doi.org/10.2307/20039358

Vernon, R. (1971). *Sovereignty at bay: the multinational spread of U.S. enterprises*. London: Longman.

Vernon, R. (1981). Sovereignty at Bay ten years after. *International Organization*, *35*(3), 517–529. https://doi.org/10.1017/S0020818300032562

Vernon, R. (1991). Sovereignty at Bay: Twenty Years After. *Millennium*, *20*(2), 191–195. https://doi.org/10.1177/03058298910200021201

Vogel, D. (2008). Private Global Business Regulation. *Annual Review of Political Science*, *11*(1), 261–282. https://doi.org/10.1146/annurev.polisci.11.053106.141706

Vogel, S. K. (1996). *Freer markets, more rules: regulatory reform in advanced industrial countries*. Ithaca ; London: Cornell University Press.

Weiss, L. (1998). *The myth of the powerless state: governing the economy in a global era*. Cambridge: Polity Press.

Weiss, T. G. (2000). Governance, good governance and global governance: Conceptual and actual challenges. *Third World Quarterly*, *21*(5), 795–814. https://doi.org/10.1080/713701075

Weiss, T. G. (2009). What Happened to the Idea of World Government. *International Studies Quarterly*, *53*(2), 253–271. https://doi.org/10.1111/j.1468-2478.2009.00533.x

Weiss, T. G., & Wilkinson, R. (2014). Rethinking Global Governance? Complexity, Authority, Power, Change. *International Studies Quarterly*, *58*(1), 207–215. https://doi.org/10.1111/isqu.12082

Williams, O. F. (2000). *Global Codes of Conduct. An idea Whose Time has Come*. University of Notre Dame Press.

Work, R. (2017, April 26). *Establishment of an Algorithmic Warfare Cross-Functional Team (Project Maven)*. Retrieved from http://dodcio.defense.gov/Portals/0/Documents/Project%20Maven%20DSD%20Memo%2020170425.pdf

Young, I. M. (2004). Responsibility and Global Labor Justice. *Journal of Political Philosophy*, *12*(4), 365–388. https://doi.org/10.1111/j.1467-9760.2004.00205.x

Young, O. R. (1980). International Regimes: Problems of Concept Formation. *World Politics*, *32*(3), 331–356. https://doi.org/10.2307/2010108

Zadek, S. (2004). The Path to Corporate Responsibility. *Harvard Business Review*, *82*(12), 125–132.

Zilinskas, R. A. (2000). *Biological warfare: modern offense and defense*. Lynne Rienner Publishers.

Zwetsloot, R., & Dafoe, A. (2019, February 11). Thinking About Risks From AI: Accidents, Misuse and Structure. *Lawfare*. Retrieved from https://www.lawfareblog.com/thinking-about-risks-ai-accidents-misuse-and-structure

Chapter 2: Modelling the politics of strategic general purpose technologies

Alic, J. A. (1994). The dual use of technology: Concepts and policies. *Technology in Society*, *16*(2), 155–172. https://doi.org/10.1016/0160-791X(94)90027-2

Chandler, A. D. (1977). *The visible hand: the managerial revolution in American business*. Cambridge, Mass.: Belknap Press.

Dallas, L. L. (1988). Two models of corporate governance: Beyond Berle and Means. *U. Mich. JL Reform*, *22*, 19.

Fuchs, D. (2013). Theorizing the Power of Global Companies. In J. Mikler (Ed.), *The Handbook of Global Companies*. Chichester: John Wiley & Sons Inc.

Harrod, J. (2006). The Century of the Corporation. In C. May (Ed.), *Global corporate power*. Retrieved from http://www.loc.gov/catdir/toc/ecip061/2005029752.html

Hecker, S. (1994). Retargeting the weapons laboratories. *Issues in Science and Technology*, *10*(3), 44.

Lake, D. A., & Powell, R. (1999). *Strategic choice and international relations*. Princeton, N.J.: Princeton University Press.

Marchant, G. E., & Pope, L. L. (2009). The Problems with Forbidding Science. *Science and Engineering Ethics*, *15*(3), 375–394. https://doi.org/10.1007/s11948-009-9130-9

Mattli, W., & Woods, N. (2009). *The politics of global regulation*. Princeton University Press.

May, C. (2015). Who's in charge? Corporations as institutions of global governance. *Palgrave Communications*, *1*, 15042.

Mazzucato, M. (2011). *The entrepreneurial state*. London: Demos.

Sell, S. K. (2003). *Private power, public law: the globalization of intellectual property rights*. Retrieved from http://www.loc.gov/catdir/toc/cam031/2002035020.html

Weinburger, S. (2017). *The Imagineers of War, The Untold Story of DARPA, the Pentagon Agency that Changed the World, Alfred A*. New York: Knopf.

WTO. (2011, May 12). As trade changes rapidly, you must help guide WTO, Lamy tells global business. *WTO News: Speeches - DG Pascal Lamy*. Retrieved from https://www.wto.org/english/news_e/sppl_e/sppl192_e.htm

Chapter 3: Aerospace technology

Air Force, Assessment and Analysis Division. (2003). *Operation Iraqi Freedom – By the numbers*. Washington, D.C.: United States Air Force.

Air Force Doctrine Center. (2004). *Air Force Doctrine Document 2-2.1, Counterspace Operations*. Washington, D.C.: U.S. Air Force.

Aldrin, A. J. (1998). Technology Control Regimes and the Globalization of Space Industry. *Space Policy*, *14*(2), 115–122.

Al-Rodhan, N. (2018a, February 14). China Aims for the Moon – and Beyond. Retrieved October 8, 2018, from The Diplomat website: https://thediplomat.com/2018/02/china-aims-for-the-moon-and-beyond/

Al-Rodhan, N. (2018b, March 12). Weaponization and Outer Space Security. Retrieved from Global Policy Opinion website: https://www.globalpolicyjournal.com/blog/12/03/2018/weaponization-and-outer-space-security

Al-Rodhan, N. (2018c, March 14). Preventing Future Conflicts in Outer Space. Retrieved from Center for Security Studies ETH Zurich website: https://isnblog.ethz.ch/security/preventing-future-conflicts-in-outer-space

Al-Rodhan, N. (2018d, March 29). What will space exploration look like in the future? Retrieved from World Economic Forum Global Agenda website: https://www.weforum.org/agenda/2018/03/what-will-space-exploration-look-like-in-the-future

Anselmo, J. (1999, May 10). Congress Seeks Fix to Export Quagmire. *Aviation Week & Space Technology*.

Astrotech. (n.d.). Astrotech | About Us. Retrieved October 7, 2018, from Astrotech Corporation website: http://www.astrotechcorp.com/about-us

Baiocchi, D., & Welser, W. (2015). The Democratization of Space: New Actors Need New Rules. *Foreign Affairs*, *94*(3), 98–104.

Baker, J. C., O'Connell, K. M., & Williamson, R. (2001). *Commercial Observation Satellites: At the Leading Edge of Global Transparency*. Retrieved from RAND Corporation website: https://www.rand.org/pubs/monograph_reports/MR1229.html

Beckhusen, R. (2015, September 18). Russia Is Concerned About America's Far-Off Space Weapons. *Motherboard*. Retrieved from https://motherboard.vice.com/en_us/article/d73az7/russia-is-concerned-about-americas-far-off-space-weapons

Bonnor, N. (2012). A Brief History of Global Navigation Satellite Systems. *Journal of Navigation*, *65*(1), 1–14. https://doi.org/10.1017/S0373463311000506

Broad, W. J., & Sanger, D. E. (2007, January 18). China Tests Anti-Satellite Weapon, Unnerving U.S. *The New York Times*. Retrieved from https://www.nytimes.com/2007/01/18/world/asia/18cnd-china.html?_r=2&mtrref=undefined

Bromberg, J. L. (2000). *NASA and the Space Industry*. Baltimore MD: JHU Press.

Butrica, A. J. (2003). *Single stage to orbit: Politics, space technology, and the quest for reusable rocketry*. JHU Press.

Chang, K. (2011, April 19). NASA Awards $269 Million for Private Projects. *The New York Times*. Retrieved from https://www.nytimes.com/2011/04/19/science/space/19nasa.html?mtrref=www.google.co.uk&gwh=37A572CC68E024B128FB470E058C7E76&gwt=pay

Chang, L. (1999, May 27). US Firms Rue Negative Effects of Cox Report – Stricter Scrutiny of Ties to China May Threaten Lucrative Contracts. *Asian Wall Street Journal*.

Chen, D. D., & MacAuley, M. K. (2010). Commercial Space Actors. In E. Sadeh, *The Politics of Space: a survey*. Routledge.

Clark, S. (2010, February 2). NASA selects winners of first commercial crew contest. *SpaceFlight Now*. Retrieved from https://spaceflightnow.com/news/n1002/02ccdev/

Coletta, D. (2009). Space and Deterrence. *Astropolitics*, *7*(3), 171–192. https://doi.org/10.1080/14777620903372982

Commission to Assess United States National Security Space Management and Organization. (2001). *Report of the Commission to Assess United States National Security Space Management and Organization: Executive Summary*. Retrieved from Committee on Armed Services of the U.S. House of Representatives website: https://fas.org/spp/military/commission/executive_summary.pdf

Couvault, C. (1991). Desert Storm Reinforces Military Space Directions. *Aviation Week and Space Technology*, *42*.

Danilenko, G. M. (2016). International law-making for outer space. *Tribute to Frances Brown from Jill Stuart, Space Policy Current Editor-in-Chief*, *37*, 179–183. https://doi.org/10.1016/j.spacepol.2016.12.002

Davenport, C. (2018). *The space barons: Jeff Bezos, Elon Musk, and the quest to colonize the cosmos* (1st ed.). New York: PublicAffairs.

David, L. (2015, November 17). Report Flags China's Space Prowess; Challenges Decades of U.S. Dominance in Space. Retrieved September 25, 2018, from Leonard David's INSIDE OUTER SPACE website: http://www.LeonardDavid.com/report-flags-chinas-space-prowess-challenges-decades-of-u-s-dominance-in-space/

David, L. (2017, January 31). Private Space Station Coming Soon? Company Aiming for 2020 Launch. *Scientific American*. Retrieved from https://www.scientificamerican.com/article/private-space-station-coming-soon-company-aiming-for-2020-launch/

Dawson, L. (2017). *The Politics and Perils of Space Exploration: Who Will Compete, Who Will Dominate?* Cham: Springer International Publishing : Imprint: Springer.

Department of Defense. (2005). *National Defense Strategy of the United States of America*. Retrieved from The White House website: http://www.au.af.mil/au/awc/awcgate/nds/nds2005.pdf

deSeldin, P. B. (1999, July 5). US Export Rules Frustrate Germans. *SpaceNews*.

Dolman, E. C. (2002). *Astropolitik : classical geopolitics in the space age*. London: Frank Cass.

Evans, B. G., Thompson, P. T., Corazza, G. E., Vanelli-Coralli, A., & Candreva, E. A. (2011). 1945–2010: 65 Years of Satellite History From Early Visions to Latest Missions. *Proceedings of the IEEE*, *99*(11), 1840–1857. https://doi.org/10.1109/JPROC.2011.2159467

Ezell, E. C., & Ezell, L. N. (1978). *The Partnership: A History of the Apollo-Soyuz Test Project*. NASA Special Publication-4209.

Fought, B. E. (1988). Legal Aspects of the Commercialization of Space Transportation Systems. *High Technology Law Journal*, *3*, 99.

Foust, J. (2006, April 10). The Space Review: China, competition, and cooperation. *The Space Review*. Retrieved from http://www.thespacereview.com/article/599/1

Frutkin, A. W. (1965). *International cooperation in space*. NASA.

Garthoff, R. L. (1980). Banning the Bomb in Outer Space. *International Security*, *5*(3), 25–40. https://doi.org/10.2307/2538418

Gazeta, R. (2016, February 8). Moscow worried over possibility of deployment of attack weapons in space. *Russia Beyond*. Retrieved from https://www.rbth.com/news/2016/02/08/moscow-worried-over-possibility-of-deployment-of-attack-weapons-in-space_565825

Glover, D. R. (1997). NASA Experimental Communication Satellites, 1958-1995. In A. J. Butrica, *Beyond the Ionosphere: Fifty Years of Satellite Communication*. Washington, D.C.: NASA History Office.

Gorove, S., Finch, E. R., Sanders, B., Small, D., & Vogt, D. A. (1982). Arms Control in Outer Space. *Proceedings of the Annual Meeting (American Society of International Law)*, *76*, 284–297.

Gotlieb, A. E., & Dalfen, C. M. (1970). International Relations and Outer Space: The Politics of Co-operation. *International Journal*, *25*(4), 685–703. https://doi.org/10.2307/40200950

Gruss, M. (2016, September 22). U.S., China will meet this year to talk space debris. *SpaceNews.Com*. Retrieved from https://spacenews.com/u-s-china-will-meet-this-year-to-talk-space-debris/

Harrison, T. (2017, November 8). Is Congress Creating a Military Space Corps? Retrieved September 25, 2018, from Center for Strategic and International Studies website: https://www.csis.org/analysis/congress-creating-military-space-corps

Harrison, T., Johnson, K., & Roberts, T. G. (2017). *Escalation and deterrence in the second space age*. Retrieved from Center for Strategic and International Studies (CSIS) website: https://www.csis.org/analysis/escalation-and-deterrence-second-space-age

Harrison, T., Johnson, K., & Roberts, T. G. (2018). *Space Threat Assessment 2018*. Retrieved from Center for Strategic and International Studies (CSIS) website: https://www.csis.org/analysis/space-threat-assessment-2018

Hays, P. L. (2010). National Security Space. In E. Sadeh, *The Politics of Space: a survey*. Routledge.

Hebert, K. D. (2014). Regulation of Space Weapons: Ensuring Stability and Continued Use of Outer Space. *Astropolitics*, *12*(1), 1–26. https://doi.org/10.1080/14777622.2014.890487

Ignatius, D. (2017, March 16). War in space is becoming a real threat. *Washington Post*. Retrieved from https://www.washingtonpost.com/opinions/war-in-space-is-becoming-a-real-threat/2017/03/16/af3c35ac-0a8f-11e7-a15f-a58d4a988474_story.html

Jammula, A. K. R. (2018, June 20). The world's biggest aerospace and defence companies in 2018. Retrieved October 3, 2018, from Army Technology website: https://www.army-technology.com/features/worlds-biggest-aerospace-defence-companies-2018/

Johnson, C. (2014). *The UN Group of Governmental Experts on Space TCBMs: A Secure World Foundation Fact Sheet*. Retrieved from Secure World Foundation website: https://swfound.org/media/109311/swf_gge_on_space_tcbms_fact_sheet_april_2014.pdf

Johnson, D. J., Pace, S., & Gabbard, B. C. (1998). *Space: Emerging Options for National power*. Retrieved from RAND Corporation website: https://www.rand.org/pubs/monograph_reports/MR517.html

Johnson-Freese, J. (2000). Alice in Licenseland: us satellite export controls since 1990. *Space Policy*, *16*(3), 195–204.

Johnson-Freese, J. (2001). Becoming Chinese: Or, How U.S. Satellite Export Policy Threatens National Security. *Space Times*.

Johnson-Freese, J. (2007). *Space as a strategic asset*. Columbia University Press.

Johnson-Freese, J. *Hearing on China's Space and Counterspace Programs*. , § U.S.-China Economic and Security Review Commission (2015).

