Explaining US Cybersecurity Policy Integration Through a National Regime Lens

A Thesis Presented to The Academic Faculty

By

Karim Farhat

In Partial Fulfillment of the Requirements for the Degree Doctor of Philosophy in Public Policy
School of Public Policy

Georgia Institute of Technology

December 2021

Explaining US Cybersecurity Policy Integration Through a National Regime Lens

Approved by:

Dr. Milton Mueller
School of Public Policy
Georgia Institute of Technology

Dr. Nadiya Kostyuk
School of Public Policy
Georgia Institute of Technology

Dr. Juan Rogers
School of Public Policy
Georgia Institute of Technology

Dr. James Lewis
Senior Vice President and Director,
Strategic Technologies Program
Center for Strategic and International Studies

Dr. Margaret Kosal
Sam Nunn School of International Affairs
Georgia Institute of Technology

Date Approved: December 10th, 2021

ACKNOWLEDGMENTS

Friends and family for their unwavering support: Linda Nhon, Elias & May Farhat, Sarah Farhat, Nathan Ochole, Sarah & Kshitij Sachar, Usayd Casewit, Elie René El Khoury.

Academics and scholars on whose shoulders I stand: Drs. Milton L. Mueller, Juan D. Rogers, Margaret Kosal, Nadiya Kostyuk, James Lewis, Richard Simmons, John Lindsay, Karl Grindal, and Jordan B. Peterson.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

SUMMARY

This research uses the Policy Regime Framework to analyze which of two policy problems, US-China rivalry or IT/OT convergence, better explain degrees of coherence and integration in the US cybersecurity regime. It explains how regime actors address and negotiate these problems across the ICT and energy sectors. A process-tracing methodology was used to track outcomes and explanatory factors, linking causal mechanisms through an analysis of the Congressional record and in-depth stakeholder interviews. The results indicate how the idea of Chinese ICTs as a Trojan horse for the Chinese Community Party's strategy was more effective than IT/OT convergence at mobilizing interests and advancing coherent cybersecurity policy. Trade and ICT policies were successfully integrated to achieve cybersecurity goals as regime interests bargained to 'weaponize' critical trade interdependencies through the US competitive advantage in the semiconductor industry. This research lends further validity to the Policy Regime Framework in researching cross-sector-spanning policy problems in the ICT space especially given recent calls for whole-of-government approaches to address emerging strategic technologies.

INTRODUCTION

This research aims to test which of two policy problems better explains degrees of coherence and integration in a policy regime. The United States (US) cybersecurity regime was selected as a case study and functionally defined by the actions of its executive and legislative branches of government in the ICT and energy sectors. The analysis aims to evaluate whether one policy problem, i.e., US-China geopolitical rivalry, generates more regime coherence and integration than the problem of IT/OT convergence, drawing on concepts of regimes coherence and integration as theorized by the Policy Regime Framework (PRF).

Scholars have formulated the PRF and advocated its suitability for policy problems encompassing more than one policymaking arena at the sub-national level (Jochim and May, 2010). The cross-cutting nature of ICT-based policy problems motivated using this theoretical framework to help answer the research question. This dissertation will primarily consist of an application of the PRF with minor modifications. It evaluates which of the two policy problems is better at focusing government action across different policy-making arenas.

A process-tracing methodology is used to track outcomes and explanatory factors by linking the causal mechanisms involved. This tracing technique outlines the sequence of cause-effect processes in a narrative (the trace), then works backward by connecting how an outcome that has occurred may have been caused by mechanisms hypothesized by theory (the process) following a Bayesian logic of inference whereby events of a low likelihood are assigned more weight in validating outcomes.

In the upcoming sections, US geopolitical rivalry with China and cyber-physical systems' convergence are presented as policy problems whose governance arrangements foster varying degrees of integrated action across different policy arenas. After presenting the problems, the outline will detail:

1. A research question for empirical testing
2. The suitability of PRF to scope and analyze the research question given the frameworks' established components and definitions
3. A theoretically grounded methodology for addressing the question, including detailed operationalization of explanatory factors
4. A sequence of chapters organized around analyzing the impact of the explanatory factors on regime outcomes and a synthesis of findings to answer the research question
5. Finally, the conclusion section provides a normative assessment of the findings' implications, including a discussion on the validity of the framework's causal theory of change and its usefulness in future ICT policy research

1.1 Background and Research Question

Nation-states are mutable and adapt their sovereignties to technological, economic, and social changes caused by ICTs. In the transnational arena, public authorities often regard cyberspace as an extension of their states' capacity to regulate the flow of information, goods, and capital across their borders (Krasner, 1999).[1] The last decade produced a distinct change in the thought and practice of broadly defined Internet governance (IG). The Snowden revelations perpetuated an overall decline in international trust following a

[1] What Krasner refers to as "interdependence sovereignty".

sharp increase in a trend known as the securitization of cyberspace, whereby traditionally nonmilitary issues are politicized and seep into the military's purview in various policy arenas (Buzan et al., 1998; Dunn Cavelty, 2013, 2007).

Governments increasingly conceptualized cyberspace in state-based terms despite the extra-territorial nature of computer network communications (Mueller, 2019). Some feared the rising trend of 'data nationalism' would eventually lead to internet balkanization (Hill, 2012). The overall decline in trust and the militarization of cyberspace resulted from a two-pronged combination of legitimate security concerns. One was the increased technological interconnectivity and interdependence of Critical Infrastructure (CI), the other a resurgence of global geopolitical competition and power politics among world superpowers (Healey, 2013; Mattis, 2018). The alignment of domestic US interests in this environment spawned lucrative enterprises as concerns about cybersecurity and national security continued to converge (Aggarwal and Reddie, 2018). Complex, multifaceted cyber dynamics resulted in an interdisciplinary approach to cybersecurity research and a contentious lexicon of terminology. While cross-domain escalation dynamics and cyber conflict remained mostly speculative, ideas like "cyber deterrence" dominated the military discourse (Libicki, 2009). International relations and political science drew analogies from conventional conflict to spawn the burgeoning subfield of cyber conflict studies with notions such as the "cybersecurity dilemma," "hybrid warfare and the gray zone," or "persistent engagement [in cyberspace]" (Buchanan, 2017; Fischerkeller and Harknett, 2019a, 2019b, 2018; Harold et al., 2017). Cyber conflict research focused on theory-building rather than testing with a scarcity of reliable data and viable metrics (Gorwa and Smeets, 2019). As the field struggles to align

theorized dynamics with empirical reality, policymakers are invariably driven by how cyberspace dynamics are represented and intersect with foreign policy and geopolitical rivalry (Dunn Cavelty, 2013; Mueller and Badiei, 2019).

The broader field of public policy has failed to consider how cross-cutting policy problems can encompass more than one set of policy-making and implementing apparatuses. Mainstream theories of public policy, such as the Advocacy Coalition Framework (ACF), Multiple Streams Framework (MSF), or Institutional Analysis and Development (IAD), tend to focus on a single policy domain and neglect cross-cutting problems. Cybersecurity, however, involves multiple policy domains, such as organizational information management, digital trade, or electric grid security. Policymakers and policy entrepreneurs in the national security space often propose policy solutions that bridge different policy domains, as evidenced by the Homeland Security (HS) regime.

PRF is a relatively new and under-theorized framework for policy analysis that shows promise for studying politics-policy feedback at a system level (instead of studying specific policy arenas and subsystems). By distinguishing the impact of either policy problem on their respective sectors, e.g., ICTs and trade policy, and studying how policy problems diffuse throughout the USG, we can find out which problem is more effective at fostering coherence and integration in a complex policy regime. This analysis also aims to understand better how threat-politics affect policy implementation and contribute to the growing literature using the regime lens at a national level.

1.2 Problem selection

IT/OT convergence and the threat of China have both generated ideas for cybersecurity legislation. One may, however, see the two as an arbitrary juxtaposition of non-equivalent problems. However, because of the qualitative differences between those two problems, differentiated theories can emerge as valid categories of explanation. The rise of China is a foreign policy threat to the US government in a context of great power competition. IT/OT convergence, on the other hand, is a system-level problem determined by networking architecture. This section explains why the comparative analysis of these two problems makes for valid empirical investigation.

The late Obama and early Trump administrations shifted the international relations paradigm to great power competition (Cheung, 2020). Russia is a valid explanatory factor when considering foreign policy threats, given its threat to US hegemony, particularly in cyberspace. Competition with Russia has involved a broad gamut of strategic situations in which the Russians apply cyber power for disruption (in the US) or coercion (abroad).[2] More lately, Russia's 2016 Information Operations and the SolarWinds hack were watershed moments forcing the reevaluation of the US cybersecurity regime into the foreseeable future.

China was selected rather than Russia for two reasons. First, many of the anomalous IT policies of the last five years at the time of writing appeared at face value as motivated by China and the intersection of trade and IT policy. The economic entanglement between

[2] Russian Offensive Cyber Operations (OCOs) include Information Operations (InfoOps) in various countries, cyber-physical attacks in Ukraine or combining denial of Service attacks with diplomatic pressure (CISA, 2021).

the US and China in goods and services trade was significant enough to justify a new Congressional institution after China's ascension to the WTO.[3] On the other hand, Russia's trade volume and its political-economic entanglement with the US are negligible.[4] While nationalism and trade protectionism could be regarded as short-lived staples of the Trump administration motivating rapid policy change, deep concerns about political-economic competition with China predates the Trump administration and has continued beyond it. The digital-mercantilism characterizing US-China relations involves political-economic dynamics unique to China (Mueller and Farhat, 2022).[5]

However, the causal mechanisms at play in the case of China remain unclear. If the expulsion of Kaspersky from US government networks was intended to bolster defenses to a specific cyber threat, then why did this trend expand to affect commerce, IT trade and involve multiple government agencies in the process (Kuerbis, 2018)? Further, Chinese Offensive Cyber Operations (OCO) have almost exclusively focused on commercial, industrial, and state-based espionage, a narrower, more specific range of activities than Russian cyber forays targeting US elections and Critical Infrastructure (CI). Therefore, the choice of China is at best revelatory of other underlying trade and strategic dynamics or, at worst, a conservative and tractable choice for analysis.

As for IT/OT convergence, Schweitzer Engineering Labs introduced microprocessor-based digital relays in the 1980s (Farhat and Mueller, 2020). Today, however, every

---

[3] The US-China Economic and Security Review Commission is central to this work.

[4] According to the USTR, the volume of trade in services with Russia amounts to a combined import-export value of $6.9 billion compared to a much more significant $76.7 billion with China.

[5] US diplomatic pressure on Russia follows a sanctions model instead. Digital-mercantilism is defined in chapter 7.

industry involves digitized infrastructures in which software is used to control hardware. This ongoing transformation in socio-technical systems creates new security risks in U.S. CI. The interdependency of infrastructure sectors and the regulatory silos erected to manage them after the Homeland Security Act of 2002 are actively debated. Public risks can be deemed partly socially constructed and partly determined by technology (as well as other things). Therefore, the intersection of technology risk with foreign threats presents novel categories of investigation.

Beyond the categorical pairing of both problems, alternative explanations could conceivably involve entrenched political interests and bureaucratic competition in the CI and Homeland Security space. For example, bureaucratic competition could have a confounding, mediating, or exacerbating effect on either policy problem (Morgan and Winship, 2015). However, since policy problems and solutions typically precede the organizational interests set up to address them, the effect of organizational interest will be included in the ideas put forward in their defense. The presence of agency competition implies that a policy idea's effect was insufficient to overcome those competitive forces. Another explanatory category involves partisan interests. It may be the case that the political party in power could explain the cybersecurity regime's trajectory. However, as this analysis will show, exogenous partisan politics did not sufficiently explain cybersecurity policy, which further reinforces the validity of this problem framing. By exploring differences in both problems' ability to impact the cybersecurity regime, disparate drivers of regime change can be better defined and isolated.

1.3 U.S. geopolitical rivalry with China

The US geostrategic environment has historically favored a strategy of primacy. After WW2, the US projected its power through forward-stationed forces, leveraging allies to maintain a favorable power balance in key regions, and spreading capital under US terms of neoliberal political economy (DoS, 2017; Porter, 2018; Turpin, 2020). After the fall of Communism, economic prosperity strengthened US hegemony and was thought to have relegated Marxism-Leninism to vestiges of a bygone era (Fukuyama, 1989). The coupling of transnational corporate interests and domestic politics tied US well-being and prosperity domestically to stability and productivity abroad. With free-flowing capital tied to American values of freedom and openness, mutually reinforcing pillars of neoliberalism formed the US basis for international relations and supported the edifice of a long-term strategy.