Joint Chiefs of Staff Department of Defense. (2002). *Joint Doctrine for Space Operations, Joint Publication 3-14*. Washington, D.C.: Department of Defense.

Kan, S. A. (2001). *China: Possible Missile Technology Transfers from U.S. Satellite Export Policy – Actions and Chronology*. Retrieved from Congressional Research Service website: https://fas.org/sgp/crs/nuke/98-485.pdf

Kirkendall, R. S. (1994). The Boeing Company and the Military-Metropolitan-Industrial Complex, 1945-1953. *The Pacific Northwest Quarterly*, *85*(4), 137–149.

KPMG Peat Marwick. (1997). *1997 Outlook: State of the Space Industry*. KPMG Peat Marwick, SpaceVest, Space Publications, and Center for Wireless Telecommunications.

Lamb, R. D. (2005). *Satellites, Security, and Scandal: Understanding the Politics of Export Control*. Retrieved from Center for International & Security Studies at Maryland website: http://www.cissm.umd.edu/publications/satellites-security-and-scandal-understanding-politics-export-control-0

Lawrence, S. V. (1999, April 8). Clipping Their Wings. *Far Eastern Economic Review*.

Lewis, J. (2014, August 9). They Shoot Satellites, Don't They? *Foreign Policy*. Retrieved from https://foreignpolicy.com/2014/08/09/they-shoot-satellites-dont-they/

Lewis, J. A. (2003). *Preserving America's Strength in Satellite Technology*. Retrieved from Center for Strategic and International Studies (CSIS) website: https://www.csis.org/analysis/preserving-americas-strength-satellite-technology

Lewis, P., & Livingstone, D. (2016, September 27). What to Know About Space Security. Retrieved September 25, 2018, from Chatham House Expert Comment website: https://www.chathamhouse.org//node/25077

Livingston, D. (2001). *Outer space commerce: Its history and prospects*. Golden Gate University.

Logsdon, J. M., Lear, L. J., Williamson, R. A., & Day, D. A. (1995). *Exploring the unknown: Selected documents in the history of the US Civil Space Program. Volume 1; Organizing for exploration*. Washington, D.C.: NASA.

Lord, L. *Hearings on FY 06 Defense Authorization Budget Request for Space Activities*. , § Senate Armed Services Committee, Strategic Forces Subcommittee (2005).

Lupton, D. E. (1998). *On space warfare: a space power doctrine*. Maxwell AFB: Air University Press.

Malik, T. (2017, September 28). Resurrected National Space Council Will Hold 1st Meeting Oct. 5. *Space.Com*. Retrieved from https://www.space.com/38300-national-space-council-first-meeting-date.html

Manno, J. (1984). *Arming the heavens: The hidden military agenda for space, 1945-1995*. Dodd Mead.

McDougall, W. A. (1997). *The heavens and the earth: a political history of the space age*. Baltimore: Johns Hopkins University Press.

McLucas, J. L. (1991). *Space commerce*. Cambridge MA: Harvard University Press.

Meijer, H. L. E. (2009). Reflections on Politics, Strategy and Norms in Outer Space. *Defense & Security Analysis*, *25*(1), 89–98. https://doi.org/10.1080/14751790902749942

Moltz, J. C. (2011). *The politics of space security: strategic restraint and the pursuit of national interests* (2nd ed.). Stanford, Calif.: Stanford University Press.

NASA. (2014). *Commercial Orbital Transportation Services: A New Era in Spaceflight*. Retrieved from NASA website: https://www.nasa.gov/sites/default/files/files/SP-2014-617.pdf

NASA. (n.d.-a). A Brief History of NASA. Retrieved October 1, 2018, from National Aeronautics and Space Administration website: https://history.nasa.gov/factsheet.htm

NASA. (n.d.-b). The First Dryden-Blagonravov Agreement - 1962. Retrieved October 6, 2018, from SP-4209 The Partnership: A History of the Apollo-Soyuz Test Project website: https://www.hq.nasa.gov/pao/History/SP-4209/ch2-3.htm

NASA Goddard Space Flight Center. (2001). *Dr. Robert H. Goddard, American Rocketry Pioneer*. Retrieved from https://www.nasa.gov/centers/goddard/about/history/dr_goddard.html

O'Donnell, D. J. (1996). *Commercialization by evolution in the jurisdiction of outer space*. Presented at the IAF, International Astronautical Congress, 47th, Beijing, China.

Paoletta, R. (2017, March 30). Military Officials Say We Need to Prepare for Space War. *Gizmodo*. Retrieved from https://gizmodo.com/military-officials-say-we-need-to-prepare-for-space-war-1793774231

Pasztor, A., & Cameron, D. (2018, September 27). Jeff Bezos' Space Startup to Supply Engines for Boeing-Lockheed Rocket Venture. *Wall Street Journal*. Retrieved from

https://www.wsj.com/articles/jeff-bezoss-space-startup-to-supply-engines-for-boeing-lockheed-rocket-venture-1538035079

Pawlikowski, E., Loverro, D., & Cristler, T. (2012). Space: Disruptive Challenges, New Opportunities, and New Strategies. *Strategic Studies Quarterly*. Retrieved from https://www.airuniversity.af.mil/Portals/10/SSQ/documents/Volume-06_Issue-1/Pawlikowski.pdf

Peebles, C. (1945). *High Frontier: The United States Air Force and the Military Space Program* (Vol. 1959). Washington, D.C.: Air Force History and Museums Program.

Peoples, C. (2011). The Securitization of Outer Space: Challenges for Arms Control. *Contemporary Security Policy*, *32*(1), 76–98. https://doi.org/10.1080/13523260.2011.556846

Reddy, V. S. (2017). U.S.-China Space Cooperation: Balancing Act between the U.S. Congress and President. *Astropolitics*, *15*(3), 235–250. https://doi.org/10.1080/14777622.2017.1378962

Roberts, T. G. (2017, December 15). Why We Should Be Worried about a War in Space. *The Atlantic*. Retrieved from https://www.theatlantic.com/science/archive/2017/12/why-we-should-be-worried-about-a-war-in-space/548507/

Rose, A. (2005). Bush's Space Vision. *National Review*.

RT. (2015, April 5). Russia boosts air defense in face of US Prompt Global Strike capacity. *RT International*. Retrieved from https://www.rt.com/news/246869-global-strike-missile-defense/

Sadeh, E. (2002). *Space politics and policy: an evolutionary perspective* (Vol. 2). Springer Science & Business Media.

Sadeh, E. (2010). *The Politics of Space: a survey*. Routledge.

Schauer, W. H. (1976). *The politics of space. A comparison of the Soviet and American space programs*. New York: Holmes and Meier.

Select Committee on US National Security and Military/Commercial Concerns with the Peoples' Republic of China. (1999). *US National Security and Military/Commercial Concerns with the Peoples' Republic of China*. Retrieved from The White House website: https://www.gpo.gov/fdsys/pkg/GPO-CRPT-105hrpt851/pdf/GPO-CRPT-105hrpt851.pdf

Shackelford, S. J. (2014). Governing the Final Frontier: A Polycentric Approach to Managing Space Weaponization and Debris. *American Business Law Journal*, *51*(2), 429–513. Retrieved from bth.

Sheehan, M. (2007). *The international politics of space*. Routledge London.

Siceloff, S. (2014, August 22). Commercial Crew Program - The Essentials [Text]. Retrieved September 25, 2018, from NASA website: http://www.nasa.gov/content/commercial-crew-program-the-essentials

Slotten, H. R. (2002). Satellite Communications, Globalization, and the Cold War. *Technology and Culture*, *43*(2), 315–350.

Smith, D. D. (2001). A double-edged sword: Controlling the proliferation of dual-use satellite systems. *National Security Studies Quarterly*, *7*(2), 31–68.

SpaceNews. (1999, October 19). Intelsat Might Move Out of US. *SpaceNews*.

SpaceNews. (2017, June 30). President Trump Re-Establishes National Space Council. *Space.Com*. Retrieved from https://www.space.com/37363-president-trump-national-space-council.html

Takala, R. (2017, March 29). How North Korea could kill 90 percent of Americans. *The Hill*. Retrieved from https://thehill.com/blogs/pundits-blog/defense/326094-how-north-korea-could-kill-up-to-90-percent-of-americans-at-any

Teets: America Must Reach for Space Dominance. (2004, September 15). *Defense-Aerospace*. Retrieved from http://www.defense-aerospace.com/articles-view/release/3/45448/america-must-dominate-space%3A-dod-%28sept.-16%29.html

The Information Office of the State Council. (2015). *China's Military Strategy in 2015 (translated by USC US-China Institute)*. Retrieved from The State Council Information Office of the People's Republic of China website: https://china.usc.edu/prc-state-council-chinas-military-strategy-2015-may-26-2015

The Information Office of the State Council. (2016). *China's Space Activities in 2016 (Published by Xinhua, translated by Global Times)*. Retrieved from The State Council Information Office of the People's Republic of China website: http://www.globaltimes.cn/content/1025893.shtml

The White House. (2002). *The National Security Strategy of the United States of America*. Retrieved from The White House website: https://www.state.gov/documents/organization/63562.pdf

The White House. (2006). *U.S. National Space Policy*. Retrieved from The White House website: https://obamawhitehouse.archives.gov/sites/default/files/microsites/ostp/national-space-policy-2006.pdf

The White House. (2010a). *National Security Strategy of the United States of America*. Retrieved from The White House website: https://www.hsdl.org/?abstract&did=24251

The White House. (2010b). *National Space Policy of the United States of America*. Retrieved from The White House website: https://www.nasa.gov/sites/default/files/national_space_policy_6-28-10.pdf

Thompson, M. O. (2013). *At the edge of space: the X-15 flight program*. Smithsonian Institution.

United Nations Office for Outer Space Affairs. (2014). Compendium of space debris mitigation standards adopted by States and international organizations. Retrieved September 25, 2018, from United Nations Office for Outer Space Affairs website: http://www.unoosa.org/oosa/en/ourwork/topics/space-debris/compendium.html

Vedda, J. A. (2010). Non-governmental Space Organizations. In E. Sadeh, *The Politics of Space: a survey*. Routledge.

von Braun, Wernher. (n.d.). Retrieved September 25, 2018, from National Aviation Hall of Fame website: https://www.nationalaviation.org/our-enshrinees/von-braun-wernher/

von der Dunk, F. G. (2018). Billion-dollar questions? Legal aspects of commercial space activities. *Uniform Law Review*, *23*(2), 418–446. https://doi.org/10.1093/ulr/uny022

Wall, M. (2017, March 29). Star Wars: US Must Prep for Space Battles, Commander Says. *Space.Com*. Retrieved from http://www.space.com/36246-united-states-prepare-space-war.html

Watts, B. (2013). *The Evolution of Precision Strike*. Retrieved from Center for Strategic and Budgetary Assessments website: https://csbaonline.org/research/publications/the-evolution-of-precision-strike

Weeks, E. (2007). *The politics of space law in a post Cold War era: Understanding regime change*. Northern Arizona University.

Weiner, T. (2006, May 18). Air Force Seeks Bush's Approval for Space Weapons Programs. *The New York Times*. Retrieved from https://www.nytimes.com/2005/05/18/business/air-force-seeks-bushs-approval-for-space-weapons-programs.html

Weiss, S. I., & Amir, A. R. (2018, April 13). Aerospace Industry. Retrieved September 29, 2018, from Encyclopædia Britannica website: https://www.britannica.com/technology/aerospace-industry

Whalen, D. J. (1997). Billion Dollar Technology: A Short Historical Overview of the Origins of Communications Satellite Technology, 1945—1965. In A. J. Butrica, *Beyond the Ionosphere: Fifty Years of Satellite Communication*. Washington, D.C.: NASA History Office.

Williamson, M. (1996). Space: Towards the Next Millennium. *The Aeronautical Journal 100*, *1000*, 426–443.

Wong, E. (2016, August 16). China Launches Quantum Satellite in Bid to Pioneer Secure Communications. *The New York Times*. Retrieved from https://www.nytimes.com/2016/08/17/world/asia/china-quantum-satellite-mozi.html

Yembrick, J., & Byerly, J. (2008, December 23). NASA Awards Space Station Commercial Resupply Services Contracts. Retrieved September 25, 2018, from NASA Commercial Crew & Cargo website: https://www.nasa.gov/offices/c3po/home/CRS-Announcement-Dec-08.html

York, H. F. (1970). *Race to oblivion: A participant's view of the arms race*. Simon and Schuster New York.

Chapter 4: Biotechnology

Alberts, B., Wulf Wm, A., & Fineberg, H. (2002). Current visa restrictions interfere with US science and engineering contributions to important national needs. *National Academies*. Retrieved from http://www8.nationalacademies.org/onpinews/newsitem.aspx?RecordID=s12132002

Anderson, J. (1998). *Microbes and Mass Casualties: Defending America Against Bioterrorism*. Retrieved from The Heritage Foundation website: /homeland-security/report/microbes-and-mass-casualties-defending-america-against-bioterrorism

Ari, M. D. (2012, May). *CDC's Implementation of Dual-Use Research of Concern (DURC) Oversight*. Presented at the Council of Science Editors Annual Meeting, Seattle. Retrieved from http://www.resourcenter.net/images/cse/files/2012/annmtg/handouts/03_ari_3.pdf

Atlas, R., Campbell, P., Cozzarelli, N. R., Curfman, G., Enquist, L., Fink, G., … Hammes, G. (2003). Statement on the consideration of biodefence and biosecurity. *Nature*, *421*(6925), 771.

Atlas, R. M. (1998). The medical threat of biological weapons. *Critical Reviews in Microbiology*, *24*(3), 157–168.

Atlas, R. M., & Dando, M. (2006). The Dual-Use Dilemma for the Life Sciences: Perspectives, Conundrums, and Global Solutions. *Biosecurity and Bioterrorism: Biodefense Strategy, Practice, and Science*, *4*(3), 276–286. https://doi.org/10.1089/bsp.2006.4.276

Audretsch, D. B., & Stephan, P. E. (1996). Company-Scientist Locational Links: The Case of Biotechnology. *The American Economic Review*, *86*(3), 641–652.

Ball, P. (2004). *Synthetic biology: starting from scratch*. Nature Publishing Group.

Banerjee, P., Gupta, B. M., & Garg, K. C. (2000). Patent Statistics as Indicators of Competition an Analysis of Patenting in Biotechnology. *Scientometrics*, *47*(1), 95–116. https://doi.org/10.1023/A:1005669810018

Barinaga, M. (2000). Asilomar Revisited: Lessons for Today? *Science*, *287*(5458), 1584–1585.

Barnaby, W. (1997). Biological weapons: an increasing threat. *Medicine, Conflict and Survival*, *13*(4), 301–313.