At the turn of the millennium, US-China relations were headed towards complete economic entanglement. A bipartisan consensus in Washington DC considered trading with China while boosting their economy as morally justified and serving long-term US interests.[6] Despite a few relationship mishaps along the way, the dominant paradigm in Washington was that China's embrace of market forces would pave the way for its political liberalization, following a reform path like South Korea (Blustein, 2019). The Clinton administration normalized trade relations with China's ascension to the World

[6] National Security Decision Directive (NSDD) 11, signed by President Reagan in 1981, went as far as permitting the Pentagon to sell advanced air, ground, naval, and missile technology to the PLA. NSDD 12 the following year brought about a cooperative program to expand China's military and civilian nuclear programs.

Trade Organization (WTO) (Lipton, 2018). However, as early as 2003, political and economic forces within the US began to question its economic relations with China.[7]

During this so-called "lost decade," DC's sanguine aspirations that China would converge were progressively thwarted as the CCP grasped economic buildup while keeping leftist elements in power to protect from liberal influences (Johnson, 2012). The paradox of a robust market economy governed by an authoritarian one-party state confronted Washington's narrative. On the geo-strategic front, Chinese forays in the South China sea became increasingly abnormal and threatened the US Navy's freedom to navigate. Secretary of State Clinton followed by signaling a US foreign policy shift to South East-Asia in 2011 (Clinton, 2011). Pacific Command (PACOM) extended its posture in Asia-Pacific with fleet deployments combined with a reaffirmation of mutual-defense pacts with regional allies.

The Eighteenth National Congress of the Chinese Communist Party (CCP) in November 2012 brought about a drastic change in leadership as Xi Jinping consolidated state power over the public sphere (Malesky et al., 2017). With Xi's inauguration, the PRC hardened its commitment to a repressive one-party rule and a state-directed economy aiming for competitive technological capabilities and greater self-reliance (Tai Ming, 2020). Xi's tenure also brought more state influence over the private sector, focusing on "civil-military integrated systems" as a top national priority (Ibid).[8] The Made In China (MIC)

[7] It was around that time that the US government claimed China engaged in currency manipulation to favor their export markets later argued to have caused the American manufacturing death spiral (Paulson, 2015).

[8] That said, it should be noted that military-civil fusion is not part of the CCP's unified grand strategy. Instead, MCF principles rest on a series of edicts and multi-year plans dating from 2005 that are designed to facilitate dual-use technology transfers through public contracts not unlike the US DIB. The first explicit

2025 policy rattled the US and European Chambers of Commerce, which started lobbying political leaders for more robust competition measures and a need to exert more pressure on Beijing.[9] Developed economies were concerned that China would treat high-end manufacturing with the mercantile trade practices they spent the last two decades applying to low-end manufacturing. The late Obama and early Trump administrations ushered a new international relations paradigm and a significant shift in US foreign policy with China.[10] Competition with China (as opposed to cooperation) is unarguably one of the dominant threat frames defining US foreign and domestic politics today (Lippert et al., 2020; Mattis, 2018). The dominant bipartisan narrative put forward by Washington assumes global US supremacy, and China has been the strongest challenger to that dominance since the collapse of the Soviet Union. According to the International Monetary Fund, using purchasing power parity valuation of country growth domestic product as an indicator, the Chinese economy's size overtook the US in 2014 (IMF, 2014). The fear that China competes directly and even surpasses the US in areas of strategic competition is well-founded: China is in a constant tug of war with the US in supercomputing and surpassed the US in Research and Development (R&D) spending and STEM education (Allison, 2017; Strohmaier and Dongarra, 2019). When it comes to

---

reference of MCF was during Hu Jintao's report to the 17th Party Congress in 2007 (CSIS, 2019). MCF notions were later set as part of Xi Jinping's national strategy in 2014 that aims to coordinate economic planning with national security (Section 301). As discussed in chapter 7 and by the CCP's own admittance, many these MCF programs have failed to bring about the anticipated public-private force multipliyer.

[9] A continuation of the 2005 *National Medium- and Long-Term Science and Technology Development Plan (MLP) for 2006-2020.*

[10] Future research would be well served to address which focusing event or combination thereof most contributed to this shift on the global stage. Notable events around the time include Xi Jing Ping's accession and consolidation of state power with the Eighteenth National Congress of the Chinese Communist Party (CCP) in November 2012, the Snowden revelations in 2013, the invasion of Crimea 2014, ongoing incursion in the South China Sea, and many others.

military dominance, a 2015 RAND study projected that China would have an advantage or "approximate parity" in six out of nine areas of conventional military capabilities by 2017 (Heginbotham, 2015).

Over the last two decades, US-China relations appear to follow a path combining the Thucydides Trap and the security dilemma (Allison, 2017; Glaser, 1997). In the former concept, a rising power makes a dominant hegemon fearful for its position as tensions escalate, risking the spark of war. In the latter, neither side is aware of the threat perception they produce, one nation regarding its securitization efforts as peaceful while interpreting the other's defensive posture as offensive, thereby inciting instability. However, the military-strategic dimension of the competition is not the whole story.

Both nations' economic interdependence and the security externalities of IT trade further complicate their respective foreign policies. World powers leverage trade measures such as export controls, tariffs, investment restrictions, and data localization requirements as tools to address cybersecurity policy problems (Grindal, 2019). Balancing the tightrope of preserving national security while maintaining openness in trade is a challenge every administration faces.

As the finer points of great power competition strategy debate were stymied by internal polarization and the seesaw of partisan administrations, it became clear that IT trade protectionism was not a short-lived staple of the Trump administration. Instead, it is part of a zero-sum political-economic logic pursued in Washington and Beijing. As a result, US-China economic interdependence was brought into question amid more restrictive US trade policies (Aggarwal and Reddie, 2020; Daugirdas and Mortenson, 2017).

At the same time, distrust of China has intruded into telecommunications policy. For example, the inter-agency working group "Team Telecom" blocked Google and Facebook from setting up the first direct submarine Internet cables from Hong Kong to the US on national security grounds due to partial ownership by Chinese firms (DoJ, 2020). The controversy around the global Chinese telecommunications firm Huawei presents a unique case study of how cybersecurity considerations intersect with trade. A long-term organized campaign of cross-cutting policy action from the US government has sought to restrict the Chinese Telecommunications equipment manufacturer Huawei from accessing global supply chains. Examples of recent policy action include export controls on semiconductor manufacturers and listing Huawei on the Bureau of Industry and Security's Entity List, which denies global telecommunications and software markets from transacting with Huawei under threat of exclusion from US technology and software supply chains (BIS, 2020; SIA, 2021). Export restrictions on semiconductor manufacturers have raised concerns among the semiconductor industry lobby and the DoD, which is concerned with American competitiveness in dual-use technologies critical for strategic competition (Davis, 2020). In other policy areas, the Federal Communications Commission (FCC) made domestic firms using Chinese equipment ineligible for Universal Service Fund (USF) subsidies (FCC, 2020). This withdrawal was an unprecedented move by an independent regulatory agency intervening due to national security concerns.

Washington and Beijing maintained ICTs and, to a lesser extent, high technology areas like quantum computing as a battleground for strategic competition. However, leadership in such strategic technologies was not defined in terms of a favorable trade posture or

innovation goals on the US side. Instead, it was stymied by a politically expedient hodgepodge of vaguely defined objectives such as 'winning the 5G race' (Brake and Bruer, 2020, p. 5). As the world accelerates towards a US-China bipolar world order, whether China's threat successfully unifies cybersecurity policy action across different policy-making arenas becomes increasingly salient.

1.4 IT/OT convergence

Powered by Moore's law and new developments in data management and algorithmic scalability, previously disparate Operations Technologies (OT) are becoming unified or internetworked with Information Technologies (IT). This phenomenon has become known as IT/OT convergence.

The convergence process is primarily driven by the need for increased economic efficiency, especially as isolated systems cannot scale in a manner commensurate with the service economy. The increasing efficiency with which energy and raw materials are converted into valuable work — while nothing short of revolutionary — has significant implications for many industries (Farhat and Mueller, 2020). These advancements provide private firms — many of which operate CI — with new process optimization capabilities powered by big data. Some have argued these profound changes to be part of an ongoing industrial paradigm shift referred to as the fourth industrial revolution (Schwab, 2017).

Terms such as the industrial internet imply a convergence between Information Technology (IT) and Operations Technology (OT), as cyberspace intersects physical

space across all sectors of the economy.[11] NIST refers to the electric grid as a "multi-layered cyber-physical system of systems," a term more common in the federal government (SGIP, 2010). Congressional representatives often refer to 'massive digitization and interconnection' that are 'layered onto existing practices and energy infrastructures.' These terms and notions all refer to the same phenomenon. Other terms such as the 'industrial internet,' 'industry 4.0,' or 'the Internet of Things' are similar but imbued with various industrial contexts grounded in the business management and organization literature. They are outside the purview of this research.

US CI is at the heart of an ongoing socio-technical transformation and is subject to potential increased security risks. While public risks are socially constructed and partly determined by technology, critical infrastructure protection (CIP) clashes the old analog world with the new digital space (May and Koski, 2013). The interdependency of infrastructure sectors and the obsolete regulatory silos erected to manage them after the Homeland Security Act of 2002 are the subjects of ongoing institutional and organizational restrictions as outlined in section 5.3 and chapter 8.

The use of IP as the unifying communication medium for modern society is such that "threats that work against IP networks spread to all converged networks, including factory control networks, banks, and transportation" (Lewis, 2019). Cyber-physical convergence is arguably most apparent in the energy sector, especially after microprocessor-based digital relays replaced analog switches in the 1980s (Haas and M, 2019). These relays converge systems by unifying once disparate physical control points

[11] The term IT/OT convergence is considered equivalent to cyber-physical systems' convergence, coined by the National Institute of Standards and Technology (NIST).

into a single hardware apparatus, often leveraged at the level of a Supervisory Control and Data Acquisition (SCADA) control center. Cyber-physical convergence is further accelerating today as SCADA communication shifts from legacy, serial-based protocols to digital standards leveraging the interoperable Internet Protocol (IP) (among many other standards), notably with the increased use of Intelligent Electronic Devices (IEDs) (Thomas and McDonald, 2017). In 2015, the US Department of Energy (DoE) stated that: "The popular transition to smart, data-driven technologies (...) has been introduced at an unprecedented rate relative to the history of the industry, and injects uncertainty into grid operations, traditional regulatory structures, and utility business models" (Clark et al., 2015). This ongoing transition in the energy sector is often referred to by the all-encompassing term, the smart grid.[12] In the IT sector, convergence is apparent through the potential of 5G mobile telecommunications to facilitate consumer and industrial Internet of Things (IoT) applications.[13]

Technologists have long considered convergence as a double-edged sword. On the one hand, it can maximize efficiency; on the other, it increases the number of possible attack vectors and furthers infrastructure interdependence (NIST, 2014). The convergence of technological systems presents risk *sui generis*, distinct from CI systems' interdependence; however, it can compound the latter's effect by expanding the potential

[12] The National Institute of Standards and Technology (NIST) defines the smart grid as a hybridized cyber-physical system combining "computer-based communication, control, and command with physical equipment to yield improved performance, reliability, resilience, and user and producer awareness" (NIST, 2014).

[13] For manufacturing and industrial applications technologists refer to an industrial internet of things (iIoT).

attack vectors (Lewis, 2019). [14] For instance, convergence opens the theoretical possibility for hackers to leverage edge network weaknesses to compromise driverless cars or crash airplanes into buildings remotely.

In addition to presenting a public risk to CI, convergence is also a cross-sector policy problem that complicates the allocation of responsibility and demarcation of property rights and resources. Policy tools intended to regulate public risk involve two broad approaches ranging from mandatory to noncoercive (May and Koski, 2013).[15] Despite their qualitative difference, both policy problems can be considered from a regime lens perspective, i.e., negotiated within and across policymaking areas. Their distinctive effects are qualitatively comparable and can be isolated despite potential interaction effects, which are analyzed accordingly. After stating the research question, a case will be made for why PRF is well suited to address policy questions spanning different policy arenas and government levels.

1.5 Research question

Two policy problems were identified as directly relevant to a conceptualized cybersecurity regime: IT/OT convergence and the threat of China.

This juxtaposition raises the question, *which of these two policy problems can better determine the degree of the cybersecurity regime's coherence and integration? Further,*

[14] The inherent interdependence of infrastructure systems implies the risk capacity for small events to achieve cascading effects of varying specificity in cyber and non-cyber dependent systems alike. These risks were formally recognized during the Clinton administration.

[15] The nuclear infrastructure is mandated for protective actions through direct regulation. The energy sector more broadly is subject to CI Protection regulations are currently administered by the North American Electric Reliability Corporation (NERC).

how are these two policy problems addressed and negotiated among regime actors across the ICT and energy sectors?

According to the PRF, either policy problem could be a more successful driver because of a specific interaction of policy ideas, interests, and institutions (the explanatory factors). By distinguishing the impact of either policy problem on their respective policy areas, we can uncover the underlying boundary-spanning dynamics and determine which problem can foster regime coherence and integration more effectively. Such framing of a research question will contribute to PRF theory-building by clarifying the explanatory factors' interaction potential, especially in their ability to impede or further regime outcomes.