Battaglia, G. (2016, May 11). Rapid Advances in Biotechnology Bring Questions about Patentability. *Bioradiations*. Retrieved from http://www.bioradiations.com/rapid-advances-in-biotechnology-bring-questions-about-patentability/

Berger, K., Stephan, R., Mauger, P., Venugopalan, G., & Casagrande, R. (2016). Biosecurity Risk Assessment of Acts Targeting a Laboratory. In Gryphon Scientific, *Risk and benefit Analysis of Gain of Function Research: Final Report*. Retrieved from

http://www.gryphonscientific.com/wp-content/uploads/2016/04/Risk-and-Benefit-Analysis-of-Gain-of-Function-Research-Final-Report.pdf

BIO. (2002, April 22). 35 Biotech Companies To Present New Technologies & Products for Homeland Security. *Biotechnology Innovation Organization*. Retrieved from https://www.bio.org/media/press-release/35-biotech-companies-present-new-technologies-products-homeland-security

Biotechnology Innovation Organisation (BIO). (2018). Synthetic Biology Explained. Retrieved July 18, 2018, from https://www.bio.org/articles/synthetic-biology-explained

Biotechnology Innovation Organisation (BIO). (n.d.). What is Biotechnology? Retrieved July 25, 2018, from BIO website: https://www.bio.org/what-biotechnology

Biotechnology Innovation Organization. (2004). *Milestones 2004: Biotechnology Industry Organization Annual Report*. Retrieved from https://www.bio.org/insights

Block, S. M. (1999). Living nightmares: biological threats enabled by molecular biology. In S. D. Drell, A. D. Sofaer, & G. D. Wilson, *The new terror: Facing the threat of biological and chemical weapons* (pp. 39–75). Hoover Institution Press.

Blue Ribbon Study Panel on Biodefense. (2015). *A National Blueprint for Biodefense: Leadership and Major Reform Needed to Optimize Efforts - Bipartisan Report of the Blue Ribbon Study Panel on Biodefense*. Washington, D.C.: Hudson Institute.

Blumenthal, D., Campbell, E. G., Causino, N., & Louis, K. S. (1996). Participation of Life-Science Faculty in Research Relationships with Industry. *New England Journal of Medicine*, *335*(23), 1734–1739. https://doi.org/10.1056/NEJM199612053352305

Blumenthal, D., Causino, N., Campbell, E., & Louis, K. S. (1996). Relationships between Academic Institutions and Industry in the Life Sciences — An Industry Survey. *New England Journal of Medicine*, *334*(6), 368–374. https://doi.org/10.1056/NEJM199602083340606

Cameron, D. E., Bashor, C. J., & Collins, J. J. (2014). A brief history of synthetic biology. *Nature Reviews Microbiology*, *12*(5), 381. https://doi.org/10.1038/nrmicro3239

Campbell, E. G., Clarridge, B. R., Gokhale, M., Birenbaum, L., Hilgartner, S., Holtzman, N. A., & Blumenthal, D. (2002). Data withholding in academic genetics: evidence from a national survey. *Jama*, *287*(4), 473–480.

Carlson, Rob. (2008, November 21). Tracking the spread of biological technologies. *Bulletin of the Atomic Scientists*. Retrieved from https://thebulletin.org/2008/11/tracking-the-spread-of-biological-technologies/

Carlson, Rob. (2009). The New Biofactories. *McKinsey Quarterly*. Retrieved from http://www.synthesis.cc/the-new-biofactories/

Carlson, Robert. (2003). The pace and proliferation of biological technologies. *Biosecurity and Bioterrorism : Biodefense Strategy, Practice, and Science*, *1*(3), 203. https://doi.org/10.1089/153871303769201851

Carlson, Robert. (2016). Estimating the biotech sector's contribution to the US economy. *Nature Biotechnology*, *34*, 247.

Carus, W. S. (2001). *Bioterrorism and Biocrimes: The Illicit Use of Biological Agents Since 1900*. Washington, D.C.: Center for Counterproliferation Research, National Defense University.

Caulfield, T., Cook-Deegan, R. M., Kieff, F. S., & Walsh, J. P. (2006). Evidence and anecdotes: an analysis of human gene patenting controversies. *Nature Biotechnology*, *24*, 1091–1094. https://doi.org/10.1038/nbt0906-1091

Center for Biosecurity. (2011). *Preserving National Security: The Growing Role of the Life Sciences - Conference Report*. Washington, D.C.: Center for Biosecurity of UPMC.

Centers for Disease Control and Prevention. (n.d.). Federal Select Agent Program. Retrieved October 17, 2018, from https://www.selectagents.gov/

Chyba, C. F. (2006). Biotechnology and the challenge to arms control. *Arms Control Today*, 11–17.

Cohen, S. N., Chang, A. C., Boyer, H. W., & Helling, R. B. (1973). Construction of biologically functional bacterial plasmids in vitro. *Proceedings of the National Academy of Sciences*, *70*(11), 3240–3244.

Council of Graduate Schools (CGS). (2004). *Council of Graduate Schools Finds Decline in New International Graduate Student Enrolment for the Third Consecutive Year*. CGS.

DARPA. (n.d.). Our Research. Retrieved October 14, 2018, from https://www.darpa.mil/program/our-research/more

Deplazes, A. (2009). Piecing together a puzzle. An exposition of synthetic biology. *EMBO Reports*, *10*(5), 428–432. https://doi.org/10.1038/embor.2009.76

DiEuliis, D., Berger, K., & Gronvall, G. (2017). Biosecurity Implications for the Synthesis of Horsepox, an Orthopoxvirus. *Health Security*, *15*(6), 629–637. https://doi.org/10.1089/hs.2017.0081

Directorate of Intelligence. (2003). *The Darker Bioweapons Future*. Retrieved from Central Intelligence Agency (CIA) website: https://fas.org/irp/cia/product/bw1103.pdf

Ernst & Young. (2017). *Biotechnology Report 2017: Beyond borders - Staying the course*. Retrieved from Ernst & Young website: https://www.ey.com/Publication/vwLUAssets/ey-

biotechnology-report-2017-beyond-borders-staying-the-course/$FILE/ey-biotechnology-report-2017-beyond-borders-staying-the-course.pdf

Ernst & Young Economics Consulting and Quantitative Analysis. (2000, May). The Economic Contributions of the Biotechnology Industry. *Biotechnology Industry Organization*. Retrieved from https://www.bio.org/articles/economic-contributions-biotechnology-industry

European Commission. (2006). *SYNBIOLOGY: An analysis of Synthetic Biology Research in Europe and North America*.

Executive Office of the President. (2017). *Modernizing the Regulatory System for Biotechnology Products: An Update to the Coordinated Framework for the Regulation of Biotechnology*. Washington, D.C.: The White House.

Ferber, D. (2004). Microbes made to order. *Science*, *303*(5655), 158.

Festel Capital. (2010, January). *Industry Structure and Business Models for Industrial Biotechnology*. Presented at the OECD Workshop on the Outlook on Industrial Biotechnology, Vienna. Retrieved from https://www.oecd.org/health/biotech/44776744.pdf

Franco, C. (2008). Billions for Biodefense: Federal Agency Biodefense Funding, FY2008-FY2009. *Biosecurity and Bioterrorism: Biodefense Strategy, Practice, and Science*, *6*(2), 131–146. https://doi.org/10.1089/bsp.2008.0025

Fridovich-Keil, J. L. (n.d.). Human Genome Project | History, Timeline, & Facts. Retrieved November 9, 2018, from Encyclopedia Britannica website: https://www.britannica.com/event/Human-Genome-Project

Friedrichs, S. (2018). *Report on statistics and indicators of biotechnology and nanotechnology*. Retrieved from OECD website: https://www.oecd-ilibrary.org/industry-and-services/report-on-statistics-and-indicators-of-biotechnology-and-nanotechnology_3c70afa7-en

Frow, E. (2017). From "Experiments of Concern" to "Groups of Concern": Constructing and Containing Citizens in Synthetic Biology. *Science, Technology, & Human Values*, 0162243917735382. https://doi.org/10.1177/0162243917735382

Garfinkel, M. S., Endy, D., Epstein, G. L., & Friedman, R. M. (2007). *Synthetic Genomics: Options for Governance*. J. Craig Venter Institute; Center for Strategic and International Studies; MIT.

Giesecke, S. (2000). The contrasting roles of government in the development of biotechnology industry in the US and Germany. *Research Policy*, *29*(2), 205–223. https://doi.org/10.1016/S0048-7333(99)00061-X

Gold, E. R. (2000). Finding common cause in the patent debate. *Nature Biotechnology*, *18*, 1217.

Guillemin, J., Meselson, M., Robinson, J. P., & Sims, N. (2015). Witness Seminar: Origins of the Biological Weapons Convention. In *Biological Threats in the 21st Century* (Vols. 1–0, pp. 357–384). https://doi.org/10.1142/9781783269488_0021

Hansen, J. E. (1999). Viruses, bacteria and toxins as biological warfare. *Ugeskrift for Laeger*, *161*(6), 772–775.

Harris, E. D. (2016). *Governance of Dual-Use Technologies: Theory and Practice*. Cambridge, MA: American Academy of Arts and Sciences.

Henderson, D. A. (1998). Bioterrorism as a public health threat. *Emerging Infectious Diseases*, *4*(3), 488.

Henderson, D. A. (1999). The looming threat of bioterrorism. *Science*, *283*(5406), 1279–1282.

Hollis, R. B. *Statement by Richard Hollis - Bioshield: Linking bioterrorism threats and countermeasure procurement to enhance terrorism preparedness*. , § Subcommittee on Emergency Preparedness, Science and Technology of the U.S. House of Representatives Committee on Homeland Security (2005).

Hoyt, K., & Brooks, S. G. (2003). A Double-Edged Sword: Globalization and Biosecurity. *International Security*, *28*(3), 123–148.

iGEM. (2017). Registry of Standard Biological Parts. Retrieved July 18, 2018, from http://parts.igem.org/Main_Page

Inglesby, T. (2018, January 19). The problem of horsepox synthesis: new approaches needed for oversight and publication review for research posing population-level risks. Retrieved October 21, 2018, from The Bifurcated Needle website: http://www.bifurcatedneedle.com/new-blog/2018/1/19/the-problem-of-horsepox-synthesis-new-approaches-needed-for-oversight-and-publication-review-for-research-posing-population-level-risks

Inglesby, T. V., & Relman, D. A. (2016). How likely is it that biological agents will be used deliberately to cause widespread harm?: Policymakers and scientists need to take seriously the possibility that potential pandemic pathogens will be misused. *EMBO Reports*, *17*(2), 127–130. https://doi.org/10.15252/embr.201541674

Institute of Medicine, & National Research Council. (2006). *Globalization, Biosecurity, and the Future of the Life Sciences*. Washington: National Academies Press.

InterAcademy Partnership (IAP) Biosecurity Working Group. (2015). *The Biological and Toxin Weapons Convention: Implications of advances in science and technology*. Retrieved from The Royal Society website: https://royalsociety.org/~/media/policy/projects/biological-toxin-weapons-convention/bwc-trends-booklet.pdf

Itakura, K., Hirose, T., Crea, R., Riggs, A. D., Heyneker, H. L., Bolivar, F., & Boyer, H. W. (1977). Expression in Escherichia coli of a chemically synthesized gene for the hormone somatostatin. *Science*, *198*(4321), 1056–1063.

Jamison, M. (2015). Patent Harmonization in Biotechnology: Towards International Reconciliation of the Gene Patent Debate. *Chicago Journal of International Law*, *15*(2), 688–720.

Jefferson, C., Lentzos, F., & Marris, C. (2014). Synthetic biology and biosecurity: challenging the "myths." *Front Public Health*, *2*. https://doi.org/10.3389/fpubh.2014.00115

Joint Chiefs of Staff. (2013). *Defense Support of Civil Authorities*. Washington, D.C.: U.S. Department of Defense.

Kempner, J., Perlis, C. S., & Merz, J. F. (2005). Forbidden knowledge. *Science*, *307*(5711), 854–854.

Kennedy, D. (2005). Editorial: Better Never than Late. *Science*, *310*(5746), 195–195.

Kenney, M. (1986). *Biotechnology : the university-industrial complex*. New Haven: Yale University Press.

Koblentz, G. (2004). Pathogens as weapons: The international security implications of biological warfare. *International Security*, *28*(3), 84–122.

Koblentz, G. D. (2017). The De Novo Synthesis of Horsepox Virus: Implications for Biosecurity and Recommendations for Preventing the Reemergence of Smallpox. *Health Security*, *15*(6), 620–628. https://doi.org/10.1089/hs.2017.0061

Krimsky, S., Ennis, J. G., & Weissman, R. (1991). Academic-Corporate Ties in Biotechnology: A Quantitative Study. *Science, Technology, & Human Values*, *16*(3), 275–287.

Leighton, R. *Leighton Read, statement on behalf of BIO - Furthering public health security: Project Bioshield.* , § Subcommittee on Health and Subcommittee on Emergency Preparedness and Response, of the Committee on Energy and Commerce, (2003).

Lentzos, F. (2006). Rationality, Risk and Response: A Research Agenda for Biosecurity. *BioSocieties*, *1*(4), 453–464. https://doi.org/10.1017/S1745855206004066

Lentzos, F. (2007). The American Biodefense Industry: From Emergency to Nonemergence. *Politics and the Life Sciences*, *26*(1), 15–23.

Lentzos, F. (2014). The Performativity of Constructed Uncertainty: Military Money and Secrecy in Biology. *Science as Culture*, *23*(4), 585–589. https://doi.org/10.1080/09505431.2014.942263

Lentzos, F. (2015a). *Dual Use in Biology and Biomedicine*. Retrieved from Nuffield Council on Bioethics website: http://nuffieldbioethics.org/wp-content/uploads/Background-paper-2016-Dual-use.pdf

Lentzos, F. (2015b, December 25). Synthetic Biology's Defence Dollars: Signals and Perception. Retrieved October 18, 2018, from PLOS Synthetic Biology Community website: https://blogs.plos.org/synbio/2015/12/24/synthetic-biologys-defence-dollars-signals-and-perceptions/

Lentzos, F. (2018, April 12). How do we control dangerous biological research? *Bulletin of the Atomic Scientists*. Retrieved from https://thebulletin.org/2018/04/how-do-we-control-dangerous-biological-research/

Lieberman, J. *Senator Joseph Lieberman's statement - Creating a BioDefense Industry: BioShield II.* , § Senate Judiciary and Senate HELP Committees (2004).

McLeish, C., & Nightingale, P. (2007). Biosecurity, bioterrorism and the governance of science: The increasing convergence of science and security policy. *Research Policy*, *36*(10), 1635–1654. http://dx.doi.org/10.1016/j.respol.2007.10.003

McMillan, G. S., Narin, F., & Deeds, D. L. (2000). An analysis of the critical role of public science in innovation: the case of biotechnology. *Research Policy*, *29*(1), 1–8. https://doi.org/10.1016/S0048-7333(99)00030-X

Medicine, I. of, & Council, N. R. (2013). *Perspectives on Research with H5N1 Avian Influenza: Scientific Inquiry, Communication, Controversy: Summary of a Workshop* (K. Matchett, A.-M. Mazza, & S. Kendall, Eds.). Retrieved from https://www.nap.edu/catalog/18255/perspectives-on-research-with-h5n1-avian-influenza-scientific-inquiry-communication

Mervis, J. (2017, March 9). Data check: U.S. government share of basic research funding falls below 50%. *Science*. Retrieved from http://www.sciencemag.org/news/2017/03/data-check-us-government-share-basic-research-funding-falls-below-50

Millett, P., & Snyder-Beattie, A. (2017). Existential Risk and Cost-Effective Biosecurity. *Health Security*, *15*(4), 373–383. https://doi.org/10.1089/hs.2017.0028

Narin, F., Hamilton, K. S., & Olivastro, D. (1997). The increasing linkage between U.S. technology and public science. *Research Policy*, *26*(3), 317–330. https://doi.org/10.1016/S0048-7333(97)00013-9

National Academies of Sciences, Engineering, & Medicine. (2017). *Preparing for Future Products of Biotechnology*. https://doi.org/10.17226/24605

National Academy of Sciences. (2004). *A Patent System for the 21st Century*. Washington, D.C.: National Academies Press.