Given the resurgence in regime perspectives in policy analysis, including their application in ICT policy research, this work applies the PRF with minor adjustments. This analysis could also set the foundation for answering other questions related to the viability of PRF as part of a more extensive research program in the future. The following section will explain the suitability of a Policy Regime Framework (PRF) for addressing these policy problems. It will also discuss the utility of adopting a sub-national level of analysis and how regime boundaries are practically defined.

CHAPTER 2.
A POLICY REGIME FRAMEWORK TO EXPLAIN NATIONAL CYBERSECURITY GOVERNANCE

2.1 From transnational to subnational policy regimes

The regime perspective has provided explanations for high-level governance arrangements starting with international regimes in the 1970s. Regimes were how institutionalist International Relations (IR) scholars referred to organized international institutions in the 1980s (Keohane, 1982).[1] IR scholars have used regime theory to analyze transnational telecommunications policy going back to the heyday of the ITU regime (Cowhey, 1990). Political scientists have also sought to integrate domestic politics models into international regimes and vice versa (Martin and Simmons, 1998; May and Jochim, 2013). The choice of the level of analysis is a divide that dates to the 1980s when regime theory focused on international cooperation, and scholars sought to integrate models of domestic politics into international regimes.

Klimburg (2012) provides a comparative analysis of national cybersecurity policies in the EU that can be conceived as separate national-level cybersecurity regimes (Klimburg and NATO Cooperative Cyber Defence Centre of Excellence, 2012). Sivan-Sevilla (2019) uses the policy regime lens to study broader cybersecurity governance arrangements in the EU but also addresses the "US policy regime (Sivan-Sevilla, 2019)." By studying the

[1] Realist scholars that adopt an anarchic worldview portray strong states with common or conflicting interests as the *de facto* enforcers of rules. While acknowledging the lack of a supranational basis for governments to police one another, institutionalist scholars explain formal state cooperation according to joint distributions of interests among international institutions.

dynamic of historical institutional arrangements, shared ideas, and interest groups' influence, he explained how the politics of the policy process could yield additional security and privacy outcomes in the US.

This analysis uses the regime lens to study cybersecurity policy at the national level, as formulated by May and Jochim (2013). A conception of a national regime is helpful to consider relations among different coordinated government institutions at a meta-constitutional level of governance where stakeholders are "in the process of constituting or reconstituting ongoing relationships" (Ostrom, 2005). For example, the 'Team Telecom' group mentioned earlier can be considered a meta-constitutional precursor to a national cybersecurity regime as it initially involved *ad hoc* coordinating arrangements among federal agencies (FCC, DoJ, DHS, and others) with no formally defined procedure for deliberation and review until the Trump administration formalized it under EO 13913 on April 4, 2020.

A regime's *raison d'etre* is determined by defining and framing the policy problems that span its relevant sectors' boundaries. While policy scholars typically start their conceptual analysis with a policy measure, the PRF starts with a policy problem.[2] More specifically, the PRF is concerned with dispersed problems that lack comprehensive governing arrangements to address them. Many societal problems, such as supply chain security, citizen privacy, or cybersecurity, give rise to various governance arrangements that could be unified under the banner of a policy regime. PRF weaves a common thread across different policy areas as complex problems nest and interlink across different policy

[2] Policy problems are defined in Table 1 as *articulated gaps between a current and desired end-state that embeds cause and effect elements that render it meaningful*.

sectors. Faced with complex and often sector-spanning problems, governments design or modify institutions specifying governance mechanisms to address them. Once established or modified, institutions act as formal rules that reveal constituent preferences while constraining allowable actions even as they evolve and are remolded by the state (Martin & Simmons, 1998). Therefore, policy regimes are considered a collection of governance and institutional mechanisms that foster integrative actions across elements of multiple government agencies (Jochim and May, 2010).

In this thesis, the backward mapping of governing arrangements for both policy problems under consideration is achieved by considering the well-documented interplay of ideas, interest, and institutional arrangements (Goldstein, 1993; Goldstein and Keohane, 1993). These governing arrangements are identified within the policy areas that make up the confines of the cybersecurity regime, as later specified.

2.2 Unit of analysis

Policy studies have traditionally considered subsystems as fundamental ontological units of analysis for understanding and analyzing policy processes. The notion of a subsystem is derived from the Advocacy and Coalition Framework (ACF) formulated to deal with "wicked" problems involving substantial goal conflicts and actors from several levels of government (Sabatier, 2007). The authors of ACF consider subsystems as semi-independent, overlapping, and interacting institutional boundaries with potential for authority that, to the extent relevant, include actor attributes, belief systems, and political resources (Sabatier and Weible, 2014).

The PRF similarly considers policy problems that span multiple areas of policymaking to be first interpreted by specific subsystems (Jochim and May, 2010). Subsystems then

shape problem definitions and policy responses, befitting their substructures, historical approaches, and the various interest communities they involve. For example, the proliferation of IoT devices entails a substantively different policy problem depending on the actors and sectors involved. While private sector actors may be concerned with behind-the-meter IoT devices' reliability and privacy-preserving ability, the CI community is concerned with foreign entities leveraging outdated and unsupported tech gadgets to crash planes into buildings or shut parts of the power grid down. The value of a conceptual unit of analysis such as subsystems is in the descriptive and analytical clarity it is supposed to provide. In this example, including any other technology-related problems such as cybersecurity, the ontology of a subsystem is undermined by indeterminate boundaries and the preponderance of private sector action. Which of the ICT, energy, or CI subsystems would be involved in addressing the convergence problem? How can subsystems be functionally defined? Similarly, the Chinese threat's broadness as a policy problem represents an overlap of disparate areas such as economic competition, industrial policy, ICT trade policy, and even human rights.

Subsystems in traditional policy scholarship are too abstract and loosely bound to be useful for this analysis, where a cybersecurity regime forms the locus of all relevant and intersecting policy problems. Therefore, this analysis follows the more definite sector-based demarcation set by the original Presidential Decision Directive 63 (PDD-63) in delimiting the policy sectors under consideration, i.e., Communications, Information Technology, and Energy. While these sectors differ in their capability to absorb or transfer problem demands to each other, they are individually considered as part of the

original institutional structure demarcating CI.[3] As the analysis will detail, the IT sector is increasingly encroaching upon the energy sector as part of IT/OT convergence. At the same time, the threat of China started in the ICT sector but was able to mobilize diverse political stakeholders in a whole-of-government response due to its higher boundary-spanning capability as a policy idea.

2.3 The dynamics of policy problems in regime sectors

The notion of a policy regime that integrates policy action among different sectors can vary along a spectrum. As policymakers seek similar or disparate goals, governance arrangements of varying coherence and integration will coalesce around their agendas. Robust regimes set government agencies on a convergent trajectory as they foster cohesion and integration among policy sectors by reinforcing shared purpose and mobilizing efforts of key participants to support a common goal (Cejudo and Michel, 2017; May and Jochim, 2013). Sustainable and robust regimes tie boundary-spanning problems to governance arrangements that foster high levels of policy integration, as interest groups seek similar goals. Unlike other theories of the policy process, PRF addresses the extent to which "spillovers translate into viable policy regimes once the urgency of crises fade [sic] and coalitions concerned about them fracture" (Jochim and May, 2010).

The complexity of boundary-spanning problems can also act as a disintegrative force that fragments government action. Fragmented government action has been analyzed as disjointed government (Pollitt, 2003), policy fragmentation (Koschinsky and Swanstrom,

[3] The absorption or transfer of sector goals and requirements is conceptualized as a problem's boundary-spanning capability (Jochim and May, 2010).

2001), departmentalism (Christensen and Lægreid, 2007; Kavanagh and Richards, 2001; Koschinsky and Swanstrom, 2001) and agencification (Van Thiel et al., 2012). Solutions to fragmentation are discussed as "joined-up government" or "whole-of-government." Jones and Baumgartner (2005) also highlight how information-processing capabilities in politics tend to be disproportionate, disjoint, and episodic as human and organizational limitations hinder it (Jones and Baumgartner, 2005). Selective attention implies some problems are heeded while others are ignored; after a focusing event occurs, however, it is often the case that a cross-cutting policy 'fix' becomes necessary because of the original inattention. In addition to problem complexity and information-processing limitations, the now commonplace principles of New Public Management have worsened fragmentation by favoring decentralized and specialized governance to the detriment of cohesive policy regime activity. This trend, which seeks to institute government reforms by specialized and non-overlapping roles and functions, has the trade-off of undermining horizontal coordination among implementing government agencies. A national regime approach holds the prospect of overcoming such limitations. While semantics differ, as defined in this paper, cybersecurity regimes have also been explored in-depth by scholars at the international and national levels (Dunn-Cavelty, 2009, 2013; Klimburg, 2012; Sivan-Sevilla, 2019). However, a fundamental understanding of the dynamics of boundary-spanning problems is still lacking, including how different ideational perspectives adopted by sectors on an issue can fragment implementation. This work aims to understand better how the problem and solution space behind addressing a boundary-spanning problem is manifested in the shared visions, the political dynamics of

the underlying interest communities, the institutional arrangements guiding their interaction, and how these components interact.

Table 1: Policy Regime Framework key concepts

	Definition	Attributes and examples	Relevance to the framework
Policy regime	Artificial demarcation made by a policy analyst to conceptualize the governing arrangement set up to address policy problems	Regimes can be conceived as nested, e.g., the Homeland Security and CIP regimes, or as interlinking, e.g., how the CIP regime relates to the cybersecurity regime	Regimes are the highest level of analysis in PRF. They require at least one problem-solution dyad to be meaningful.
Policy sector	A governance domain comprised of public and private actors of different interests, belief systems, and jurisdictions.	The ICT and energy sectors interact along physical and institutional boundaries and are unified by a cybersecurity regime in sharing similar policy problems. They are part of the sixteen CI sectors designated by DHS as per PPD-21.	Regime subcomponent that typically confines policy problems to the governance arrangements avail able to address them. With complex and boundary-spanning problems, a regime lens presents opportunities for analysis.
Policy entre-preneurs	Any actor that consistently advocates and contends for a specific policy idea, i.e., actors that propose solutions using consistent causal theories of change and couple it to that problem.	Coded by name, title, affiliation (committee, sub-committee, or organizational type). Entrepreneurs include testifying issue-experts (academic, business stakeholders, or federal employees) or Congressional representatives.	Indicators of interest groups in various forms. Policy entrepreneurs use ideas as organizing principles to rally support from interest groups as they provide leverage for political commitments from policymakers.

Table 1: continuation

Policy idea	A policy idea is an articulated gap between a current state and a desired end. The policy idea embeds an implicit or explicit causal pathway rendering ideas meaningful for political action and implementation (the policy solution). Policy ideas are the primary currency for debate in presenting solutions to policy problems. This work considers the policy problem-solution dyad as ontologically synonymous with a policy idea. Policy ideas can integrate action across subsystems as the implementation of policy solutions is designed to cohere.	Example 1: Chinese ICT firms are a Trojan horse of CCP grand strategy. Foreign vendors are therefore not allowed to transact in the infrastructure supply chain. Example 2: Given the interdependence of CI sectors, cyber-threat information sharing should be mandatory.	Policy ideas turn into regime ideas after monopolizing all the relevant sectors and policy areas. Powerful and shared policy ideas absent a binding institutional structure form a divergent regime. Solution ideas are eventually embodied in institutions, e.g., Homeland Security Act, Cybersecurity Information Sharing Act
Policy problem	A policy problem is an undesirable situation that an interest group can rectify via collective action.	e.g., IT/OT convergence or the rise of China	Regime problems are boundary-spanning because they are inconsistently defined, continuously re-solved, and subject to diverse value systems

CHAPTER 3. METHODOLOGY

This work sets out to uncover how two policy problems affect the cohesiveness and integration of the cybersecurity regime. A secondary goal is to assess the efficacy of that regime's policy implementation and provide a basis for making normative assertions about the policy problems' viability as a force for regime integration. Following that, explanatory factors are introduced, including selection criteria. The following section discusses how PRF was reformulated to account for theoretical shortcomings.

3.1 Shortcomings in the original PRF formulation

As shown in figure 1, May et al. proposed three primary PRF constructs that can be operationalized into different explanatory variables. They posit that legitimacy, coherence, and durability are three legs of a stool that provides a regime's "strength." Those three constructs are positively associated with a regime's strength and its associated policy-politics feedback loop. With a weak or "anemic" regime, the inertia of different subsystems undermines the coherence of policies across the regime. With a strong regime, endogenous reinforcement of political commitments realigns interests across various subsystems to support the regime through integrated policymaking. In other words, the higher the observed construct values, the stronger the regime. While May et al. present a novel conceptualization in how the politics-policy feedback mediates those three constructs, the original formulation of PRF presents two notable shortcomings.

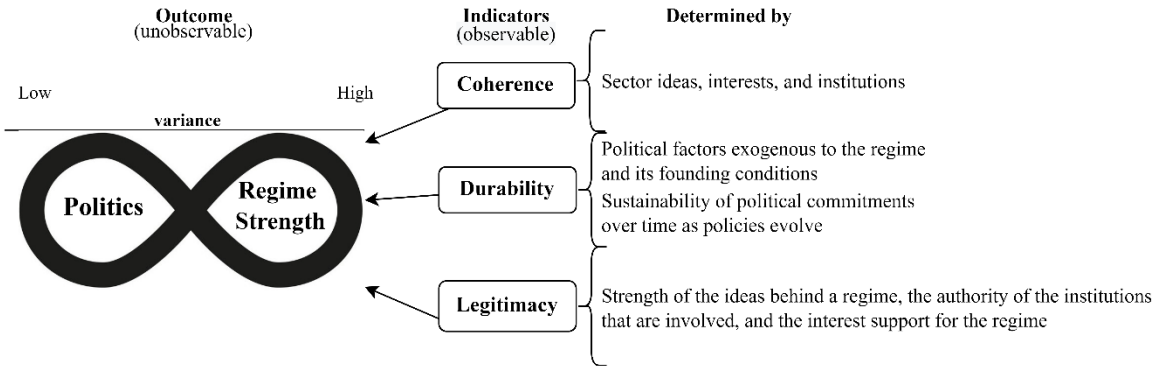


Figure 1: Original PRF formulation

First, the relationship between distinct endogenous and exogenous political effects in a regime requires more articulation—the conditions under which partisan politics and party affiliation override sector-specific interests and bureaucratic competition are not specified. Second, while relevant and useful to the conceptual understanding of policy regimes*, legitimacy and durability* must be reformulated to describe underlying causal mechanisms that will allow the operationalization of dependent and independent variables.

Given that the three central constructs are positively associated with a regime's strength, a regime can be compromised by one or more weak legs. However, 'wobbly' stools, referred to by May et al. as "anemic" regimes, are not necessarily less durable than stronger ones. While the explanatory construct of *durability* is useful in distinguishing long-lasting regimes from shorter ones, the logic of its conceptualization is brought into question by the continued existence of anemic regimes.[1] Given the paradox of weak yet durable regimes, what factors best explain how regimes evolve and accommodate given an enduring institutional structure? The durability of a policy regime is said to be "as

[1] Conversely, strong regimes can be short-lived, such as drug criminalization (Jochim and May, 2010).

much dependent on the broader political context (the exogenous political effects) as it is on the (internal) forces that shape the emergence and strength of a regime" (May and Jochim, 2013). Suppose we assume that bipartisan Congressional politics (exogenous to a regime) can further foster or impede a regime's strength, i.e., affect the strength of the political commitments and its feedback-loop to policymaking. In that case, researchers need to understand better how broader shifts in political alignments can support or undermine a regime's trajectory. Distinguishing between these effects is necessary to avoid the trap of politically reductionist explanations while capturing the PRF's focus on the effects of politics on policy. Given these shortcomings, the explanatory and outcome variables will reflect a minor framework adjustment in the following sections.

Legitimacy is defined as a polity's acceptance of the goals and authorities that guide how policy problems are solved. It is conceptualized as "shaped by assessments of the strength of the ideas behind a regime, the authority of the institutions that are involved, and the interest support for a regime (Jochim & May 2013)." This definition fails to sufficiently demarcate how regime legitimacy relates to and interacts with other constructs and contributing factors. Given that the legitimacy construct overlaps with ideas and interests, it will therefore be excluded from the analysis and considered embedded in the interaction of ideas and institutions as detailed later.

The notion of institutional durability is directly relevant to account for anemic regimes (Knight, 1992). For Knight, departing from social efficiency and Pareto optimality as desirable social outcomes allows a better understanding of suboptimally stable institutions. Institutions are stable when individuals have no incentives to violate the rule or form a coalition to change them because everyone else is already complying.

However, stable inferior payoffs may incentivize a group past a threshold to change the previous arrangement. While institutional stability increases the reliability of information and stabilizes future expectations of behavior, the benefits of stability typically depend on the substantive nature of an institution's distributional outcomes. For example, if a community is in a permanent minority, the benefits of stable institutions are perceived as less valuable, especially if that permanent minority is systematically underserved. While rationalizing Homeland Security as an anemic yet durable and suboptimally stable regime can be justified theoretically, the label alone does not provide much in the way of explanatory power. Absent any large-scale focusing event such as 9/11, the interaction of ideas, interests, and institutions should provide a theoretical basis specifying conditions that allow sub-optimal institutions to endure. The following section sets the stage for the outcome variable of interest, a regime's trajectory.

3.2 Outcome variable: regime trajectory

The regime perspective starts with a set of policy-implementing sectors unified under an overarching regime. Therefore, a conceptual distinction should be made that accounts for variance between degrees of interest mobilization at the policy sector level.

Table 1 defined policy solutions as an implicit or explicit causal pathway that renders the ideas meaningful for political action and implementation. A convergent trajectory is one where policy goals are unified across sectors, and a regime-level of analysis becomes readily apparent ontologically. Therefore, one could differentiate a trajectory characterized by a movement from a divergent path where within-sector inertia of ideas, interests, and institutions resists subordination to a higher-level regime goal to integrated policy solutions across sectors over time. This distinction allows the crucial

operationalization of contrasting whether a particular sector's activity conforms with an overarching regime and whether its interactions with other sectors contribute to regime ends. A regime's trajectory can be conceptualized as a composite outcome variable with different stages for further specificity. The following section discusses those stages as part of a typology based on Cejudo and Michael (2017).

Policy coherence and integration are traditionally regarded in policy research as antidotes to fragmented government action. Fragmentation makes complex boundary-spanning problems harder to solve.[2] The CIP regime provides a practical example of policy fragmentation where competing and ambiguous objectives, overreaction, and issues that compete for attention are prevalent (May & Koski, 2013). These challenges are typical of complex societal issues emerging in traditional hierarchical sector governance (May et al., 2016). The CIP regime provided fertile ground for fragmentation given that its subsystems had "relatively stable actor configurations, each of which [is] characterized by specific sets of associated interests, belief systems, and problem perceptions" (Candel and Biesbroek, 2016). The following section outlines how the analysis conceptualizes coordination as a necessary condition for coherence and integration.

3.2.1 Coordination and Coherence

Policy coherence is a property of a set of policies in a regime characterized by complementarity and consistency of policy instruments and goals across policymaking sectors. A lack of policy coherence implies that sectors are at best working autonomously

[2] Cejudo and Michael (2017) claim that part of the reason for fragmented government action is a byproduct of New Public Management (NPM) reforms. NPM involved applying lessons from the private sector such as increasing specialization among other things to run a lean government. NPM specialization in the case of the cybersecurity regime could worsen governance systems' abilities to deliver holistic solutions for boundary-spanning problems.

with no shared objectives or, at worst, working entirely at cross-purposes. Coherence is determined at the policy design level, a function of pre-existing or new institutional capacity, shared policy ideas, and other contextual factors, including a willingness for organizations to coordinate (Cejudo and Michael, 2017). Targeted public policy aimed at resolving 'tame' problems is typically direct and sector-specific. However, boundary-spanning problems require coherent policy design across sectors to address problems in a complementary and self-reinforcing way jointly. In the absence of coherent policy design, boundary-spanning problems are subject to fragmented action exhibiting anything from counterproductive redundancies to obstructions or gaps. For example, as different sectors contend to shape problem definitions and policy responses to fit their substructures, inertia may lower coherence and undermine regime-level goals. Therefore, the coherence of policy goals refers to how objectives within sector policies are made to complement other sectors within the same regime to serve a common purpose. Goal coherence implies no redundancy, duplication, or gaps in how a policy targets a population. Finally, any measure of policy coherence encompasses coordination over inter-organizational programs, a necessary precondition for coherent policy design.

That said, implementing coherent policies in a regime does not guarantee the resolution of complex problems. Adjustments are often made during the implementation stage as policymakers cannot always account for policies' secondary effects and potential emergent regime properties due to exogenous political considerations. As the following section outlines, adjustments at the level of integration ensure that operational decisions at the sector level comply with macro regime objectives.

3.2.2 Integration

Policy researchers have typically used coherence and integration synonymously or have conceived their distinction as different degrees of coordination, often leading to policy researchers talking past each other (Cejudo and Michael, 2017). In a coherent regime absent policy integration, organizations would continue to preside over their structures, resources, and planning processes despite jointly working towards a regime goal. A sector's inertia can create lock-in effects and path-dependency that may preferentially serve incumbent interests, such as in cases of regulatory capture. Therefore, regime integration implies a subordination of sectoral objectives to serve an overarching regime goal. Such a function is typically enabled by an authoritative decision-making body such as a policy czar or an expert committee with cross-sectoral jurisdiction over agenda-setting and budgets.

Integration is therefore defined as an asynchronous process of strategic and administrative decision-making aimed at solving regime problems in a manner that encompasses but exceeds a sector's individual operational goals and subordinates them when needed. Integration does not necessarily move linearly towards convergence on an outcome; instead, it is best conceptualized as a positive (integrative) or negative (disintegrative) process of regime-level adjustments to the overarching policy idea. At the same time, lack of political will or resources may also limit integration to symbolic action or stymie it completely (Candle and Biesbroek, 2016). Candle and Biesbroek hypothesized a relationship between institutional variables of policy regimes (the configuration of organizations and their supporting beliefs) and variables related to concrete sets of policy goals and instruments. They contend that institutional change happens earlier in the

integration process and is a necessary precondition. Ideas, in that sense, are embodied in rules (institutions). In other words, advancing coherent policy goals and instruments towards regime integration follows sequential shifts in sectors' configuration, including the ideas they advance and the normative beliefs about the problem and its governance. The dissemination of coherent policy, therefore, requires an institutional change of some sort.[3] This conjecture is compatible with a stage-based conceptualization of the composite outcome variable as operationalized in table 2 below.

[3] For example, institutional scope expansions that build on pre-existing rules or the issuance of new Congressional authorities.

Table 2: Operationalization of outcome factor (regime trajectory)

Trajectory	Mobilization around regime	Stage operationalization
None to low convergence. Evidence of some coordination	Information sharing is limited. The bureaucracy is competitive rather than cooperative. Inter-organizational programs are purely sectoral and policy problems are embedded solely within the goals of the dominant sector. Policy problems are governed independently with no formal cross-sectoral involvement.	Is there a shared goal among organizations? Do organizations establish rules and define responsibilities for coordination? Do organizations share information?
Low to medium convergence. Evidence of coordination and some coherence	Procedural information-sharing occurs between public-private organizations across sectors. Sectors adjust inter-organizational programs to mitigate negative externalities. Rising awareness of externalities and mutual concerns prompts sectors to address boundary-spanning problems as part of their policy goals. Coherent policy design that does not operate at cross-purposes becomes an explicit aim.	Do sectoral policies overlap? Do sectoral policies reinforce or undermine each other? Are inter-organizational programs consistent in serving the same overarching regime idea?
Medium to high convergence. Evidence of coordination, coherence, and some integration	Two or more sectors have formal responsibility and engage in information sharing where joint decisions are made regarding existing resources to tackle policy problems. Interagency programs span across sectors where sectoral goals are fully coordinated and regime-level procedure is available. A decision-making platform is established to preside over coordinated agencies and coherent policies. Organizations subordinate their objectives to the regime's decision-making apparatus. The priority of the overarching regime goal overcomes the individual sector's policy goals. The process of integration yields integrated government actions as an outcome. The regime problem should be solved unless its causal theory of change is flawed.	Is there a mandate to address the problem and a causal theory for doing so that involves several organizations and policies unified under a decision-making body? Does the decision-making body have the authority, resources, and information for guiding its decision about the programs, agencies, financial and human resources to solve the problem? Is the decision-making body effective at subordinating an individual sector's goals to pursue the overarching regime idea?

The PRF emphasizes the positive effect of politics on policy implementation. May and Jochim consider the 'strength' of a regime equivalent to its political feedback and the extent to which a regime reinforces political commitments made in addressing a given problem (May & Jochim, 2013). Political feedback "enhances policymaking and implementation by reducing conflict over policy ideas by mobilizing key supporters and undermining potential opponents." However, feedback can also impede integration as it activates bureaucratic competition and pits various political interests against each other (Ibid). Instead of operationalizing a regime's "strength," which can be misleading due to the framework shortcomings mentioned earlier, this analysis regards regime "trajectory" as the operative outcome variable. The formulation of this typology allows tracking cybersecurity regime dynamics over time and across policymaking sectors while making the limitation of interpretive social science clearer.[4] It also allows for a functional demarcation of regime outcomes by considering how coherent design and policy integration help achieve regime-spanning goals.