National Academy of Sciences. (2005). *Reaping the Benefits of Genomic and Proteomic Research: Intellectual Property Rights, Innovation, and Public Health*. Washington, D.C.: National Academies Press.

National Research Council. (2004). *Biotechnology Research in an Age of Terrorism*. https://doi.org/10.17226/10827

National Research Council. (2007). *Science and Security in a Post 9/11 World: A Report Based on Regional Discussions Between the Science and Security Communities*. Retrieved from https://www.nap.edu/catalog/12013/science-and-security-in-a-post-911-world-a-report

National Research Council. (2009a). *A Survey of Attitudes and Actions on Dual Use Research in the Life Sciences: A Collaborative Effort of the National Research Council and the American Association for the Advancement of Science*. https://doi.org/10.17226/12460

National Research Council. (2009b). *Beyond "Fortress America": National Security Controls on Science and Technology in a Globalized World*. https://doi.org/10.17226/12567

National Science Advisory Board for Biosecurity. (2007). *Proposed Framework for the Oversight of Dual Use Life Sciences Research: Strategies for Minimizing the Potential Misuse of Research Information*. National Science Advisory Board for Biosecurity (NSABB).

National Science Advisory Board for Biosecurity. (2010). *Addressing Biosecurity Concerns Related to Synthetic Biology*. Washington, D.C.: NSABB.

National Science Advisory Board for Biosecurity. (2016). *Recommendations for the Evaluation and Oversight of Proposed Gain-of-Function Research*. Washington, D.C.

National Science Advisory Board for Biosecurity. (2017). *Responsible Communication of Life Sciences Research with Dual-Use Potential*. Retrieved from National Institutes of Health (U.S.). Office of Biotechnology Activities website: https://www.hsdl.org/?abstract&did=704404

Office of Science and Technology Policy. (2017). *Recommended Policy Guidance for Departmental Development of Review Mechanisms for Potential Pandemic Pathogen Care and Oversight*. Washington, D.C.: The White House.

OpenWetWare. (2017). OpenWetWare. Retrieved July 18, 2018, from https://openwetware.org/wiki/Main_Page

Osterholm, M. T. (1997, November 17). The Silent Killers. *Newsweek*. Retrieved from https://www.highbeam.com/doc/1G1-19979945.html

Osterholm, M. T., & Schwartz, J. (2001). *Living Terrors: What America Needs to Know to Survive the Coming Bioterrorist Catastrophe*. New York: Delacorte Press.

Pang, S., Lee, S. Y., & Seul, J. Y. (2017). Policy Challenges and Ethical Issues with the Breakthrough Technology: The Case of Synthetic Biology. *Science, Technology and Society*, *22*(3), 455–472. https://doi.org/10.1177/0971721817723388

Powell, W. W., Koput, K. W., & Smith-Doerr, L. (1996). Interorganizational Collaboration and the Locus of Innovation: Networks of Learning in Biotechnology. *Administrative Science Quarterly*, *41*(1), 116–145. Retrieved from bth.

Prabhakar, A. *Department of Defense (DOD) Fiscal Year 2016 Science and Technology Programs: Laying the Groundwork to Maintain Technological Superiority*. , § Subcommittee on Emerging Threats and Capabilities, Armed Services Committee (2015).

President's Council of Advisors on Science and Technology. (2016). *Biodefense Report 2016*. Retrieved from Executive Office of the President website: https://obamawhitehouse.archives.gov/sites/default/files/microsites/ostp/PCAST/pcast_biodefense_letter_report_final.pdf

Rao, R. R. (2012). *Patenting in Biotechnology - An Overview*. Retrieved from SSRN website: http://dx.doi.org/10.2139/ssrn.1999541

Rhodes, C. (2010). The History of the Biotechnology Revolution. In *Science Ethics and Society*. *International Governance of Biotechnology : Needs, Problems and Potential* (1st ed., pp. 8–21). Retrieved from http://www.bloomsburycollections.com/book/international-governance-of-biotechnology-needs-problems-and-potential/ch2-the-history-of-the-biotechnology-revolution/

Ruttan, V. W. (2001). *The Role of the Public Sector in Technology Development: Generalizations from General Purpose Technologies* (Science, Technology, and Innovation Discussion Paper No. 11). Retrieved from Harvard University Center for International Development website: http://ageconsearch.umn.edu/record/13563/files/p01-11.pdf

SBOL. (2018). The Synthetic Biology Open Language (SBOL). Retrieved July 18, 2018, from http://sbolstandard.org/

Schoch-Spana, M., Cicero, A., Adalja, A., Gronvall, G., Kirk Sell, T., Meyer, D., … Inglesby, T. (2017). Global Catastrophic Biological Risks: Toward a Working Definition. *Health Security*, *15*(4), 323–328. https://doi.org/10.1089/hs.2017.0038

Selgedid, M. J. (2007). A tale of two studies: ethics, bioterrorism, and the censorship of science. *Hastings Center Report*, *37*(3), 35–43.

Sell, T. K., & Watson, M. (2013). Federal Agency Biodefense Funding, FY2013-FY2014. *Biosecur Bioterror*, *11*(3), 196–216.

Si, T., & Zhao, H. (2016). A brief overview of synthetic biology research programs and roadmap studies in the United States. *Synthetic Biology in China, UK and US*, *1*(4), 258–264. https://doi.org/10.1016/j.synbio.2016.08.003

Slater, M. S., & Trunkey, D. D. (1997). Terrorism in America: an evolving threat. *Archives of Surgery*, *132*(10), 1059–1066.

Spelling, A., McLeish, C., & Balmer, B. (2015). *Where did the Biological Weapons Convention come from? Indicative timeline and key events, 1925 - 75*. Retrieved from University of Sussex Science Policy Research Unit (SPRU) website: https://www.ucl.ac.uk/sts/sites/sts/files/wheredidbwccomefrom.pdf

Stone, K. (2018, April 27). The Gene Patents Debate. *The Balance*. Retrieved from https://www.thebalance.com/the-gene-patents-debate-2663137

The Synthetic Biology Project. (2015). *U.S. Trends in Synthetic Biology Research Funding*. Retrieved from Woodrow Wilson International Center for Scholars website: https://www.wilsoncenter.org/publication/us-trends-synthetic-biology-research-funding

The United States Government. (2012). *United States Government Policy for Oversight of Life Sciences Dual Use Research of Concern*. Retrieved from https://www.phe.gov/s3/dualuse/Documents/us-policy-durc-032812.pdf

The United States Government. (2014). *United States Government Policy for Institutional Oversight of Life Sciences Dual use Research of Concern*. Retrieved from https://www.phe.gov/s3/dualuse/Documents/durc-policy.pdf

The White House. (2014). *U.S. Government Gain-of-Function Deliberative Process and Research Funding Pause on Selected Gain-of-Function Research Involving Influenza, MERS, and SARS Viruses*. Washington, D.C.

Tucker, J. B., & Zilinskas, R. A. (2006). The Promises and Perils of Synthetic Biology. *The New Atlantis*. Retrieved from https://www.thenewatlantis.com/publications/the-promise-and-perils-of-synthetic-biology

Watson, C., Watson, M., & Kirk Sell, T. (2017). Federal Funding for Health Security in FY2018. *Health Security*, *15*(4), 351–372. https://doi.org/10.1089/hs.2017.0047

Watson, J. D., & Crick, F. H. (1953). Molecular structure of nucleic acids. *Nature*, *171*(4356), 737–738.

Wein, L. M., & Liu, Y. (2005). Analyzing a bioterror attack on the food supply: The case of botulinum toxin in milk. *Proceedings of the National Academy of Sciences of the United States of America*, *102*(28), 9984. https://doi.org/10.1073/pnas.0408526102

Weiner, C. (1999). Is self-regulation enough today?: Evaluating the recombinant DNA controversy. *Health Matrix (Cleveland, Ohio : 1991)*, *9*(2), 289.

Weiner, C. (2001). Drawing the line in genetic engineering: self-regulation and public participation. *Perspectives in Biology and Medicine*, *44*(2), 208–220.

Wright, D. P. *Statement by David Wright - Bioshield: Linking bioterrorism threats and countermeasure procurement to enhance terrorism preparedness.* , § Subcommittee on Emergency Preparedness, Science and Technology of the U.S. House of Representatives Committee on Homeland Security (2005).

Wright, S., & Wallace, D. A. (2000). Varieties of Secrets and Secret Varieties: The Case of Biotechnology. *Politics and the Life Sciences*, *19*(1), 45–57.

Wysocki, B. (2005, July 11). US struggles for drugs to counter biological threat. *The Wall Street Journal*.

Young, A., & Penzenstadler, N. (2015, May 28). Inside America's secretive biolabs. *USA TODAY*. Retrieved from https://www.usatoday.com/story/news/2015/05/28/biolabs-pathogens-location-incidents/26587505/

Chapter 5: Cryptography

Abelson, Hal, Anderson, R. J., Bellovin, S. M., Benaloh, J., Blaze, M., Diffie, W., … Schiller, J. I. (1997). The risks of key recovery, key escrow, and trusted third-party encryption. *World Wide Web Journal*, *2*(3), 241–257.

Abelson, Harold, Anderson, R., Bellovin, S. M., Benaloh, J., Blaze, M., Diffie, W., … Neumann, P. G. (2015). Keys under doormats: mandating insecurity by requiring government access to all data and communications. *Journal of Cybersecurity*, *1*(1), 69–79.

Ablon, L., Libicki, M. C., & Golay, A. A. (2014). *Markets for Cybercrime Tools and Stolen Data: Hackers' Bazaar*. Retrieved from RAND Corporation website: https://www.rand.org/pubs/research_reports/RR610.html

American Council on Education. (1981). *Report of the Public Cryptography Study Group*. ACE.

Ball, J., Borger, J., & Greenwald, G. (2013, September 6). Revealed: how US and UK spy agencies defeat internet privacy and security | US news. *The Guardian*. Retrieved from https://www.theguardian.com/world/2013/sep/05/nsa-gchq-encryption-codes-security

Bamford, J. (1982). *The Puzzle Palace: Inside the National Security Agency*. Penguin.

Banisar, D. (1999). Stopping science: the case of cryptography. *Health Matrix: Journal of Law-Medicine*, *9*(2), 253–287. Retrieved from lft.

Bankston, K. (2015, February 25). West Coast vs. East Coast. *Slate Future Tense*. Retrieved from http://www.slate.com/articles/technology/future_tense/2015/02/yahoo_s_alex_stamos_and_nsa_s_mike_rogers_fight_about_encryption.html?wpsrc=sh_all_dt_tw_top

Bellovin, S. M., Blaze, M., Boneh, D., Landau, S., & Rivest, R. L. (2018, May 10). *Analysis of the CLEAR Protocol per the National Academies' Framework*. Retrieved from https://mice.cs.columbia.edu/getTechreport.php?techreportID=1637

Bennett, C. (2015, March 22). Silicon Valley spars with Obama over "backdoor" surveillance. *The Hill*. Retrieved from http://thehill.com/policy/cybersecurity/236512-silicon-valley-spars-with-obama-over-backdoor-surveillance

Biddle, P., England, P., Peinado, M., & Willman, B. (2002). The darknet and the future of content protection. *ACM Workshop on Digital Rights Management*, 155–176. Springer.

Blaze, M. (1994). Protocol failure in the escrowed encryption standard. *Proceedings of the 2nd ACM Conference on Computer and Communications Security*, 59–67. ACM.

Buchanan, B. (2016). Cryptography and Sovereignty. *Survival*, *58*(5), 95–122. https://doi.org/10.1080/00396338.2016.1231534

Christie, R. (2000, January 18). U.S. limbers up for encryption sales: Companies are cheered as rules are eased on exporting privacy software. *Financial Times (London)*.

Cocoran, E. (1996, January 12). U.S. Closes Investigation in Computer Privacy Case. *Washington Post*.

Comey, J. B. (2014, October). *Going Dark: Are Technology, Privacy, and Public Safety on a Collision Course?* Presented at the Brookings Institution, Washington, D.C. Retrieved from https://www.fbi.gov/news/speeches/going-dark-are-technology-privacy-and-public-safety-on-a-collision-course

Committee to Study National Cryptography Policy, Computer Science and Telecommunications Board, & Commission on Physical Sciences, Mathematics, and Applications. (1996). *Cryptography's Role in Securing the Information Society* (K. W. Dam & H. S. Lin, Eds.). Washington, D.C.: National Academies Press.

Cook, T. (2014, September 17). *A message from Tim Cook about Apple's commitment to your privacy*. Retrieved from https://www.apple.com/privacy/

Council, N. R. (1991). *Computers at Risk: Safe Computing in the Information Age*. Retrieved from https://www.nap.edu/catalog/1581/computers-at-risk-safe-computing-in-the-information-age

Crocker, T. E. (2000, February 14). Decoding rules of encryption: The ins and outs of new regulations governing exports. *Legal Times*.

Denning, D. E., & Smid, M. (1994). Key escrowing today. *IEEE Communications Magazine*, *32*(9), 58–68.

Dewitt, P. E. (1993, March 14). Who should keep the keys? *TIME*.

Diffie, W., & Hellman, M. (1976). New directions in cryptography. *IEEE Transactions on Information Theory*, *22*(6), 644–654.

Diffie, W., & Landau, S. (2001). *The Export of Cryptography in the 20th Century and the 21st*. Retrieved from https://privacyink.org/pdf/export_control.pdf

Diffie, W., & Landau, S. (2010). *Privacy on the line: The politics of wiretapping and encryption*. MIT press.

Drummond, D. (2010, January 12). A new approach to China. Retrieved from Google Policy BLog website: https://googleblog.blogspot.com/2010/01/new-approach-to-china.html

Electronic Frontiers Foundation. (1998). *Cracking DES: Secrets of Encryption Research, Wiretap Politics & Chip Design*. O'Reilly Media.

Freeh, L. *Hearing of the Terrorism, Technology and Government Information Subcommittee; Subject: Encryption Technology.* , § Senate Judiciary Committee (1997).

Fung, B. (2013, October 30). Even after NSA revelations, Yahoo won't say if it plans to encrypt data center traffic. *Washington Post*. Retrieved from

https://www.washingtonpost.com/news/the-switch/wp/2013/10/30/even-after-nsa-revelations-yahoo-wont-say-if-it-plans-to-encrypt-data-center-traffic/

Gasser, U., Gertner, N., Goldsmith, J., Landau, S., Nye, J., O'Brien, D. R., … Zittrain, J. (2016). *Don't Panic: Making Progress on the "Going Dark" Debate*. The Berkman Center for Internet & Society.

Gellman, B., & Soltani, A. (2013, October 20). NSA Infiltrates Links to Yahoo, Google Data Centers Worldwide, Snowden Documents Say. *Washington Post*. Retrieved from https://www.washingtonpost.com/world/national-security/nsa-infiltrates-links-to-yahoo-google-data-centers-worldwide-snowden-documents-say/2013/10/30/e51d661e-4166-11e3-8b74-d89d714ca4dd_story.html

George, R. (2002, July). *Keynote Address by Richard George, Technical Director, Security Evaluations Group, National Security Agency*. Presented at the Black Hats Briefing.

Gilbert, L. A. (1982). Patent Secrecy Orders: The Unconstitutionality of Interference in Civilian Cryptography Under Present Procedures. *Santa Clara Law Review*, *22*, 325.