In contrast, observations of fragmented action across policy sectors imply divergence in a regime's ability to rally interest communities behind a goal and implement cohesive and integrated policy. Should a boundary-spanning problem fail to be resolved given a convergent regime trajectory, the fundamental causality of its theory of change can be questioned. For example, if the decoupling of the US economy from Chinese ICT is

[4] The goal of interpretive social science is to explain past and present outcomes while making broad directional future predictions. Predictions are non-nomic (law-like) as they cannot be falsified (Popper, 2005).

insufficient to garner a US strategic advantage over its peer competitor, the fundamental policy ideas motivating regime change would have to be reconsidered.

The following section introduces factors theorized to affect a regime's trajectory. By studying how different policy ideas can foster cohesion and integration across the CI sectors under consideration, i.e., the information technology, communications sectors, and energy sectors, we can better understand the relationship and feedback loop between political forces and policymaking in a regime, a functional analytical component often overlooked in policy studies.

3.4 Explanatory factors and selection criteria

Political science has long embraced a pluralist theoretical tradition whereby ideas, interests, and institutions are used as foundational variables explaining outcomes (Parsons, 2007). According to the PRF, a regime's ideas, interests, and institutions determine its coherence and integration. Jochim and May (2010) make no claims about these variables' interaction and leave it to future research to uncover. The original formulation of PRF was undertheorized, but the literature on political economy and institutional theory can supplement May et al.'s analysis with a more productive accounting of the institutions' role in shaping regimes.

The PRF uses the term *institutions* broadly to include rules, norms, and organizations. This analysis similarly defines institutions as any formal or informal constraint actors devise to shape their interactions, including the organizations created to leverage the ensuing opportunities (Alt and North, 1990). That way, institutions determine the extent to which political interests can focus attention, information, and resources supporting policy goals in a regime.

Instead of offering competing theories to explain the same phenomena as do more positivistic research programs, the approach in this work is to leverage institutional theories that complement the PRF and explain unclear interaction effects in the explanatory factors. In determining the interaction of various factors and depending on the direction of the relationship, the process implies searching for clues indicating that political interests or specific institutional configurations are sufficient to overcome a loosely defined idea in fostering cohesion or integration. Should the relationship point in the other direction, the empirical search attempts to uncover how powerful and shared policy ideas absent a binding institutional structure could still yield a cohesive regime (Chisholm, 1995).

3.4.1 Policy ideas

Policy problems often have competing definitions within and across sectors. Different problem foci compete as sectors shape problem definitions and policy responses to fit their particular modus operandi (Jochim & May, 2013).[5] If a problem is recognized by at least one sector as requiring a holistic governance approach, it is considered *boundary-spanning*. Policy ideas are the basic building blocks by which sectors with boundary-spanning problems can be unified under the same regime banner (Jochim & May, 2013). Policy entrepreneurs use them as organizing principles to rally support from interest groups as they provide leverage to extract political commitments from policymakers (May et al., 2016). In discussing the role of ideas in politics, Hall argued that interests acquire power by influencing the political discourse with their ideas, therefore

[5] For example, as CI protection underwent phase evolutions, the identification of CI sectors and what counts as key resources was modified and expanded (Lewis, 2014).

influencing policymaking without the more formal trappings of power and influence (Hall, 1993). That way, when interest groups use policy ideas to signal their political commitments across sectors, they can foster coherence within a regime even before the implementation stage by reducing uncertainty (Kingdon, 1995).[6]

The perceived nature of a problem is crucial in determining its capacity to mobilize interest groups in a regime. 'Tame' problems such as national infrastructure projects have a clear mission, and their resolution is readily apparent because they are "definable, understandable, and consensual (Rittel and Webber, 1973)." However, boundary-spanning problems are considered "wicked" by definition, i.e., "ill-defined," continuously re-solved, and subject to diverse value systems (Chisholm, 1995; Coyne, 2005; Rittel and Webber, 1973; Simon, 1977). The decision-making, communication, and organization theory literature have explored problem selection and framing related to the resolution process (Chisholm, 1995; Coyne, 2005; Reitman, 1964; Rittel and Webber, 1973).[7] Problem and solution ideation are considered a result of underlying cognitive and intrapsychic processes outside the scope of this analysis. Instead, a pragmatic approach is adopted: no functional distinction between problem formulations and the ideas presented as solutions is made if they are tightly coupled.[8] Therefore, this work considers the

[6] Congressional hearings are often motivated by a search for ideational consensus to reduce problem uncertainty (Kingdon, 1989).

[7] As pointed out by Chisholm, it remains unclear the extent to which the generation of solution alternatives is distinct from the representation of problems. Depending on the model of decision-making adopted, policymakers may be considered to embrace ideas as foundations for policy design by embedding a problem definition while simultaneously suggesting a resolution pathway or they may involve sepearate cognitive processes.

[8] Distinctions are still made wherever relevant should issue experts exhibit noticable patterns of focus on either problems or solutions.

policy problem-solution dyad as ontologically relevant and synonymous with policy ideas.[9] This operationalization posits that wicked problems of professional interest are already 'solved' when identified, framed, and defined (Rittel and Webber, 1976; Coyne, 2005). Therefore, policy ideas are defined as an articulated gap between a current state (a policy problem) and the desired end (a policy goal). The policy idea embeds an implicit or explicit causal pathway rendering ideas meaningful for political action and implementation (the policy solution). Interest groups bargain and negotiate for different interpretations of ideas. Once an interpretation is set, it can integrate action across sectors as policymakers design specific solutions to cohere.

Ideas are a powerful conceptual tool for regime analysis. However, their usefulness as a concept depends on the validity of their operationalization. Although ideas may be articulated in foundational policy documents, they are not always easily identifiable. Ideas do not spread in a vacuum; however, qualitative analysis requires having relevant selection criteria to bind the analysis (Yin, 2017). The relevant analytic question to consider when isolating ideas as an explanatory variable is the meaningfulness and relevance of the core regime issue to the key actors implementing the policy. Operationalization requires capturing how ideas are reinforced through statements and actions of policy entrepreneurs. For example, by looking at the consistency of definitional ideas motivating the Homeland Security regime, Jochim and May (2013) operationalized ideas as the degree of "ideational uptake," i.e., the endorsement of core ideas that serve organizing principles around a regime. The logic is that officials' use of ideational labels

[9] Kingdon (1986) highlighted how policy entrepreneurs couple problems with solutions and then couple both elements in a political narrative. Both terms are used interchangeably.

in congressional testimonies, strategy documents, and other media are good indicators of their "buy-in" to these concepts. In the cybersecurity regime, the specific definition of terms such as the 'national security interest' or 'interdependent CI systems' and the consistency of their usage across sectors denotes the coherence of ideas around what constitutes the relevant potential threat. Comparing the ideational uptake level across sectors can also gauge whether a specific use of language is part of an integrated regime effort or contained within a specific sector. Table 3 below describes the operationalization of the explanatory variable on both the threat of China and that of IT/OT convergence as the selection criteria. The section following table 3 outlines two institutional theories helpful in confining the analysis and complementing shortcomings left by the original PRF formulation.

Table 3: Operationalization of explanatory variable

Scope of policy ideas	Interest groups	Institutions
Characterization of ideas: How did ideas evolve in relevant Congressional hearings and agency-specific proceedings? When considering ideas' underlying themes (NVivo nodes), is one distinct pathway followed at the detriment of another, and why? Do both policy ideas interact, and is one leveraged to bolster the other? Relationship of ideas to the regime: To what extent do hearings involve a boundary-spanning formulation of ideas between relevant sectors? Are there any sector-specific differences for the characterization of both ideas?	Who are the main interest groups involved? Are policy entrepreneurs (issue-experts or policymakers) consistently pushing the same ideas across policy sectors? Is the causal theory of change introduced as a solution to the problem consistently leveraged? Are policy entrepreneurs distributed into distinct interest groups advocating a specific ideational pathway at the expense of another? Do presented policy ideas appear to be self-serving? Are any political commitments to ideas made and are any bargains struck?	Is the pre-existing institutional makeup supporting the main policy ideas? Have rules been modified to accommodate the policy idea? Is institutional change significant, swift, and encompassing i.e., is a critical policy juncture operative? What are the distributional implications of ideas' institutionalization?

3.4.2 Interests and institutions

While there are many different schools of thought within Institutional Theory, two specific strands can fill gaps left by the original PRF formulation. Historical institutionalism (HI) derives its explanatory power based on the conditions behind institutions' genesis, i.e.,

resource allocation and the substantive makeup of rules created. Rational-choice institutionalism (RCI) highlights the capacity for actors in subsystems to strategically bargain for benefits. RCI derives its explanatory power from analyzing distributional outcomes (Knight, 1992). Both theories are considered compatible with the PRF; they derive explanatory power from considering costs of collective action and how institutions reduce uncertainty for actors.[10] HI's focus on path-dependence and policy junctures is relevant to the interplay of policy ideas and institutions, while RCI's emphasis on strategic bargaining provides a language to analyze interest groups.[11]

Historical institutionalism studies the condition under which institutions evolve using a broad historical vantage point, analyzing the past to explain the present and making guarded predictions. The HI approach divides history between "normal periods" and "critical junctures," where significant change happens. It is appropriate for this analysis given the long arc of historical evolution with the cybersecurity regime where major exogenous shocks such as the terror attacks of 9/11 were a critical juncture resulting in the Homeland Security regime.[12] Cyberspace includes countless other examples where new

[10] The process of institutional change emphasizes collective action and uncertainty problems within the different social groups. Both HI and RCI theories agree that high uncertainty and costs of collective action make for weak institutions. These costs prevent having more socially efficient rules and laws that increase a community's output. The analysis then considers what intervention will allow groups to either maintain or change rules and resolve the collective-action problems to achieve their distributive goals.

[11] While both ideas and institutions reinforce each another, the discursive aspect of ideas and their potential to induce institutional change requires they are considered as an *a priori* causal explanatory factor.

[12] The original legislation that formedHomeland Security was borne out of many previously existing entities' conglomerations. The DoJ, Customs enforcement, and intelligence gathering. It was a consolidation of authority under a new umbrella concept of HS. New bureaucracies and organizational structures were created by consolidating and expanding existing institutional structures. The cybersecurity regime is similarly conceived as a new regime borne out of existing structures and creating new ones. The various mechanisms

technology features that are not captured by pre-existing rules are introduced, causing a power struggle, renegotiation, and setting off a new institutional path. Critical junctures are a confluence of triggering events that set institutional or policy change in motion (Hogan and Doyle, 2007). The duration of a juncture may involve a relatively brief period in which a fork in the institutional path occurs or an extended reorientation period. In the latter case, however, a logical pitfall must be avoided. Critical junctures are separated by long periods of stability, as with the more mainstream punctuated equilibrium theory of policy change (Jones and Baumgartner, 2005). Change can be non-existent or incremental but must necessarily be, at times, significant and abrupt. Thus, HI commits its adherents to distinguish incremental change from critical junctures. Defining what constitutes a critical juncture must be specified at the onset of research to follow an operationalized and falsifiable methodology (Hogan, 2006).

First, the tension inherent in the gap between a perceived policy problem and its solution leading up to a period of change must be present and identified.[13] Second, change must be "significant, swift, and encompassing" (Hogan, 2006). Large exogenous shocks such as 9/11 produce an overwhelming mandate for structural and policy change. Threats to

---

to address collective action problems and uncertainty in the cybersecurity regime include coordinating authorities, partnership networks, private contracts, regulatory oversight, and other instruments considered in the analysis.

[13] Hogan and Doyle argue that policy change depends on entrepreneurs reaching consensus around a particular set of new ideas. This is a period of institutional flux where policy entrepreneurs bargain for reforming existing distributional arrangements they find suboptimal by contesting the definition, meaning, and solution to the problems identified (Blyth, 1997). They exploit windows of opportunity to contest prevailing paradigms and replace old ideas with new ones (Kingdon, 1995). As policy entrepreneurs replace old ideas with new ones, the tension inherent in the gap between a perceived policy problem and its solution, leads to a period of change. Therefore, ideas predate institution, and their change becomes a necessary condition for a critical policy juncture to be meaningful (Hogan and Doyle, 2007).

national security have been studied as exhibiting such tensions (Cortell and Peterson, 1999). However, less dramatic events and more long-standing wicked problems such as China's threat can also contribute to significant institutional change. The change itself, however, cannot be a long, gradual process. Swiftness needs to be operative; otherwise, the change would be incremental.

Further, the effect of the change bringing about a critical juncture must be distributed among relevant regime actors with 'skin in the game' (the encompassing condition). Finally, it should be noted that critical junctures do not necessarily create path dependency.[14] Pierson argues that institutional stability can result from non-path-dependent causes (Pierson, 2004). For PRF, these causes are revealed by an interplay of ideas and interests.