Global Internet Liberty Campaign. (1998, February). Cryptography and Liberty 1998: An International Survey of Encryption Policy. Retrieved from GILC website: http://gilc.org/crypto/crypto-survey.html

Gore, A. (1996, July 12). *Administration Statement on Commercial Encryption Policy*. Retrieved from https://www.epic.org/crypto/key_escrow/wh_cke_796.html

Gore, A. (1998, September 16). *Holds news briefing on encryption*.

Greenberg, A. (2014, November 18). Whatsapp Just Switched on End-to-End Encryption for Hundreds of Millions of Users. *Wired*. Retrieved from https://www.wired.com/2014/11/whatsapp-encrypted-messaging/

Greenwald, G. (2013, June 6). NSA collecting phone records of millions of Verizon customers daily. *The Guardian*. Retrieved from https://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order

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

Helwich, D. (2001). *Cryptography, critique and power: A critical inquiry into the federal encryption regulation controversy*.

Hoffman, L., Ali, F., Heckler, S., & Huybrechts, A. (1994). Cryptography policy. *Association for Computing Machinery. Communications of the ACM*, *37*(9), 109. https://doi.org/10.1145/182987.184079

Ito, J., Narula, N., & Ali, R. (2017, March 8). The Blockchain Will Do to the Financial System What the Internet Did to Media. *Harvard Business Review*. Retrieved from https://hbr.org/2017/03/the-blockchain-will-do-to-banks-and-law-firms-what-the-internet-did-to-media

Kahn, D. (1996). *The Codebreakers: The comprehensive history of secret communication from ancient times to the internet*. Simon and Schuster.

Kelsey, J. (2013). *SHA3: Past, Present, and Future*. Presented at the Workshop Cryptographic Hardware and Embedded Systems. Retrieved from https://csrc.nist.gov/CSRC/media/Projects/Hash-Functions/documents/kelsey_ches2013_presentation.pdf

Koblitz, A. H., Koblitz, N., & Menezes, A. (2011). Elliptic curve cryptography: The serpentine course of a paradigm shift. *Journal of Number Theory*, *131*(5), 781–814.

Kolata, G. (1986). NSA to provide secret codes. *Science*, *230*, 45–47.

Koops, B.-J., & Kosta, E. (2018). Looking for some light through the lens of "cryptowar" history: Policy options for law enforcement authorities against "going dark." *Computer Law & Security Review*, *34*(4), 890–900. https://doi.org/10.1016/j.clsr.2018.06.003

Kruh, L. (1986). The Control of Public Cryptgraphy and Freedom of Speech - A Review. *Cryptologia*, *10*(1), 2–9.

Landau, S. (2013). *Making Sense from Snowden: What's Significant in the NSA Surveillance Revelations*. IEEE Computer and Reliability Societies.

Landau, S. (2014a). *Making Sense from Snowden, Part II: What's Significant in the NSA Surveillance Revelations*. IEEE Security & Privacy.

Landau, S. (2014b). Under the Radar: NSA's Efforts to Secure Private-Sector Telecommunications Infrastructure. *Journal of National Security Law & Policy*, *7*(3), 1–31.

Landau, S. *Testimony for House Judiciary Committee Hearing on "The Encryption Tightrope: Balancing Americans" Security and Privacy"."* , § House Judiciary Committee (2016).

Landau, S. (2016b). The real security issues of the iPhone case. *Science*, *352*(6292), 1398. https://doi.org/10.1126/science.aaf7708

Landau, S. (2018, March 30). Revelations on the FBI's Unlocking of the San Bernardino iPhone: Maybe the Future Isn't Going Dark After All. Retrieved from Lawfare website:

https://www.lawfareblog.com/revelations-fbis-unlocking-san-bernardino-iphone-maybe-future-isnt-going-dark-after-all

Levy, S. (2001). *Crypto: How the code rebels beat the government--saving privacy in the digital age*. Penguin.

Levy, S. (2018, April 25). Can This New Encryption Method Finally Crack the Crypto War? *Wired*. Retrieved from https://www.wired.com/story/crypto-war-clear-encryption/

Lichtblau, E., & Benner, K. (2017, December 21). Apple Fights Order to Unlock San Bernardino Gunman's iPhone. *The New York Times*. Retrieved from https://www.nytimes.com/2016/02/18/technology/apple-timothy-cook-fbi-san-bernardino.html

Lin, H. (2016). Governance of Information Technology and Cyber Weapons. In E. D. Harris (Ed.), *Governance of Dual-Use Technologies: Theory and Practice*. American Academy of Arts and Sciences.

Litt, R. S. *Prepared statement of Robert S. Litt, Principle Associate Deputy Attorney General; Subject: Privacy in a digital age: Encryption and mandatory access.* , § Senate Judiciary Committee, Subcommittee on the Constitution, Federalism, and Property Rights (1998).

Markoff, J. (1992, May 7). A Public Battle Over Secret Codes. *The New York Times*.

Markoff, J. (1993a, April 16). Electronics Plan Aims to Balance Government Access with Privacy. *The New York Times*.

Markoff, J. (1993b, April 17). Communication Plan Draws Mixed Reaction. *The New York Times*.

Markoff, J. (1994, June 2). Scientist Insists U.S. Computer Chip Has Big Flaw. *Detroit Free Press*.

McConnell, M., Chertoff, M., & Lynn, W. (2015, July 28). Why the fear over ubiquitous data encryption is overblown. *Washington Post*. Retrieved from https://www.washingtonpost.com/opinions/the-need-for-ubiquitous-data-encryption/2015/07/28/3d145952-324e-11e5-8353-1215475949f4_story.html

Medcraft, G. (2018, March). *The OECD and the Blockchain Revolution*. Presented at the OECD Friends of Going Digital Meeting, Paris. Retrieved from https://www.oecd.org/parliamentarians/meetings/meeting-on-the-road-london-april-2018/The-OECD-and-the-Blockchain-Revolution-Presentation-by-Greg-Medcraft-delivered-on-29-March-2018.pdf

Meinrath, S. D., & Vitka, S. (2014). Crypto War II. *Critical Studies in Media Communication*, *31*(2), 123–128. https://doi.org/10.1080/15295036.2014.921320

Menn, J. (2013, December 20). Exclusive: Secret contract tied NSA and security industry pioneer. *Reuters*. Retrieved from https://www.reuters.com/article/us-usa-security-

rsa/exclusive-secret-contract-tied-nsa-and-security-industry-pioneer-idUSBRE9BJ1C220131220

Merkle, R. (1991). Fast Software Encryption Functions. *Advances in Cryptology*, 476.

Nakashima, E., & Gellman, B. (2015, April 10). As encryption spreads, U.S. grapples with clash between privacy, security. *Washington Post*. Retrieved from https://www.washingtonpost.com/world/national-security/as-encryption-spreads-us-worries-about-access-to-data-for-investigations/2015/04/10/7c1c7518-d401-11e4-a62f-ee745911a4ff_story.html

Nakashima, E., & Peterson, A. (2015a, September 16). Obama faces growing momentum to support widespread encryption. *Washington Post*. Retrieved from https://www.washingtonpost.com/world/national-security/tech-trade-agencies-push-to-disavow-law-requiring-decryption-of-phones/2015/09/16/1fca5f72-5adf-11e5-b38e-06883aacba64_story.html

Nakashima, E., & Peterson, A. (2015b, October 8). Obama administration opts not to force firms to decrypt data – for now. *Washington Post*. Retrieved from https://www.washingtonpost.com/world/national-security/obama-administration-opts-not-to-force-firms-to-decrypt-data--for-now/2015/10/08/1d6a6012-6dca-11e5-aa5b-f78a98956699_story.html

National Academies of Sciences, Engineering, and Medicine. (2018). *Decrypting the Encryption Debate: A Framework for Decision Makers*. Retrieved from https://www.nap.edu/catalog/25010/decrypting-the-encryption-debate-a-framework-for-decision-makers

Office of the Inspector General. (2018). *A Special Inquiry Regarding the Accuracy of FBI Statements Concerning its Capabilities to Exploit an iPhone Seized During the San Bernardino Terror Attack Investigation*. Retrieved from U.S. Department of Justice website: https://oig.justice.gov/reports/2018/o1803.pdf

Office of the White House Press Secretary. (1984, September 17). *National Security Decision Directive 145: National Policy on Telecommunications and Automated Information Systems Security*. Retrieved from https://fas.org/irp/offdocs/nsdd145.htm

Office of the White House Press Secretary. (1993, April 15). *Presidential Directive / NSC-5: Public Encryption Management*. Retrieved from https://fas.org/irp/offdocs/pdd/pdd-5.pdf

Pascoe, E. (1998, March 17). The average Net user wants more, not less government involvement in data protection. *The Independent (London)*.

Perlroth, N., & Sanger, D. (2015, October 11). Obama Won't Seek Access to Encrypted User Data. *The New York Times*. Retrieved from https://www.nytimes.com/2015/10/11/us/politics/obama-wont-seek-access-to-encrypted-user-data.html

Pierce, K. J. (1984). Public Cryptography, Arms Export Controls, and the First Amendment: A Need for Legislation. *Cornell International Law Journal*, *17*(1), 197.

Poitras, L., & Greenwald, G. (2013, June 9). NSA whistleblower Edward Snowden: "I don't want to live in a society that does these sort of things" – video. *The Guardian*. Retrieved from https://www.theguardian.com/world/video/2013/jun/09/nsa-whistleblower-edward-snowden-interview-video

Proctor, P., & Byrnes, C. (1999). The politics of cryptography. *Performance Computing*, *17*(11), 25–29.

Quittner, J. (1994, June 8). U.S. Nears Standard on Coding Messages. *Newsday*.

Relyea, H. C. (1994). *Silencing science: National security controls and scientific communication*.

Rivest, R. L., Shamir, A., & Adleman, L. (1978). A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM*, *21*(2), 120–126.

Roeper, F., & Ziring, N. (2012, March). *Address by Fred Roeper, Technical Director, National Security Agency & Neal Ziring, Technical Director, National Security Agency*. Presented at the RSA Conference 2012.

Rosenstein, R. J. (2017, October). *Deputy Attorney General Rod J. Rosenstein Delivers Remarks on Encryption at the United States Naval Academy: Remarks as prepared for delivery*.

Sanger, D. (2014, September 26). Signaling Post-Snowden Era, New iPhone Locks Out N.S.A. *The New York Times*. Retrieved from https://www.nytimes.com/2014/09/27/technology/iphone-locks-out-the-nsa-signaling-a-post-snowden-era-.html

Sanger, D. E. (1987, March 19). Rise and Fall of U.S. Data Directive. *The New York Times*. Retrieved from https://www.nytimes.com/1987/03/19/us/rise-and-fall-of-us-data-directive.html

Sanger, E., & Clausing, J. (2000, January 13). U.S. removes more limits on encryption. *The New York Times*.

Schneier, B. (2015). *Data and Goliath: The hidden battles to collect your data and control your world*. WW Norton & Company.

Schneier, B., & Banisar, D. (1997). *The electronic privacy papers: documents on the battle for privacy in the age of surveillance*. John Wiley & Sons, Inc.

Schneier, B., Seidel, K., & Vijayakumar, S. (2016). *A Worldwide Survey of Encryption Products*. Retrieved from https://www.schneier.com/academic/paperfiles/worldwide-survey-of-encryption-products.pdf

Schulz, W., & Van Hoboken, J. (2016). *Human Rights and Encryption*. Retrieved from UNESCO website: http://unesdoc.unesco.org/images/0024/002465/246527E.pdf

Shearer, J., & Gutmann, P. (1996). Government, cryptography, and the right to privacy. *Journal of Universal Computer Science*, *2*(3), 113–146.

Shumow, D., & Ferguson, N. (2007). *On the Possibility of a Back Door in the NIST SP800-90 Dual Ec Prng*. Retrieved from http://rump2007.cr.yp.to/15-shumow.pdf

Simonite, T. (2013, October 8). NSA's Own Hardware Backdoors May Still Be a "Problem from Hell." *MIT Technology Review*. Retrieved from https://www.technologyreview.com/s/519661/nsas-own-hardware-backdoors-may-still-be-a-problem-from-hell/

Singleton, S. (1998). *Encryption Policy for the 21st century: A future without government-prescribed key recovery*. Retrieved from Cato Institute Policy Analysis website: https://www.cato.org/publications/policy-analysis/encryption-policy-21st-century-future-without-governmentprescribed-key-recovery

Sircar, S. (2017). *The Crypto Wars: Interpreting the Privacy Versus National Security Debate from a Standards Perspective*. Georgetown University, Washington, D.C.

SPIEGEL Staff. (2013, October 27). Embassy Espionage: The NSA's Secret Spy Hub in Berlin. *Spiegel Online*. Retrieved from http://www.spiegel.de/international/germany/cover-story-how-nsa-spied-on-merkel-cell-phone-from-berlin-embassy-a-930205.html

Stamos, A. (2015, March 15). User-Focused Security: End-to-End Encryption Extension for Yahoo Mail. Retrieved from Yahoo Blog website: https://yahoo.tumblr.com/post/113708033335/user-focused-security-end-to-end-encryption

The Economist. (2016, February 27). Taking a bite at the Apple. *The Economist*. Retrieved from https://www.economist.com/science-and-technology/2016/02/27/taking-a-bite-at-the-apple

The New York Times. (2013). Secret Documents Reveal N.S.A. Campaign Against Encryption. *The New York Times*. Retrieved from https://archive.nytimes.com/www.nytimes.com/interactive/2013/09/05/us/documents-reveal-nsa-campaign-against-encryption.html

The White House. (1982, April 2). *Executive Order 12356 —National security information*. Retrieved from https://www.archives.gov/federal-register/codification/executive-order/12356.html

The White House. (2015). *NSC Draft Options Paper on Encryption*. Retrieved from https://www.scribd.com/document/281807768/NSC-Draft-Options-Paper-on-Encryption

Timberg, C. (2013, September 6). Google Encrypts Data Amid Backlash against NSA Spying. *Washington Post*. Retrieved from https://www.washingtonpost.com/business/technology/google-encrypts-data-amid-backlash-against-nsa-spying/2013/09/06/9acc3c20-1722-11e3-a2ec-b47e45e6f8ef_story.html

Timberg, C. (2015, September 18). Newest Androids will join iPhones in offering default encryption, blocking police. *Washington Post*. Retrieved from https://www.washingtonpost.com/news/the-switch/wp/2014/09/18/newest-androids-will-join-iphones-in-offering-default-encryption-blocking-police/

Timberg, C., Gellman, B., & Soltani, A. (2013, November 26). Microsoft, suspecting NSA spying, to ramp up efforts to encrypt its Internet traffic. *Washington Post*. Retrieved from https://www.washingtonpost.com/business/technology/microsoft-suspecting-nsa-spying-to-ramp-up-efforts-to-encrypt-its-internet-traffic/2013/11/26/44236b48-56a9-11e3-8304-caf30787c0a9_story.html

Van Hoboken, J., & Rubinstein, I. (2013). Privacy and security in the cloud: Some realism about technical solutions to transnational surveillance in the Post-Snowden Era. *Maine Law Review*, *66*, 487.

Walport, M. (2016). *Distributed ledger technology: beyond block chain*. Retrieved from UK Government Office for Science website: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/492972/gs-16-1-distributed-ledger-technology.pdf

Wang, X., Yin, Y. L., & Yu, H. (2005). Finding collisions in the full SHA-1. *Annual International Cryptology Conference*, 17–36. Springer.