When it comes to RCI, the theory's explanatory power is in analyzing the political-economic dynamic of interest groups. The intersection of trade and ICTs and the crucial coupling between economics and security externalities warranted its consideration. For RCI, the neoclassical postulate of maximizing social welfare is not the evaluative criteria; instead, what counts as the best institutional structure, depends strictly on distributional consequences. While institutions can still provide collective benefits, they are considered the by-products of distributional conflict over preferred outcomes.[15]

---

[14] Path-dependency is defined as a quality of persistence that triggers a positive feedback and generates increasing switching costs once a path is followed. For example, the Biden administration did not reverse USG policies on Chinese ICT. A possible explanation is due to the political costliness of the return process. The logic of institutional path-dependence entails a set of initial conditions with multiple potential equilibria and outcomes at critical junctures that, given the correct sequence, can trigger positive or negative feedback mechanisms that reinforce and lock a pattern into the future (Pierson, 2000).

[15] The efficiency of institutions is irrelevant. Instead, distributional outcomes and their implications on relevant stakeholder are operative. Adopting an evaluative criterion around transaction costs in the search

The focus on distributional outcomes sheds light on two crucial aspects of collective action. Distributional bias divides actors into those who reap a larger share of benefits through a more favorable institutional arrangement and actors with smaller shares that prefer a different arrangement. This disparity can increase enforcement costs and enter the cost-benefit calculus of those who benefit more from the institution. If costs are high enough, those that benefit may opt for less biased rules to lessen the tension for change. Meanwhile, the underserved community must pay the standard cost of collective action and fight to change the status quo. For HI, the strength of exogenous shocks or the level of ideational tension, once overcome, will decide whether group members overcome the costs of collective action (Hogan, 2006; Hogan & Doyle, 2007). In contrast, for RCI, the cost of collective action is pitted against the incentive to overcome distributional outcomes that yield power and resource asymmetries.

Competitive sectors are characterized by fluid institutional arrangements where participation is uncertain, e.g., the ISE environment and the PPP structure. The degree to which institutions reinforce cohesion depends on "prior interest relationships and the power of the coalescing idea" (Jochim and May, 2010). While institutional forms vary, the analytic concern is the degree to which institutional form fits regime circumstances. For example, the US-China Economic and Security Review Commission provided more

for how current instiitutions fall short of an "optimal" model would have struggled with a multiplicity of policy sectors and their divergent values e.g., trade and tech policy pitted against military competition and foreign policy (Williamson, 1989). The aim is to determine whether current regime rules are fulfilling their intended objectives while providing distributional benefits to a majority and understanding why. However, no assertions are made as to the validity of a regime's causal theory of change. In other words, a convergent and coherent regime is not necessarily a 'good' regime.

institutional backing to the idea of China's threat in Congress compared to the Obama administration's cybersecurity czar.

CHAPTER 4. METHOD AND CASE STUDY PROTOCOL

4.1 Process tracing

Process tracing (PT) is a research method that identifies intervening causal mechanisms by linking contributing factors to an outcome.[1] PT is analytically focused on the "dynamic, interactive influence of causes on outcomes (Beach and Pedersen, 2019)". The technique works by explicating the sequence of cause-effect processes in a narrative (the trace) then works backward by linking how an outcome that has occurred may have been caused by mechanisms hypothesized by theory (the process).

The PT variant in this analysis is used for theory-testing. It leverages the PRF literature to test whether a hypothesized causal mechanism is present.[2] This analysis selected cybersecurity regime problems where regime cohesion is observed, i.e., US-China geopolitical rivalry and cyber-physical convergence. The goal is to evaluate if sufficient qualitative evidence indicates that a hypothesized causal mechanism links either contributing factor to regime outcomes as theorized by PRF. That way, PT also tests whether the empirical evidence at hand strengthens or weakens our confidence in PRF's validity as a general framework explaining regime phenomena.

---

[1] A quantitative language is used to better illustrate hypothesized causal directions between factors of interest.

[2] Both theory-building and theory-testing variants have inductive and deductive components in their logic sequence. The two variants differ in whether they place theory before the fact or vice versa. In both cases, variables are known and specified ahead of time and the analytical focus is the CM linking them. A theory-building approach is later adopted when considering how ideas, interests, and institutions interact to foster or impede on regime cohesion.

The inference model used in PT proceeds on a within-case basis, based on in-depth, single-case studies that are not feasible using other social science techniques.[3] PT allows the analyst to make use of "both generalizing and particularizing explanations, placing cases as instances of a class of events while also giving detailed historical explanations of each case (George and Bennett, 2005)." Therefore, the aim is to generalize beyond the single case study to a population-level phenomenon relating to regime coherence. Statistical inference and comparative cross-case methods are not applicable to make within-case inferences about causal mechanisms given the research question.[4] PT instead infers the presence or absence of a hypothesized CM within a single case. Therefore, PT can be used to explain macro-historical phenomena and identify "*which* aspects of the initial conditions observed, in conjunction with *which simple principles* of the many that may be at work would have *combined* to generate the observed sequence of events (Ibid)."

The assessment of whether specific evidence confirms or disconfirms a hypothesis follows Bayesian logic.[5] Formally, the theorem states that belief in the validity of a hypothesis after evidence p (h | e) (the posterior probability) is given by the prior p (h) — which is the degree of confidence in the validity of a hypothesis based on prior

[3] Whereas other techniques such as the congruence methods test for the same prediction for X and Y at different times, process tracing predictions are set such as to capture both entity and activity involved in each part of a CM.

[4] Statistical techniques estimate the magnitude of effects independent variables have on a dependent variable and infer effects to a population, i.e., cross-case inference.

[5] Mathematical notion is used for illustrative purposes only. Bayesian logic contrasts with post-positivist Popperian falsificationism as it only allows for convergence or divergence from certainty but never reaches a state of full confirmation or disconfirmation.

theoretical knowledge (before data gathering) — divided by the prior itself and likelihood ratio.

In a quantitative setting, the likelihood ratio, denoted by p (e | ~ h) p (~h) / p (e | h), is given by the expected probability of having found the evidence if the hypothesis was not true p (e | ~ h) p (~h) divided by the expected probability of finding new evidence in support of a hypothesis p (e | h). While the estimation of the expected probability is an interpretive assessment based on previous knowledge, the same logic applies. The expected evidence for a CM must be specified ahead of time in a project log, including whether that evidence would increase or decrease confidence levels. Contrary evidence supporting alternative hypotheses is noted following the same procedure.

Therefore, increased confidence in a theory's validity is achieved when a posterior probability exceeds the prior probability before evidence was collected. It follows that an analyst assigns a higher weight to evidence (if found) that was *a priori* expected to be less probable based on previous knowledge of the phenomenon. Any surprising finding is subjectively balanced against contrary evidence pointing in the direction of another hypothesis. In other words, given that observations are accurate, evidence of a lower expected likelihood has more power to corroborate (or disconfirm) a theory compared to evidence of a higher expected prior likelihood.

4.2 The drawbacks of process tracing

The subjective nature of qualitative probability expectations is guarded against by leveraging prior research and a generally conservative approach to updating belief and admitting evidence. At the same time, this type of analysis forces the researcher to take

equifinal interpretations into account, i.e., considering how different paths could have led to similar outcomes (Von Bertalanffy, 2010). If explanatory factors are expected to affect the outcomes via underlying CMs, the researcher pre-specifies these associations then sets out to uncover them, noting surprising evidence along the way. However, the ruling out of spurious explanations remains challenging. It should be noted that process tracing can only reach provisional conclusions when data is limited. The implication is that direct, in-depth interviews are warranted as secondary data sources, notably when archival records are missing. Triangulation methods that ensure data sources are independent and complete are also used as a safeguard.

4.3 Case study protocol and data collection method

4.3.1 Case Study Overview

The following case study protocol contained general procedures and rules followed during data collection and a detailed explanation of how factors were operationalized. The case study protocol guided the data collection process and needed to be regularly consulted. It provided the grounds on which knowledge claims are validated by linking data to propositions using the research instrument (specifying internal validity) as a method to increase its reliability and assess the validity of its claims (Yin, 2017). Practically, repeating work cycles outlined the information that needs to be collected using the protocol template, how measurements are made, how evidence is interpreted, then updated assumptions accordingly.

4.3.2 Uncovering causal mechanisms

This single case study aims to test which of two policy problems (US-China geopolitical rivalry and cyber-physical systems' convergence) better explains degrees of coherence and integration in a defined cybersecurity policy regime.

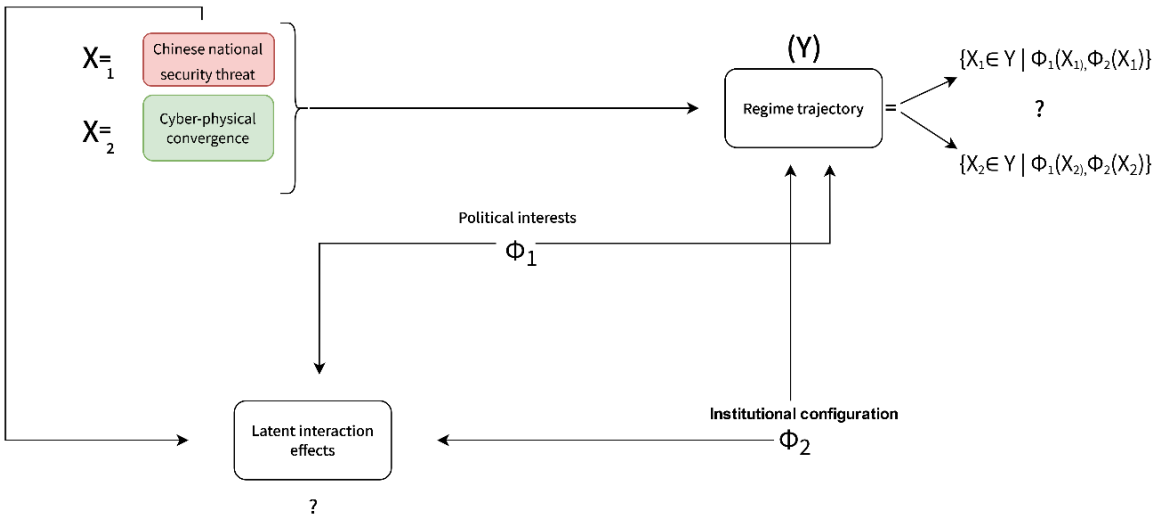


Figure 2: Causal Model

Figure 2 outlines that ideas propagated by political interests and those prevalent in institutions can interact through θ_1 and θ_2 and affect a regime's convergence or divergence. Figure 3 below compares the theoretical and empirical levels of the methodology.

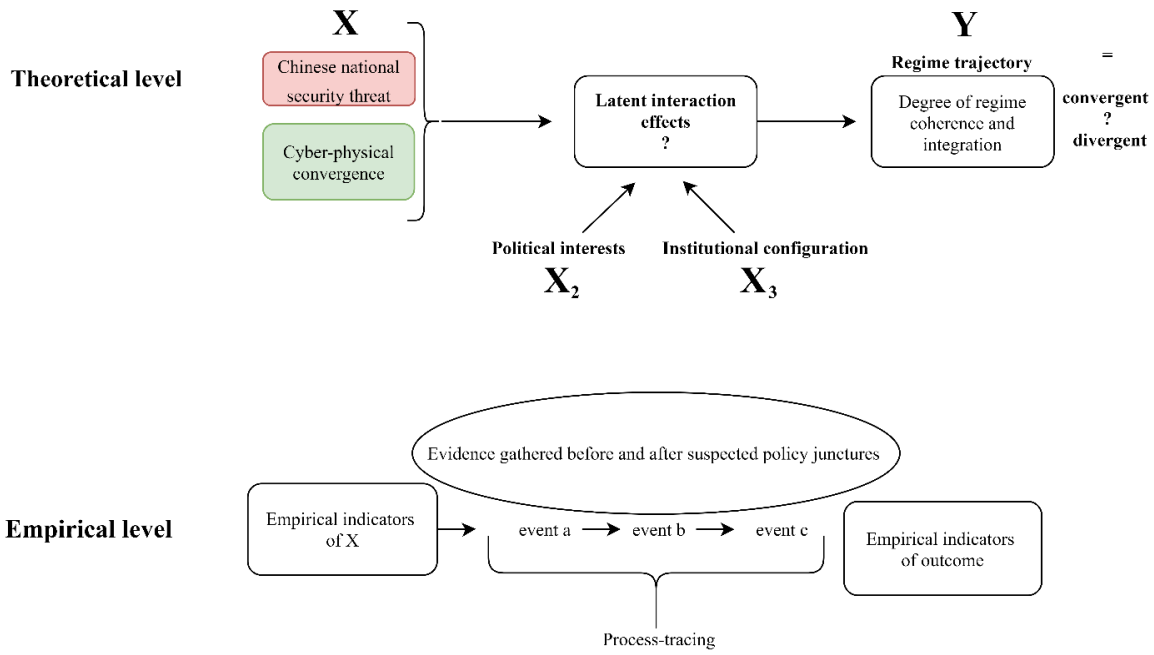


Figure 3: theoretical and empirical model comparison

PT distinguishes between raw empirical data and evidence, processed for accuracy and interpreted in a specific context. That way, observations, and case-specific knowledge combine to form evidence. Sources of evidence are theory-driven, and their evaluation involves three steps. First, data is collected based on the predictions we would expect to see if a hypothesized CM is present. Second, the collected observations' content is assessed using specific contextual knowledge to determine how they can inform the analysis.[6] This assessment of evidence is used to make updating inferences as per the previously outlined Bayesian logic.