Watt, N., Mason, R., & Traynor, I. (2015, January 12). David Cameron pledges anti-terror law for internet after Paris attacks. *The Guardian*. Retrieved from https://www.theguardian.com/uk-news/2015/jan/12/david-cameron-pledges-anti-terror-law-internet-paris-attacks-nick-clegg

Weingarten, F. W. (1992). Cryptography and National Security. *Information Systems Security*, *1*(1), 9–12. https://doi.org/10.1080/19393559208551309

Weitzner, D. J. (2016, March 16). The Encryption Debate Enters Phase Two. Retrieved from Lawfare website: https://www.lawfareblog.com/encryption-debate-enters-phase-two

Wittes, B. (2015, September 18). The Obama Administration's Encryption Wrangling. Retrieved August 14, 2018, from Lawfare website: https://www.lawfareblog.com/obama-administrations-encryption-wrangling

Chapter 7: Artificial Intelligence

2018 Public-Private Analytic Exchange Program. (2018). *Emerging Technology and National Security*. Retrieved from Department of Homeland Security (DHS) website: https://www.dhs.gov/sites/default/files/publications/2018_AEP_Emerging_Technology_and_National_Security.pdf

ACLU. (2018, May 22). *Amazon Rekognition Coalition Letter to Jeffrey P. Bezos*. Retrieved from https://www.aclunc.org/docs/20180522_AR_Coalition_Letter.pdf

AI Now Institute. (2018, October 24). AI in 2018: A Year in Review. Retrieved from AI Now Institute Blog website: https://medium.com/@AINowInstitute/ai-in-2018-a-year-in-review-8b161ead2b4e?_hsenc=p2ANqtz--C_ZUXgmw0DPz2_QDAM70a27Mzyxoc_Y70F6UtFHxYQCSLhZ8DubXSSw3X3nRA8pMD3vBgCHTBOm0d3ZlZ9VQhpqEAPg&_hsmi=68751142

Allen, G., & Chan, T. (2017). *Artificial Intelligence and National Security*. Belfer Center for Science and International Affairs.

Amazonians. (2018). *Letter to Jeff Bezos*. Retrieved from https://www.scribd.com/document/382334740/Dear-Jeff?campaign=SkimbitLtd&ad_group=44681X1458326X9354476c7cb92ebbd7a6950bd5ad7b80&keyword=660149026&source=hp_affiliate&medium=affiliate

Amodei, D., Olah, C., Steinhardt, J., Christiano, P., Schulman, J., & Mané, D. (2016). Concrete Problems in AI Safety. *ArXiv*. Retrieved from https://arxiv.org/abs/1606.06565

Ashkenas, J. (2018, December 11). Sundar Pichai's Congressional Testimony on Google's Project Dragonfly. Retrieved from Observable website: https://observablehq.com/@jashkenas/sundar-pichais-congressional-testimony-on-googles-projec

Auslin, M. (2018, October 23). Can the Pentagon Win the AI Arms Race? *Foreign Affairs*. Retrieved from https://www.foreignaffairs.com/articles/united-states/2018-10-19/can-pentagon-win-ai-arms-race

BAE Systems. (n.d.). Taranis. Retrieved March 6, 2019, from BAE Systems website: https://www.baesystems.com/en/product/taranis

Bank of America Merrill Lynch. (2015). *Robot Revolution - Global Robot & AI Primer*. Retrieved from Bank of America Merrill Lynch website: http://www.bofaml.com/content/dam/boamlimages/documents/PDFs/robotics_and_ai_condensed_primer.pdf

Barnes, J. E., & Chin, J. (2018, March 2). The New Arms Race in AI. *Wall Street Journal*. Retrieved from https://www.wsj.com/articles/the-new-arms-race-in-ai-1520009261

Bergen, M. (2015, November 26). Mercedes-Benz Wants to Beat Google, Uber to Our Driverless Future. *Recode*. Retrieved from http://www.recode.net/2015/11/26/11620962/mercedes-benz-wants-to-beat-google-uber-to-our-driverlessfuture

Bezos, J. (2017, April 17). 2016 Letter to Shareholders. Retrieved April 7, 2018, from The Amazon Blog website: https://blog.aboutamazon.com/working-at-amazon/2016-letter-to-shareholders

Bidwell, C. A., & MacDonald, B. W. (2018). *Emerging Disruptive Technologies and Their Potential Threat to Strategic Stability and National Security*. Retrieved from Federation of American Scientists website: https://fas.org/wp-content/uploads/media/FAS-Emerging-Technologies-Report.pdf?utm_source=FAS+General&utm_campaign=9b44d2bccd-EMAIL_CAMPAIGN_2017_02_21_COPY_01&utm_medium=email&utm_term=0_56a7496199-9b44d2bccd-199323333

Bloomberg Opinion Editorial Board. (2017, October 22). Think the U.S. Has a Facebook Problem? Look to Asia. *Bloomberg Opinion*. Retrieved from https://www.bloomberg.com/opinion/articles/2017-10-22/facebook-has-a-bigger-problem-than-washington

Booz Allen Hamilton. (2018, July 30). U.S. Government & GSA FEDSIM Select Booz Allen to Help Apply Artificial Intelligence. Retrieved from Booz Allen Hamilton website: https://www.boozallen.com/e/media/press-release/booz-allen-selected-to-help-apply-artificial-intelligence.html

Bremmer, N. T., Ian. (2018, October 23). The AI Cold War That Threatens Us All. *Wired*. Retrieved from https://www.wired.com/story/ai-cold-war-china-could-doom-us-all/

Brown, M., & Singh, P. (2018). *China's Technology Transfer Strategy: How Chinese Investments in Emerging Technology Enable A Strategic Competitor to Access the Crown Jewels of U.S. Innovation*. Retrieved from Defense Innovation Unit Experimental (DIUx) website: https://admin.govexec.com/media/diux_chinatechnologytransferstudy_jan_2018_(1).pdf

Brundage, M., Avin, S., Clark, J., Toner, H., Eckersley, P., Garfinkel, B., … Amodei, D. (2018). *The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation*. Retrieved from Future of Humanity Institute website: https://maliciousaireport.com/

Bryant, R. (2016, February 12). Google's AI Becomes First Non-Human to Qualify as a Driver. *Dezeen*. Retrieved from https://www.dezeen.com/2016/02/12/google-self-driving-car-artficial-intelligence-system-recognized-as-driver-usa

Brynjolfsson, E., & Mitchell, T. (2017). What can machine learning do? Workforce implications. *Science*, *358*(6370), 1530–1534. https://doi.org/10.1126/science.aap8062

Bureau of Industry and Security, Commerce. (2018, November 19). *Review of Controls for Certain Emerging Technologies*. Retrieved from https://www.federalregister.gov/documents/2018/11/19/2018-25221/review-of-controls-for-certain-emerging-technologies

Burgess, M. (2015). Microsoft's AI Can Detect Your Emotions (but Only If You're Angry). *Wired*. Retrieved from http://www.wired.co.uk/article/microsoft-predictemotions-artificial-intelligence

Busby, M. (2018, April 9). Killer robots: pressure builds for ban as governments meet. *The Guardian*. Retrieved from https://www.theguardian.com/technology/2018/apr/09/killer-robots-pressure-builds-for-ban-as-governments-meet

Carter, A. (2016, October). *Keynote Address: The Path to the Innovative Future of Defense*. Presented at the Center for Strategic and International Studies: Assessing the Third Offset Strategy: Progress and Prospects for Defense Innovation, CSIS Headquarters, Washington, D.C. Retrieved from https://csis-prod.s3.amazonaws.com/s3fs-public/event/161028_Secretary_Ashton_Carter_Keynote_Address_The_Path_to_the_Innovative_Future_of_Defense.pdf

Cassano, J. (2018, August 15). Pentagon's Artificial Intelligence Programs Get Huge Boost in the NDAA. *Sludge*. Retrieved from https://readsludge.com/2018/08/15/pentagons-artificial-intelligence-programs-get-huge-boost-in-the-ndaa/

CB Insights. (2017, February 3). From Virtual Nurses To Drug Discovery: 106 Artificial Intelligence Startups In Healthcare. Retrieved from CB Insights Research Briefs website: https://www.cbinsights.com/research/artificial-intelligence-startups-healthcare/

CB Insights. (2018, February 27). *The Race For AI: Google, Intel, Apple In A Rush To Grab Artificial Intelligence Startups*. Retrieved from https://www.cbinsights.com/research/top-acquirers-ai-startups-ma-timeline/

Chan, T. F. (2018, March 27). Parts of China are using facial recognition technology that can scan the country's entire population in one second. *Business Insider US*. Retrieved from

https://www.businessinsider.sg/china-facial-recognition-technology-works-in-one-second-2018-3/

Chen, A. (2019, June 5). Regulating or breaking up Big Tech: an antitrust explainer. *MIT Technology Review*. Retrieved from https://www.technologyreview.com/s/613628/big-tech-breakup-regulation-antitrust-apple-amazon-google-facebook-doj-ftc-policy/

Chesney, R., & Citron, D. K. (2019). Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security. *California Law Review*, *107*. Retrieved from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3213954

Choudhury, S. R. (2018, February 28). Alibaba just set up its first joint research center outside China to focus on A.I. *CNBC*. Retrieved from https://www.cnbc.com/2018/02/28/alibaba-sets-up-joint-a-i-research-lab-in-singapore.html

Clark, C. (2017, November 1). Our Artificial Intelligence 'Sputnik Moment' Is Now: Eric Schmidt & Bob Work. *Breaking Defense*. Retrieved from https://breakingdefense.com/2017/11/our-artificial-intelligence-sputnik-moment-is-now-eric-schmidt-bob-work/

Clifford, C. (2018, February 1). Google CEO: A.I. is more important than fire or electricity. *CNBC*. Retrieved from https://www.cnbc.com/2018/02/01/google-ceo-sundar-pichai-ai-is-more-important-than-fire-electricity.html

Cockburn, I. M., Henderson, R., & Stern, S. (2018). The Impact of Artificial Intelligence on Innovation: An Exploratory Analysis. In A. K. Agrawal, J. Gans, & A. Goldfarb (Eds.), *The Economics of Artificial Intelligence: An Agenda*. Retrieved from https://www.nber.org/chapters/c14006

Conger, K. (2018a, May 14). Google Employees Resign in Protest Against Pentagon Contract. *Gizmodo*. Retrieved from https://gizmodo.com/google-employees-resign-in-protest-against-pentagon-con-1825729300

Conger, K. (2018b, June 1). Google Plans Not to Renew Its Contract for Project Maven, a Controversial Pentagon Drone AI Imaging Program. *Gizmodo*. Retrieved from https://gizmodo.com/google-plans-not-to-renew-its-contract-for-project-mave-1826488620

Conger, K., & Cameron, D. (2018, March 6). Google is helping the Pentagon build AI drones. *Gizmodo*. Retrieved from https://gizmodo.com/google-is-helping-the-pentagon-build-ai-for-drones-1823464533

Crevier, D. (1993). *AI: The Tumultuous Search for Artificial Intelligence*. New York: Basic Books.

Cylance. (2017, August 1). *Black Hat Attendees See AI as Double-Edged Sword*. Retrieved from threatmatrix.cylance.com/en_us/home/black-hat-attendees-see-ai-as-double-edged-sword.html.

Dafoe, A. (2018). *AI Governance: A Research Agenda*. Retrieved from Future of Humanity Institute website: https://www.fhi.ox.ac.uk/wp-content/uploads/GovAIAgenda.pdf

Danzig, R. (2018). *Technology Roulette*. Retrieved from Center for a New American Security website: https://www.cnas.org/publications/reports/technology-roulette

DARPA. (1983). *Strategic Computing--New Generation Technology: A Strategic Plan for Its Development and Application to Critical Problems in Defense*. Arlington, VA: - Defense Advanced Research Projects Agency (DARPA).

De Spiegeleire, S., Maas, M., & Sweijs, T. (2017). *Artificial Intelligence and the Future of Defense: Strategic Implications for Small and Medium Sized Force Providers*. Retrieved from The Hague Centre for Strategic Studies website: https://hcss.nl/sites/default/files/files/reports/Artificial%20Intelligence%20and%20the%20Future%20of%20Defense.pdf

DeepMind. (2017). The story of AlphaGo so far. Retrieved from DeepMind Blog website: https://deepmind.com/research/alphago/

DeepMind. (2018). AlphaStar: Mastering the Real-Time Strategy Game StarCraft II. Retrieved from DeepMind Blog website: https://deepmind.com/blog/alphastar-mastering-real-time-strategy-game-starcraft-ii/

DeepMind Ethics & Society. (n.d.). DeepMind Ethics & Society Principles. Retrieved from DeepMind website: https://deepmind.com/applied/deepmind-ethics-society/principles/

Defense Advanced Research Projects Agency (DARPA). (1997). *DARPA Technology Transition*. Arlington, VA: DARPA.

Defense Advanced Research Projects Agency (DARPA). (2018, September 7). DARPA Announces $2 Billion Campaign to Develop Next Wave of AI Technologies. Retrieved from DARPA website: https://www.darpa.mil/news-events/2018-09-07

Defense Innovation Board (DIB). (n.d.). Defense Innovation Board: Recommendations. Retrieved from Defense Innovation Board website: https://innovation.defense.gov/Recommendations/

Defense Science Board. (2016). *Summer Study on Autonomy*. Retrieved from United States Defense Science Board website: https://www.hsdl.org/?abstract&did=794641

Department of Defense (DOD). (2014). *Unmanned Systems Integrated Roadmap: FY2013-2038*. Retrieved from Department of Defense website: https://apps.dtic.mil/dtic/tr/fulltext/u2/a592015.pdf

Department of Defense (DOD). (2018). *Summary of the 2018 National Defense Strategy of the United States of America*. Retrieved from The White House website: https://dod.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf

Department of Defense Office of Net Assessment. (2016). *Summer Study: (Artificial) Intelligence: What questions should DoD be asking*. Washington, DC: Department of Defense.

Ding, J. (2018). *Deciphering China's AI Dream: The context, components, capabilities and consequences of China's strategy to lead the world in AI*. Retrieved from Future of Humanity Institute website: https://www.fhi.ox.ac.uk/wp-content/uploads/Deciphering_Chinas_AI-Dream.pdf

Eckersley, P., & Nasser, Y. (2017). AI Progress Measurement. Retrieved from Electronic Frontiers Foundation (EFF) website: https://www.eff.org/ai/metrics

Etherington, D. (2018, March 19). An Uber self-driving car in autonomous mode hit and killed a pedestrian in Tempe, Arizona. *TechCrunch*. Retrieved from https://techcrunch.com/2018/03/19/uber-self-driving-test-car-involved-in-accident-resulting-in-pedestrian-death/

Executive Office of the President. (2016). *Artificial Intelligence, Automation, and the Economy*. Washington DC: Executive Office of the President.

Faggella, D. (2019, February 19). Valuing the Artificial Intelligence Market, Graphs and Predictions | Emerj - Artificial Intelligence Research and Insight. *Emerj*. Retrieved from https://emerj.com/ai-sector-overviews/valuing-the-artificial-intelligence-market-graphs-and-predictions/

Fang, L. (2018, November 27). Amnesty International to Stage Worldwide Protests Against Google's "Dystopian" Censored Search for China. *The Intercept*. Retrieved from https://theintercept.com/2018/11/26/google-dragonfly-project-china-amnesty-international/

Fang, L. (2019, March 9). Defense Tech Startup Founded by Trump's Most Prominent Silicon Valley Supporters Wins Secretive Military AI Contract. *The Intercept*. Retrieved from https://theintercept.com/2019/03/09/anduril-industries-project-maven-palmer-luckey/

Felten, E. (2016, May 3). Preparing for the Future of Artificial Intelligence. Retrieved April 8, 2018, from The White House Blog website:

https://obamawhitehouse.archives.gov/blog/2016/05/03/preparing-future-artificial-intelligence

Financial Times. (2007, December 31). *FT Global 500 December 2007*. Retrieved from https://im.ft-static.com/content/images/813c979e-0faa-11dd-8871-0000779fd2ac.pdf

Financial Times. (2017, December 31). *FT Global 500 December 2017*. Retrieved from https://www.ft.com/signup?offerId=1dbc248e-b98d-b703-bc25-a05cc5670804&ft-co=markets-inline

Financial Times (FT). (2015, December 15). The Future Military-Artificial Intelligence Complex? *Financial Times*. Retrieved from https://ftalphaville.ft.com/2015/12/15/2147846/the-future-military-artificial-intelligence-complex/

Fleck, J. (1982). Development and Establishment in Artificial Intelligence. In N. Elias (Ed.), *Scientific Establishments and Hierarchies* (pp. 169–217). Dordrecht, Holland: Reidel Publishing Company.

Ford, M. (2018). *Architects of Intelligence: The truth about AI from the people building it*. Packt Publishing Limited.

Forrest, C. (2018, April 5). South Korea university faces major backlash after opening AI weapons lab. *TechRepublic*. Retrieved from https://www.techrepublic.com/article/south-korea-university-faces-major-backlash-after-opening-ai-weapons-lab/

Freedberg Jr., S. J. (2018, June 29). Joint Artificial Intelligence Center Created Under DoD CIO. *Breaking Defense*. Retrieved from https://breakingdefense.com/2018/06/joint-artificial-intelligence-center-created-under-dod-cio/

Furman, J. (2016). *Is This Time Different? The Opportunities and Challenges of Artificial Intelligence [Remarks at AI Now: The Social and economic Implications of Artificial Intelligence Technologies in the Near Term]*. Retrieved from New York University website: https://obamawhitehouse.archives.gov/sites/default/files/page/files/20160707_cea_ai_furman.pdf

Furness, D. (2016, October 6). AI in Agriculture? Algorithms Help Farmers Spot Crop Disease like Experts. *Digital Trends*. Retrieved from http://www.digitaltrends.com/computing/ai-crop-disease/

Future of Life Institute. (2017). Asilomar AI Principles. Retrieved from https://futureoflife.org/ai-principles/?cn-reloaded=1

Future of Life Institute. (n.d.). National and International AI Strategies. Retrieved December 11, 2018, from https://futureoflife.org/national-international-ai-strategies/

Gallagher, R. (2018a, November 29). Google Shut Out Privacy and Security Teams from Secret China Project. *The Intercept*. Retrieved from https://theintercept.com/2018/11/29/google-china-censored-search/

Gallagher, R. (2018b, December 17). Google's Secret China Project "Effectively Ended" After Internal Confrontation. *The Intercept*. Retrieved from https://theintercept.com/2018/12/17/google-china-censored-search-engine-2/

Geist, E., & Lohn, A. (2018). *How Might Artificial Intelligence Affect the Risk of Nuclear War?* Retrieved from RAND Corporation website: https://www.rand.org/pubs/perspectives/PE296.html

Gibney, E. (2016). Google's AI reasons its way around the London Underground. *Nature News*. https://doi.org/10.1038/nature.2016.20784

Goldfarb, A., & Trefler, D. (2018). AI and International Trade. In A. K. Agrawal, J. Gans, & A. Goldfarb (Eds.), *The Economics of Artificial Intelligence: An Agenda*. Retrieved from https://www.nber.org/chapters/c14012

Goldstein, N. (1992). Defense Advanced Research Project Agency's Role in Artificial Intelligence R&D: Case Study of the Military as the National Agent for Technological and Industrial Change. *Defense Analysis*, *8*(1), 61–80.

Goodfellow, I. J., Pouget-Abadie, J., Mirza, M., Xu, B., Warde-Farley, D., Ozair, S., … Bengio, Y. (2014). Generative Adversarial Networks. *ArXiv:1406.2661 [Cs, Stat]*. Retrieved from http://arxiv.org/abs/1406.2661

Google. (2010a, January 12). A new approach to China. Retrieved from Google Official Blog website: https://googleblog.blogspot.com/2010/01/new-approach-to-china.html

Google. (2010b, March 22). A new approach to China: an update. Retrieved from Google Official Blog website: https://googleblog.blogspot.com/2010/03/new-approach-to-china-update.html

Google Employees Against Dragonfly. (2018, November 27). We are Google employees. Google must drop Dragonfly. Retrieved from Medium website: https://medium.com/@googlersagainstdragonfly/we-are-google-employees-google-must-drop-dragonfly-4c8a30c5e5eb

Granville, K. (2018, March 19). Facebook and Cambridge Analytica: What You Need to Know as Fallout Widens. *The New York Times*. Retrieved from https://www.nytimes.com/2018/03/19/technology/facebook-cambridge-analytica-explained.html

Gunning, D. (n.d.). Explainable Artificial Intelligence (XAI). Retrieved April 8, 2018, from Defense Advanced Research Projects Agency (DARPA) website: https://www.darpa.mil/program/explainable-artificial-intelligence

HAL 90210. (2016, June 10). This Is What Happens When an AI-Written Screenplay Is Made into a Film. *The Guardian*. Retrieved from https://www.theguardian.com/technology/2016/jun/10/artificial-intelligence-screenplay-sunspring-silicon-valley-thomas-middleditch-ai

Hauteville, J.-M. (2017, January 17). Satya Nadella: Calling for Global Cooperation on Artificial Intelligence. *Handelsblatt TODAY*. Retrieved from https://www.handelsblatt.com/today/companies/satya-nadella-calling-for-global-cooperation-on-artificial-intelligence/23565430.html

Hermann, K. M., Kočiský, T., Grefenstette, E., Espeholt, L., Kay, W., Suleyman, M., & Blunsom, P. (2015). Teaching Machines to Read and Comprehend. *ArXiv:1506.03340 [Cs]*. Retrieved from http://arxiv.org/abs/1506.03340

Hinton, G. E., Srivastava, N., Krizhevsky, A., Sutskever, I., & Salakhutdinov, R. R. (2012). Improving neural networks by preventing co-adaptation of feature detectors. *ArXiv Preprint ArXiv:1207.0580*.

Hogarth, I., & Benaich, N. (2018). *The State of Artificial Intelligence in 2018: A Good Old Fashioned Report*. Retrieved from https://www.stateof.ai/

Horwitz, J. (2017, June 7). A key question is at the heart of China's new cybersecurity law: Where should data live? *Quartz*. Retrieved from https://qz.com/999613/a-key-question-at-the-heart-of-chinas-cybersecurity-law-where-should-data-live/

Howard, P. N., & Woolley, S. C. (2017). *Computational Propaganda Worldwide: Executive Summary* (No. Working Paper No. 2017.11). Retrieved from Oxford Internet Institute website: http://comprop.oii.ox.ac.uk/wp-content/uploads/sites/89/2017/06/Casestudies-ExecutiveSummary.pdf

Hutchins, J. (2005). *The history of machine translation in a nutshell*. Retrieved from http://www.hutchinsweb.me.uk/Nutshell-2005.pdf

Isaac, M., & Boudette, N. E. (2017, February 10). Ford to Invest $1 Billion in Artificial Intelligence Start-Up. *The New York Times*. Retrieved from https://www.nytimes.com/2017/02/10/technology/ford-invests-billion-artificial-intelligence.html

Israel Aerospace Industries. (n.d.). HARPY NG. Retrieved March 6, 2019, from Israel Aerospace Industries website: http://www.iai.co.il/2013/36694-16153-en/Business_Areas_Land.aspx

Iyengar, V. (2016, August 24). Why AI consolidation will create the worst monopoly in US history. *TechCrunch*. Retrieved from http://social.techcrunch.com/2016/08/24/why-ai-consolidation-will-create-the-worst-monopoly-in-us-history/

Jang, E. (2017, February 24). What Companies Are Winning The Race For Artificial Intelligence? *Forbes*. Retrieved from https://www.forbes.com/sites/quora/2017/02/24/what-companies-are-winning-the-race-for-artificial-intelligence/

JASON. (2017). *Perspective on Research in Artificial Intelligence and Artificial General Intelligence Relevant to DoD*. Washington, DC: The MITRE Corporation.

Jeangene Vilmer, J.-B. (2017, September 22). The French Turn to Armed Drones. *War on the Rocks*. Retrieved from https://warontherocks.com/2017/09/the-french-turn-to-armed-drones/

Jee, C. (2019, April 5). Google has now cancelled its AI ethics board after a backlash from staff. *MIT Technology Review*. Retrieved from https://www.technologyreview.com/f/613271/google-has-now-cancelled-its-ai-ethics-board-after-a-backlash-from-staff/

Johnson, T. R. (2016, November 29). Donald Trump's Pentagon and the Future of the Third Offset Strategy: Will the Department of Defense Invest in People or Technology? *The Atlantic*. Retrieved from https://www.theatlantic.com/politics/archive/2016/11/trump-military-third-offset-strategy/508964/

Jones, N. (2017). How machine learning could help to improve climate forecasts. *Nature News*, *548*(7668), 379. https://doi.org/10.1038/548379a

Kahn, R. (1988). Later Years at IPTO. In H. W. Sams (Ed.), *Expert Systems and Artificial Intelligence: Applications and Management* (By T. C. Bartee). Indianapolis, Ind.: Sams Technical Publishing.

Kaminska, I. (2017, November 2). When AI becomes too big to fail. *Financial Times*. Retrieved from http://ftalphaville.ft.com/2017/11/01/2195451/when-ai-becomes-too-big-to-fail/

Karmanov, F., & Hudson, S. (2018). *Global AI Talent Report 2018*. Retrieved from jfg website: http://www.jfgagne.ai/talent/

Karnofsky, H. (2016, May 6). Some Background on Our Views Regarding Advanced Artificial Intelligence. Retrieved April 7, 2018, from Open Philanthropy Project website:

https://www.openphilanthropy.org/blog/some-background-our-views-regarding-advanced-artificial-intelligence

Kleeman, A. (2016). Cooking with Chef Watson, I.B.M.'s Artificial-Intelligence App. *The New Yorker*. Retrieved from http://www.newyorker.com/magazine/2016/11/28/cooking-with-chef-watson-ibms-artificial-intelligence-app

Knight, H. (2006). Early Artificial Intelligence Projects. Retrieved December 14, 2018, from https://projects.csail.mit.edu/films/aifilms/AIFilms.html

Krakovna, V. (2018). Specification gaming examples in AI. Retrieved from Deep Safety website: https://vkrakovna.wordpress.com/2018/04/02/specification-gaming-examples-in-ai/

Krauth, O. (2018, January 12). The 10 tech companies that have invested the most money in AI. *TechRepublic*. Retrieved from https://www.techrepublic.com/article/the-10-tech-companies-that-have-invested-the-most-money-in-ai/

LeCun, Y., Boser, B., Denker, J. S., Henderson, D., Howard, R. E., Hubbard, W., & Jackel, L. D. (1989). Backpropagation Applied to Handwritten Zip Code Recognition. *Neural Computation*, *1*(4), 541–551.

Lee, K.-F. (2018, September 17). AI Could Devastate the Developing World. *Bloomberg Opinion*. Retrieved from https://www.bloomberg.com/opinion/articles/2018-09-17/artificial-intelligence-threatens-jobs-in-developing-world

Lehman, J., Clune, J., Misevic, D., Adami, C., Altenberg, L., Beaulieu, J., … Yosinski, J. (2018). The Surprising Creativity of Digital Evolution: A Collection of Anecdotes from the Evolutionary Computation and Artificial Life Research Communities. *ArXiv:1803.03453 [Cs.NE]*. Retrieved from https://arxiv.org/abs/1803.03453

Leung, J., & Fischer, S.-C. (2018, August 8). JAIC: Pentagon debuts artificial intelligence hub. *Bulletin of the Atomic Scientists*. Retrieved from https://thebulletin.org/2018/08/jaic-pentagon-debuts-artificial-intelligence-hub/

Leung, J., Fischer, S.-C., & Dafoe, A. (2019, August 28). Export Controls in the Age of AI. *War on the Rocks*. Retrieved from https://warontherocks.com/2019/08/export-controls-in-the-age-of-ai/

Lewis-Kraus, G. (2016, December 14). The Great A.I. Awakening. *The New York Times Magazine*. Retrieved from https://www.nytimes.com/2016/12/14/magazine/the-great-ai-awakening.html

Lighthill, J. (1973). Artificial Intelligence: A General Survey. *Artificial Intelligence: A Paper Symposium*. Retrieved from www.math.snu.ac.kr/~hichoi/infomath/Articles/Lighthill%20Report.pdf

Marshall, A. (2017, January 22). From Jingles to Pop Hits, A.I. Is Music to Some Ears. *The New York Times*. Retrieved from https://www.nytimes.com/2017/01/22/arts/music/jukedeck-artificial-intelligence-songwriting.html

Martinage, R. (2014). *Toward a New Offset Strategy: Exploiting U.S. Long-Term Advantages to Restore U.S. Global Power Projection Capability*. Retrieved from Center for Strategic and Budgetary Assessments website: https://csbaonline.org/research/publications/toward-a-new-offset-strategy-exploiting-u-s-long-term-advantages-to-restore

McCain, J. S. *National Defense Authorization Act for Fiscal Year 2019*. , Pub. L. No. H.R.5515 (2018).

McCarthy, J., Minsky, M. L., Rochester, N., & Shannon, C. E. (2006). A Proposal for the Dartmouth Summer Research Project on Artificial Intelligence, August 31, 1955. *AI Magazine*, *27*(4). Retrieved from https://aaai.org/ojs/index.php/aimagazine/article/view/1904

McClain, D. (1998, January 19). Voice Technology Appears Ready to Recognize Bottom Line. *The New York Times*.

McCorduck, P. (2004). *Machines who Think: A Personal Inquiry Into the History and Prospects of Artificial Intelligence:* AK Peters.

McCulloch, W. S., & Pitts, W. (1943). A logical calculus of the ideas immanent in nervous activity. *Bulletin of Mathematical Biophysics*, *5*.

Menegus, B. (2018, April 4). Thousands of Google Employees Protest Company's Involvement in Pentagon AI Drone Program. *Gizmodo*. Retrieved from https://gizmodo.com/thousands-of-google-employees-protest-companys-involvem-1824988565

Metz, C. (2015). Teaching AI to play Atari will help robots make sense of our world. *Wired*. Retrieved from https://www.wired.com/2015/12/teaching-ai-to-play-atari-will-help-robots-make-sense-of-our-world/

Metz, C. (2018, August 26). Artificial Intelligence Is Now a Pentagon Priority. Will Silicon Valley Help? *The New York Times*. Retrieved from https://www.nytimes.com/2018/08/26/technology/pentagon-artificial-intelligence.html

Metz, R. (2015). Toyota Investing $50M for Autonomous-Car Research at Stanford and MIT. *MIT Technology Review*. Retrieved from https://www.technologyreview.com/s/541046/toyota-investing-50m-with-stanford-mit-for-autonomouscar-research/

Microsoft employees. (2018, October 13). An Open Letter to Microsoft: Don't Bid on the US Military's Project JEDI. Retrieved from Medium website: https://medium.com/s/story/an-open-letter-to-microsoft-dont-bid-on-the-us-military-s-project-jedi-7279338b7132

Minsky, M. L. (1956). *Heuristic Aspects of the Artificial Intelligence Problem* (No. Report 34-55 ASTIA Doc. No. AS236885). Cambridge, MA: MIT Lincoln Laboratory.