Empirical evidence from the cybersecurity regime was collected and used to infer that all the parts of the hypothesized Causal Mechanism (CM) specified by PRF were present in

[6] Contextual specificity is defined as the relevant scope and initial conditions that are necessary for a given causal mechanism to function.

both the outcome variable and contributing factors. Four types of evidence relevant to process tracing analysis were specified before data collection: pattern, sequence, trace, and account data. Pattern-based evidence relates to meta-data derived from the data catalog using NVivo, e.g., number of hearings, the prevalence of coded nodes, and node attribution (issue expert, interest group, and other coding categories). For example, in testing mechanisms of ideational transference, testimonies across hearings and repeat appearance were recorded as a relevant pattern. Sequence evidence described the spatio-temporal dimension of events. If a hypothesis involved expectations about the timing of events, then sequence evidence was operative. For example, if a newly proposed rule proposes export controls to target a Chinese firm, other data is included to provide evidence of coordination in targeting that firm on other fronts. In that example, evidence of coordinated action between agencies suggested increased confidence in the validity of a policy idea's effect on regime coordination. Trace evidence is that whose existence proves that mechanism did occur. For example, the transcript of congressional testimony is evidence that a testimony occurred.[7] Lastly, account evidence pertains to the qualitative content of empirical material, e.g., substantive evidence derived from congressional testimonies and the synthesis of relevant policy ideas. Table 4 below describes the operationalization of the explanatory variable on both the threat of China and that of IT/OT convergence as the selection criteria. Table 5 outlines the hypothesized levels of the explanatory variable.

[7] Despite the tautology, this type of evidence is highlighted to emphasize the notion of surprise in cases when the mere presence of evidence is sufficient to validate or invalidate a mechanism.

Table 4: Operationalization of explanatory variable

Scope of policy ideas	**Interest groups**	**Institutions**
Characterization of ideas: How did ideas evolve in relevant Congressional hearings and agency-specific proceedings? When considering ideas' underlying themes (NVivo nodes), is one distinct pathway followed at the detriment of another, and why? Do both policy ideas interact, and is one leveraged to bolster the other? Relationship of ideas to the regime: To what extent do hearings involve a boundary-spanning formulation of ideas between relevant sectors? Are there any sector-specific differences for the characterization of both ideas?	Who are the main interest groups involved? Are policy entrepreneurs (issue-experts or policymakers) consistently pushing the same ideas across policy sectors? Is the causal theory of change introduced as a solution to the problem consistently leveraged? Are policy entrepreneurs distributed into distinct interest groups advocating a specific ideational pathway at the expense of another? Do presented policy ideas appear to be self-serving? Are any political commitments to ideas made and are any bargains struck?	Is the pre-existing institutional makeup supporting the main policy ideas? Have rules been modified to accommodate the policy idea? Is institutional change significant, swift, and encompassing i.e., is a critical policy juncture operative? What are the distributional implications of ideas' institutionalization?

Table 5: Hypothesized levels of the explanatory variable

Scope of policy ideas	**Interest groups**	**Institutions**
Possibility 1: Both policy ideas are presented equally Possibility 2: One policy idea is more prevalent than the other Possibility 3: Both ideas are interdependent, i.e., one idea reinforces the other, or new ideas are created altogether.	Interest groups cooperate, compete or dynamically alter behavior according to policy windows. Possibility 1: Groups are cohesive and consistently advocate the same ideas. Group's role in governance is static Possibility 2: groups' role in governance is dynamic; they can evolve due to infighting, evolving policy windows, or both.	Possibility 1: Preexisting structure is expanded Possibility 2: new institutions are created **Levels**: Institutions either direct information flows and authority to structure cohesion and integration or, remain more fluid with uncertain participation. Both outcomes are theorized to depend on unknown interaction effects. The analytical consideration is the goodness of fit for the regime

4.3.3 Unit Selection Basis

To avoid endless historical regress searching for foundational causes, conceptualizing a meaningful starting point for analysis starts with relevant institutional genesis (Hogan, 2006; Hogan and Doyle, 2007). China's ascendence to the World Trade Organization (WTO) was a significant event followed by creating the US-China Economic and Security Review Commission in 2002, a significant locus of policy ideas on the China threat. After 9/11, the Bush administration integrated previously existing CIP institutions into a new Homeland Security regime with society-wide implications, including ICTs and cybersecurity. The newly created Department of Homeland Security (DHS) consolidated

departments from various branches of government. The cybersecurity regime comprises government agencies involved with the IT, Communications, and Energy sectors, many of which were institutionally defined during this era.

Given that other institutional analyses focused on the consequences of 9/11 and the Homeland Security regime, this analysis focuses primarily on the last decade at the time of writing. As a single case study, the research included relevant outcome evidence from the last decade as outlined in the data catalog available in the appendix. The outcome selection criteria included sector-level policies, including Congressional legislation and federal and independent regulatory rulemaking.[8] Inter-organizational behavior was recorded as evidence of coordination.

However, observations for explanatory factors went as far back as 2003 and included policy ideas propagated by testifying issue experts and political interests. Policy problems and ideas cannot propagate in a vacuum. Instead, they are lobbied for by political interests and are embedded in institutions. Policy ideas were compared to how they reflect an institutional change as evidence of political bargaining and compromise. The content of testimonies was coded according to categorical patterns that emerged, i.e., themes related to the purpose of the testimony. Themes were generated following an inductive lumping and splitting evidence as appropriate for case study research (Yin, 2018).

The inductive search for patterns followed a query for keywords, displaying and tracking results in word trees using the NVivo software. For example, search terms for the

[8] the IT and Communications sector, the Energy sector was included only if relevant for IT/OT convergence. Individual legislation does not constitute a policy juncture

potential threat of China included terms and acronyms like: China, cyber-threat-actor, PLA, CCP, MCF, and others. For IT/OT convergence, terms like cyber-physical systems, analog, technology control systems were used.

Congress' main website congress.gov was queried for congressional records, including hearings, reports, and the congressional research service. The web service govtrack.us was cross-checked for accuracy and supplemental information.[9] Nested nodes included ICT trade and national security, which branches out to two separate nodes, *cooperative associations of bilateral IT trade and national security,* and *competitive associations of bilateral IT trade and national security.* Both nodes are further subdivided into child nodes.

Finding one of the two policy ideas as shaping the regime is not a sufficient finding *per se*. Instead, a detailed explanation characterizing what aspect of those ideas facilitated regime formation and perpetuation was needed. Since not all regime outcomes are equally relevant, particular focus was afforded to suspected critical junctures i.e., periods of swift, all-encompassing change. While counterfactual causal claims are not possible, direct characterization of the dynamics of regime formation that the policy idea has produced was achieved by systematically untangling and linking sub-elements of both ideas.

[9] Other sources included the federal register, agency-specific regulation dockets at regulations.gov and US-China commission reports at https://www.uscc.gov/

4.3.3.1 Policymaking departments and agencies in the federal government

The descriptive value of the policy regime lens is in outlining how governing arrangements are set up to address a specific problem. Regimes are artificial constructs and constitute a superordinate structure to defined policy sectors. However, a regime's boundaries should be delimited in such a way as to facilitate understanding of policy-politics feedback mechanisms instead of adding complexity. Therefore, a regime's scope should be pragmatically determined by boundaries suited for a specific purpose. As May and Jochim put it: "the test of the value of the depiction of a policy regime, as with other constructs in the policy literature, is not the particular construction but the insights provided by that construction" (May and Jochim, 2013).

Therefore, boundaries were determined artificially following an inductive approach. As specified by the PRF, the main ideas and institutional arrangements provided a basis for extrapolating boundaries through backward induction. Whenever an entity part of the PPP structure was found issuing authoritative action bearing on the ICT and energy sector regarding the identified policy problems, that entity was considered within scope for analysis. The following Cabinet departments under the Obama and Trump house were considered for relevant outcomes: HS, particularly the Cybersecurity Infrastructure and Security Agency (CISA), the Office of the Trade Representative, Treasury, State, Commerce (including NIST), and Justice departments. Relevant Executive Orders and communication by the White House are considered within scope. Independent regulatory agencies and other bodies included the Federal Communications Commission (FCC), the Federal Energy Regulatory Commission (FERC), the National Infrastructure Advisory Council (NIAC), and the Office of Trade and Manufacturing Policy (OTMP). The scope

of the federal government is limited to civilian policy-making agencies, thereby excluding military agencies involved with cyber doctrine and implementation. Despite being offense-focused, military agencies such as Defense Information Systems Agency (DISA), Cyber Command (USCYBERCOM), or combat support agencies like the National Security Agency (NSA) may be indirectly involved with the protection of CI and the defense of military networks. While these agencies may be involved with information sharing with the civilian sector (public and private), they are not involved in policy design and were therefore excluded.[10] The following figure 4 outlines the national U.S. cybersecurity regime, starting with the federal government.

[10] Unless direct coordination with civilian agencies was found

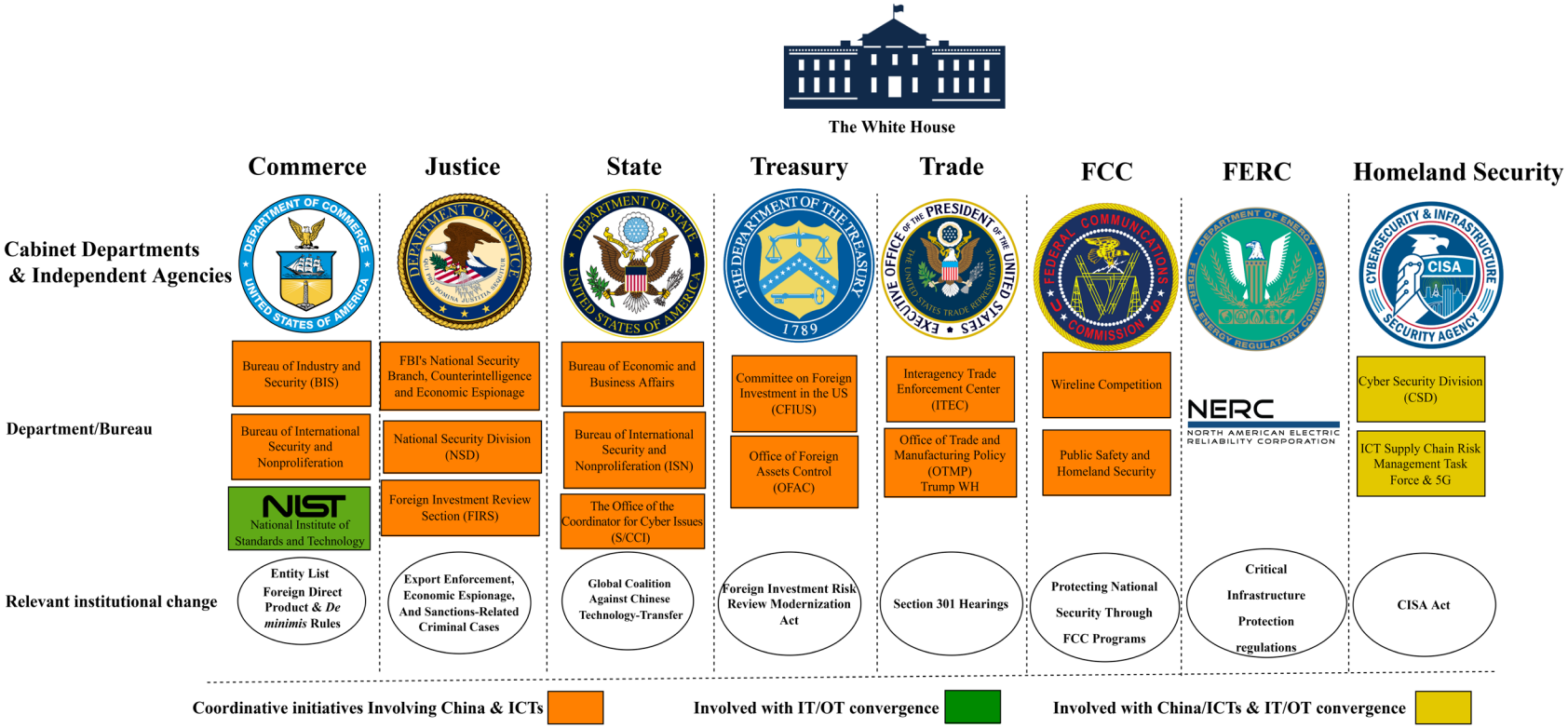


Figure 4: The cybersecurity regime's civilian federal government

4.3.3.2 Legislative policy-making bodies

Rulings by the House, Senate (or joint Houses) dating from 111-116th Congress provided the institutional basis for regime outcomes. Partial rulemakings, those passed by one chamber or incorporated into other legislation, were included to the extent they provide relevant background and context to understanding a subsequent rule that passes both Chambers (for a more detailed list outlining selection criteria, refer to the appendix).