Minsky, M. L. (1979). The Society Theory of Thinking. In P. H. Winston & R. H. Brown, *Artificial Intelligence: An MIT Perspective* (pp. 423–450). Cambridge, MA: MIT Press.

Moravec, H. (1995). *Mind Children: The Future of Robot and Human Intelligence*. Cambridge, MA: Harvard University Press.

Mulholland, M. (2018, November 7). Our shared responsibility for AI. Retrieved April 5, 2019, from Microsoft Partner Network website: https://blogs.partner.microsoft.com/mpn/shared-responsibility-ai-2/

Mulvaney, M., & Kratsios, M. (2018, July 31). *Memorandum for the Heads of Executive Departments and Agencies: FY 2020 Administration Research and Development Budget Priorities*. Retrieved from https://www.whitehouse.gov/wp-content/uploads/2018/07/M-18-22.pdf

Nadella, S. (2018, March 28). Satya Nadella email to employees: Embracing our future: Intelligent Cloud and Intelligent Edge. Retrieved April 7, 2018, from Microsoft News Center website: https://news.microsoft.com/2018/03/29/satya-nadella-email-to-employees-embracing-our-future-intelligent-cloud-and-intelligent-edge/

National Research Council. (1999). Developments in Artificial Intelligence. In *Funding a Revolution: Government Support for Computing Research*. https://doi.org/10.17226/6323

National Science and Technology Council. (2016a). *Preparing for the Future of Artificial Intelligence*. Washington DC: Executive Office of the President.

National Science and Technology Council. (2016b). *The National Artificial Intelligence Research and Development Strategic Plan*. Washington DC: Executive Office of the President.

Newell, A. (1989). Reports on artificial intelligence from Carnegie-Mellon University: introduction to the COMTEX microfiche edition. *Readings from the AI Magazine*, 328–332. American Association for Artificial Intelligence.

Newell, A., Shaw, J. C., & Simon, H. A. (1959). *Report on a general problem solving program*. Santa Monica, California: RAND Corporation.

Newell, A., & Simon, H. A. (1956). *Current developments in complex information processing*. Santa Monica, California: RAND Corporation.

Ng, A. (2016, November 9). What Artificial Intelligence Can and Can't Do Right Now. *Harvard Business Review*. Retrieved from https://hbr.org/2016/11/what-artificial-intelligence-can-and-cant-do-right-now

Nix, N. (2018, October 8). Google Drops Out of Pentagon's $10 Billion Cloud Competition. *Bloomberg*. Retrieved from https://www.bloomberg.com/news/articles/2018-10-08/google-drops-out-of-pentagon-s-10-billion-cloud-competition

Novet, J., & Pramuk, J. (2018, June 18). Microsoft condemns "forcible separation" of children from families after criticism over work with ICE. *CNBC*. Retrieved from https://www.cnbc.com/2018/06/18/microsoft-condemns-forcible-separation-of-families-after-ice-flap.html

Office of Science and Technology Policy. (2018a). *Summary of the 2018 White House Summit on Artificial Intelligence for American Industry*. Retrieved from The White House website: https://www.whitehouse.gov/wp-content/uploads/2018/05/Summary-Report-of-White-House-AI-Summit.pdf

Office of Science and Technology Policy. (2018b, June 27). Readout from the Inaugural Meeting of the Select Committee on Artificial Intelligence. Retrieved from White House OSTP website: https://epic.org/privacy/ai/WH-AI-Select-Committee-First-Meeting.pdf

Office of Technology Assessment (OTA). (1985). *Information Technology R&D: Critical Trends and Issues, OTA-CIT-268*. Washington, D.C.: U.S. Government Printing Office.

OpenAI. (2018, April 9). OpenAI Charter. Retrieved April 5, 2019, from OpenAI website: https://openai.com/charter/

Osborn, K. (2017, June 1). Cisco, DOD move JRSS to cloud tech and greater automation. *Defense Systems*. Retrieved from https://defensesystems.com/articles/2017/06/01/cisco.aspx

Partnership on AI (PAI). (n.d.). About - The Partnership on AI. Retrieved April 5, 2019, from https://www.partnershiponai.org/about/

Paulas, R. (2018, September 4). A New Kind of Labor Movement in Silicon Valley. *The Atlantic*. Retrieved from https://www.theatlantic.com/technology/archive/2018/09/tech-labor-movement/567808/

Pawlyk, O. (2018, July 30). China Leaving US Behind on Artificial Intelligence: Air Force General. *Military.Com*. Retrieved from https://www.military.com/defensetech/2018/07/30/china-leaving-us-behind-artificial-intelligence-air-force-general.html

Paysa. (2017, April 18). U.S. Companies Raising $1 Billion or More to Fuel Artificial Intelligence (AI) Development Looking to Staff 10,000+ Openings, Cites New Paysa Research. *Global News Wire*. Retrieved from https://www.globenewswire.com/news-release/2017/04/18/961603/0/en/U-S-Companies-Raising-1-Billion-or-More-to-Fuel-Artificial-Intelligence-AI-Development-Looking-to-Staff-10-000-Openings-Cites-New-Paysa-Research.html

Pearson, G., Jolley, P., & Evans, G. (2018). A Systems Approach to Achieving the Benefits of Artificial Intelligence in UK Defence. *ArXiv:1809.11089 [Cs]*. Retrieved from http://arxiv.org/abs/1809.11089

Pichai, S. (2018, June 7). AI at Google: our principles. Retrieved from Google Blog: The Keyword website: https://www.blog.google/technology/ai/ai-principles/

PR Newswire. (2018, November 7). Raytheon wins two National Geospatial Agency contracts valued at up to $600M. *Seeking Alpha*. Retrieved from https://seekingalpha.com/pr/17325208-raytheon-wins-two-national-geospatial-agency-contracts-valued-600m

Pressman, A., & Roberts, J. J. (2018, May 31). Data Sheet: What AI Will Do to the Financial System. *Fortune*. Retrieved from http://fortune.com/2018/05/31/data-sheet-ai-finance-jp-morgan-chase/

PwC. (2017). *Sizing the prize: What's the real value of AI for your business and how can you capitalise?* Pricewaterhouse Coopers.

Ratzer, C. (2018, October 1). The U.S. Department of Defense selects BAE Systems to help develop and deliver next generation mission technologies. Retrieved from BAE Systems Newsroom website: https://www.baesystems.com/en-us/article/the-u-s--department-of-defense-selects-bae-systems-to-help-develop-and-deliver-next-generation-mission-technologies

Reed Jr, H. L. (1952). Firing table computations on the ENIAC. *Proceedings of the 1952 ACM National Meeting*, 103–106. Pittsburgh: ACM.

Roland, A., & Shiman, P. (2002). *Strategic Computing: DARPA and the Quest for Machine Intelligence, 1983 - 1993*. Retrieved from https://ondoc.logand.com/d/2721/pdf

Ross, C., & Swetlitz, I. (2018, July 25). IBM's Watson supercomputer recommended 'unsafe and incorrect' cancer treatments, internal documents show. *STAT+*. Retrieved from https://www.statnews.com/wp-content/uploads/2018/09/IBMs-Watson-recommended-unsafe-and-incorrect-cancer-treatments-STAT.pdf

Roumeliotis, G., & Bartz, D. (2017, July 21). Exclusive: U.S. toughens stance on foreign deals in blow to China's buying spree. *Reuters*. Retrieved from https://www.reuters.com/article/us-usa-china-companies-idUSKBN1A532M

Rumelhart, D. E., Hinton, G. E., & Williams, R. J. (1986). Learning representations by back-propagating errors. *Nature*, *323*, 533–536.

Russell, J. (2017, December 13). Google is opening a China-based research lab focused on artificial intelligence. *TechCrunch*. Retrieved from https://techcrunch.com/2017/12/12/google-opening-an-office-focused-on-artificial-intelligence-in-china/

Russell, S. J., & Norvig, P. (2010). *Artificial intelligence: a modern approach* (3rd ed.). Upper Saddle River, N.J.: Prentice Hall.

Sacasas, L. C. (2018). The Tech Backlash We Really Need. *The New Atlantis*, *55*(Spring 2018). Retrieved from https://www.thenewatlantis.com/publications/the-tech-backlash-we-really-need

Samuel, A. L. (1967). Some studies in machine learning using the game of checkers. II—Recent progress. *IBM Journal of Research and Development*, *11*(6), 601–617.

Samuel, S. (2019, April 27). The growing backlash against facial recognition tech. *Vox*. Retrieved from https://www.vox.com/future-perfect/2019/4/27/18518598/ai-facial-recognition-ban-apple-amazon-microsoft

Schleifer, T. (2019, June 4). Why does Washington suddenly seem ready to regulate Big Tech? Look at the polls. *Vox*. Retrieved from https://www.vox.com/2019/6/4/18652469/washington-antitrust-regulate-amazon-google-facebook-look-at-polls

Schmidt, E. (2017). *Eric Schmidt Keynote Address at the Center for a New American Security Artificial Intelligence and Global Security Summit*. Retrieved from Center for a New American Security website: https://www.cnas.org/publications/transcript/eric-schmidt-keynote-address-at-the-center-for-a-new-american-security-artificial-intelligence-and-global-security-summit

Schmidt, E., Kissinger, H., & Huttenlocher, D. (2019, August). The Metamorphosis. *The Atlantic*. Retrieved from https://www.theatlantic.com/magazine/archive/2019/08/henry-kissinger-the-metamorphosis-ai/592771/

Science and Technology Policy Office. (2016, June 27). Request for Information on Artificial Intelligence. Retrieved April 8, 2018, from Federal Register: Daily Journal of the United States Government website:

https://www.federalregister.gov/documents/2016/06/27/2016-15082/request-for-information-on-artificial-intelligence

Segal, A. (2017). *Rebuilding Trust Between Silicon Valley and Washington*. Retrieved from Council on Foreign Relations website: https://www.cfr.org/report/rebuilding-trust-between-silicon-valley-and-washington

Shane, S., & Wakabayashi, D. (2018, April 4). "The Business of War": Google employees Protest Work for the Pentagon. *The New York Times Magazine*. Retrieved from https://www.nytimes.com/2018/04/04/technology/google-letter-ceo-pentagon-project.html

Shead, S. (2018, May 3). Facebook Reportedly Has A Dedicated AI Ethics Team. *Forbes*. Retrieved from https://www.forbes.com/sites/samshead/2018/05/03/facebook-reportedly-has-a-dedicated-ai-ethics-team/

Shoham, Y., Perrault, R., Brynjolfsson, E., Clark, J., Manyika, J., Carlos Niebles, J., … Bauer, Z. (2018). *The AI Index 2018 Annual Report*. Stanford, CA: AI Index Steering Committee, Human-Centered AI Initiative.

Statt, N. (2018, November 8). Amazon told employees it would continue to sell facial recognition software to law enforcement. *The Verge*. Retrieved from https://www.theverge.com/2018/11/8/18077292/amazon-rekognition-jeff-bezos-andrew-jassy-facial-recognition-ice-rights-violations

Suchman, L. (1984). DARPA Strategic Computing Initiative: A progress report on the CPSR response. Retrieved from The Computer Professinoals for Social Responsibility Newsletter website: http://cpsr.org/prevsite/publications/newsletters/old/1980s/Spring1984.txt/

The Economist. (2018, May 29). Why Uber's self-driving car killed a pedestrian. *The Economist*. Retrieved from https://www.economist.com/the-economist-explains/2018/05/29/why-ubers-self-driving-car-killed-a-pedestrian

The Seattle Times. (2018, June 19). Microsoft employees protest company's work with ICE. *The Seattle Times*. Retrieved from https://www.seattletimes.com/business/microsoft-employees-protest-companys-work-with-ice/

The United States Government. (2017). *National Security Strategy of the United States of America*. Retrieved from The White House website: https://partner-mco-archive.s3.amazonaws.com/client_files/1513628003.pdf

The White House. (2018, May 10). *Artificial Intelligence for the American People*. Retrieved from https://www.whitehouse.gov/briefings-statements/artificial-intelligence-american-people/

The White House. *Executive Order on Maintaining American Leadership in Artificial Intelligence*. , (2019).

Thomson, J. (2018, July 29). Are Amazon, Alphabet too big to regulate? *Australian Financial Review*. Retrieved from https://www.afr.com/chanticleer/tech-giant-numbers-amazon-alphabet-revenue-jump-revives-competition-debate-20180726-h13775

Trajtenberg, M. (2018). AI as the Next GPT: A Political-Economy Perspective. In A. K. Agrawal, J. Gans, & A. Goldfarb (Eds.), *The Economics of Artificial Intelligence: An Agenda*. Retrieved from https://www.nber.org/chapters/c14025

Turing, A. M. (1950). Computing machinery and intelligence. *Mind*, *59*(236), 433.

United States Government. (2018). *United States Government Budget FY2019: Research and Development*. Retrieved from The White House website: https://www.whitehouse.gov/wp-content/uploads/2018/02/ap_18_research-fy2019.pdf

U.S. Congress. *Defense Authorization Act.* , Pub. L. No. 91–121 (1969).

Varian, H. (2018). Artificial Intelligence, Economics, and Industrial Organization. In A. K. Agrawal, J. Gans, & A. Goldfarb (Eds.), *The Economics of Artificial Intelligence: An Agenda*. Retrieved from https://www.nber.org/chapters/c14017

Walker, K. (2018, December 18). Google AI Principles updates, six months in. Retrieved April 5, 2019, from Google Blog: The Keyword website: https://www.blog.google/technology/ai/google-ai-principles-updates-six-months/

Weise, E. (2017, November 1). Russian fake accounts showed posts to 126 million Facebook users. *USA TODAY*. Retrieved from https://www.usatoday.com/story/tech/2017/10/30/russian-fake-accounts-showed-posts-126-million-facebook-users/815342001/

Work, R. (2017, April 26). *Establishment of an Algorithmic Warfare Cross-Functional Team (Project Maven)*. Retrieved from http://dodcio.defense.gov/Portals/0/Documents/Project%20Maven%20DSD%20Memo%2020170425.pdf

Wu, T. (2018, November 13). How Google and Amazon Got So Big Without Being Regulated. *Wired*. Retrieved from https://www.wired.com/story/book-excerpt-curse-of-bigness/

Xiong, W., Droppo, J., Huang, X., Seide, F., Seltzer, M., Stolcke, A., … Zweig, G. (2016). Achieving Human Parity in Conversational Speech Recognition. *ArXiv:1610.05256 [Cs, Eess]*. Retrieved from http://arxiv.org/abs/1610.05256

Zhang, S. (2017, February 16). China's Artificial-Intelligence Boom. *The Atlantic*. Retrieved from https://www.theatlantic.com/technology/archive/2017/02/china-artificial-intelligence/516615/

Zilis, S. (2016). The Current State of Machine Intelligence 3.0. Retrieved from Shivon Zilis website: http://www.shivonzilis.com//machineintelligence

Zwetsloot, R., Toner, H., & Ding, J. (2018, November 20). Beyond the AI Arms Race. *Foreign Affairs*. Retrieved from https://www.foreignaffairs.com/reviews/review-essay/2018-11-16/beyond-ai-arms-race