Regime outcomes were selected and analyzed first using a rulemaking's textual content (from congress.gov and govtrack.us), academic research, (academia including the Journal of the NPS Center for Homeland Defense and Security and the Congressional Research Service to detail the inner workings of DHS and congress respectively), the Government Accountability Office (addressing the efficacy of implementation), and various other archival sources to either triangulate findings or help better define the political context. Failed rulemakings are only included if they can provide a context for understanding enacted rules. They do not follow the standard DV typology following accounts of coordination, coherence, and integration. Sources of analysis of Independent Variables IVs follow according to the catalog. Themes are grouped and retrieved from NVivo into this document progressively.

Congressional records of deliberations, Senate treaty deliberations, House Committee meetings reports, and rulemakings were included and outlined in the data catalog in the appendix section. Transcripts were collected for relevant session titles and coded according to the case study protocol using NVivo. For a complete list of sessions, see the

appended list. The *trace evidence* of hearings was recorded (a hearings' meta-data) along with a substantive synthesis.

Special Commission recommendations such as the Solarium Commission and other relevant specially commissioned reports were also considered. Evidence of policy implementation was provided by self-reported sector assessment, the Government Accountability Office (GAO), and secondary data from the academic literature. Figure 5 below presents a non-exhaustive account of Congressional hearings examined that include the two selection criteria and their intersection.

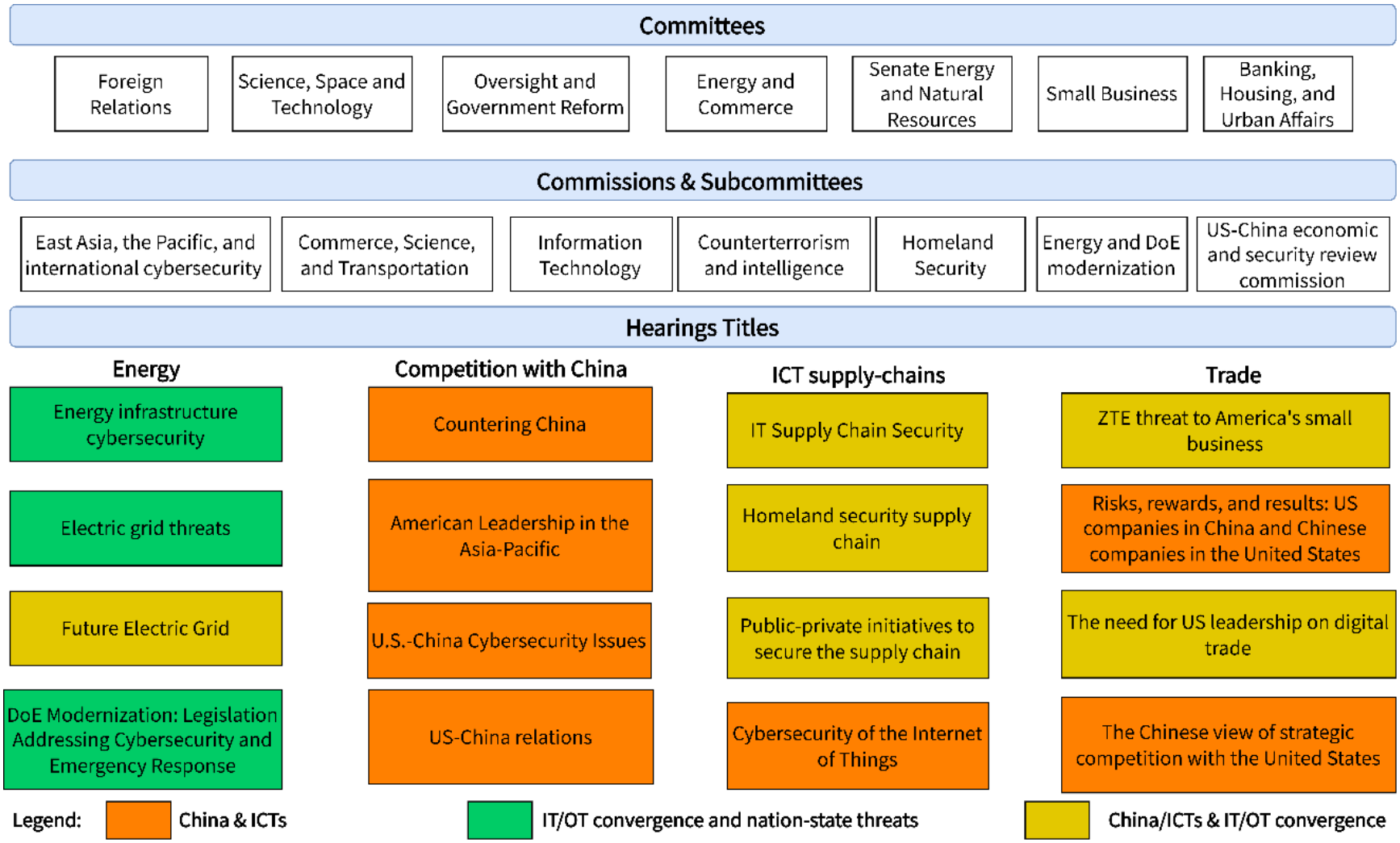


Figure 5: The cybersecurity regime's legislative government

CHAPTER 5. THE ORIGINS OF THE US CYBERSECURITY REGIME: FROM "ALL-HAZARDS" RESILIENCE TO CYBER THREATS

This chapter sets the stage for the upcoming analysis of how both policy problems impact the cybersecurity regime in chapters 6 and 7. It starts by summarizing the relevant history of the critical infrastructure protection environment in 5.1. Section 5.2 outlines how the perception of evolving threats has complicated conceptual and practical issues of regime demarcation. Finally, section 5.3 describes problems endemic to the DHS's institutional structure, i.e., what the PRF refers to as endogenous politics, especially given their impact on regime integration.

5.1 Critical Infrastructure protection

The protection of US infrastructure became a central tenet of national security in the 1990s, CI sectors' interdependence was recognized as US society reeled from natural disasters, culminating in a case of domestic terrorism in 1995. The Oklahoma City bombing catalyzed rapid change as the Clinton Administration created institutional capacity for whole-of-government action to protect CI.[1] In 1997, the President's Blue-Ribbon Commission on CI Protection (PCCIP) stated that the "rapid proliferation and integration of telecommunications and computer systems have connected infrastructures in a complex network of interdependence. This interlinkage has created a new dimension of vulnerability, which, when combined with an emerging constellation of threats, poses

[1] However, the ratio of planning to implementation was heavily skewed in favor of the former.

unprecedented national risk" (PCCIP, 1997). While these new threats have yet to result in a "cyber-9/11", they are still actively debated in the USG.

The National Infrastructure Protection Plan of 2006 would later identify "lifeline" functions – Energy, Water, Communications, Transportation, and Emergency Services – as systemically interdependent infrastructure sectors whose reliable operation is so critical that a disruption or loss of capability would ripple across other sectors and entail potentially devastating consequences (NIPP, 2006; 2013).[2] These "lifeline" sectors of CI are highly critical, and their prioritization grants them more salience than other sectors, such as the dams or transportation sectors (Lewis, 2019). [3] As addressed in chapter 7, digital convergence and cybersecurity are merging many security functions in the energy and ICT sectors, complicating public and private sector security responsibilities.

CI sectors are socio-technical environments with non-linear cause-effect relationships. An ongoing debate about the effect of complex systems on security highlights the value-laden and often political nature of security arguments, given the lack of empirical evidence in the case of all-out disaster scenarios. One system-level perspective presents CIP as a chain that is only as strong as its weakest link. Given that security threats are increasingly niched in the 'long tail' of a Pareto distribution, complex systems with last-minute interventions are susceptible to unforeseen 'black swan' events that carry the potential for devastating cascading effects (Taleb, 2007; Lewis, 2015; 2020). The

[2] The national plan was updated in 2013.

[3] CIP follows a model or risk-informed decision-making which involves prioritizing high-risk assets. However, these prioritization assessments are complicated by the fact that the cost of risk reduction differs nonlinearly for socio-political reasons.

opposite side of this debate holds that society has thrived despite inherently insecure information systems (Odlyzko, 2019).[4] Economists of information security have argued that one can limit the attack surface but not eliminate it. Given the costliness of security measures regarding equipment and constraints on legitimate users, one can only optimize the allocation of available resources and modify the incentives of cybersecurity breaches (Böhme, 2013).

From a public policy perspective, the tension between risk preferences reflects an incompatible overlay of converging ecosystems. In IT, the long tail of security threats is rationalized according to an equilibrium framework driven by the economics of information security. Whereas in OT, the concern instead shifts to running resilient systems in the face of stressors and allocating resources to points of criticality.

This work sets technical considerations and system-level properties aside and is instead concerned with the socio-political impediments to CIP, such as the path-dependent institutional conditions of having separate IT and Communications sectors and the ensuing organizational overlap. Such considerations are increasingly relevant in the ICT and energy sectors today as CI sectors continue expanding vertically across levels of government and horizontally across the public and private sectors. The following section describes how as threat-frames evolved from terrorism and weapons of mass destruction

[4] The economics of information security reflects a reality that one can limit the attack surface but not get rid of it completely. Equipment and security solutions are costly in terms of resources and in constraining legitimate users' productivity. For Odlyzko, complex systems such as CI sectors cannot be securely designed, given the plethora of functionalities from an engineering perspective. However, insecurity amidst complexity has benefits such as having a net that can still block the bigger insects despite having many holes. The appropriate course of action to remedy what Odlyzko calls the “long tail of security threats” is to adopt an equilibrium-seeking framework that balances technologists’ risk-aversion, optimizes resource allocation between security and productivity while engineering incentives for strong security (Odlyzko, A., 2019).

to cyber threats, concern about the USG's capacity to manage and integrate its response grew, with confusion around CI jurisdictional boundaries amid many warning calls for more infrastructure resilience (Nowlin, 2011).

5.2 Evolving threats to the nation and their institutional conceptualization

The original definition for CI was "physical and cyber-based systems essential to the minimum operations of the economy and government" (PDD-63). As the protection of CI became a national objective with Presidential Decision Directive-63, disparate national security threats were interlinked. For lack of a better approach, political mobilization was achieved through a broad, all-encompassing threat-frame dubbed "all-hazards" (Cavelty, 2007). Despite rallying CIP behind the idea of resilience to all-hazards, what applies as CI has varied throughout the years as sectors were added and institutions restructured (Lewis, 2019).[5]

Previous regime-based analyses of CI have focused on different eras where the central ideas shifted from all-hazard-preparedness and disaster mitigation to the threat of terrorism after 9/11 (Dunn-Cavelty, 2009; Jochim and May, 2013). By adopting a higher level of analysis, regime theorists Jochim and May (2010), May et al. (2011), May and Koski (2013), May and Jochim (2013) have argued that the Homeland Security and CI Protection regimes are ontologically different.

If, as the authors contend, policy regimes can be envisioned "for any set of problems for which there has been authoritative actions at some level of government," a case must be

[5] As a complex socio-technical environment, any precise definition for what counts as CI is bound to grapple with political and organizational forces beyond the scope of this work.

made for functional demarcation criteria on a case-by-case basis to allow meaningful analysis. While conceding that "the breadth of the policy regime is largely determined by the boundaries that one establishes in conceptualizing the problem or set of problems" as issues can nest and interlink, these authors have failed to capture meaningful links between Homeland Security and CIP. These links could have contributed to our further understanding of the PRF, especially regarding the interaction effects of the components of foundational constructs such as regime coherence, i.e., ideas, interests, and institutions. Such links would have also furthered our understanding of the extent to which powerful regime ideas can overcome institutional fragmentation or explain durable yet weak and 'anemic' regimes (May and Sapotichne, 2011).

May et al. (2011) found the Homeland Security regime to be 'anemic' because relevant stakeholders (CI sectors, the private sector, and the USG) pursued separate agendas reflecting their concerns and historical ways of conducting business. Notionally, Homeland Security meant different things for different stakeholders and, in practice, organizations diverged in implementation. The central motivating idea behind the Homeland Security and CIP regime (terrorism, all-hazard-preparedness, and disaster mitigation, respectively) was not shared. In other words, in trying to do too much, too little was achieved. Further, there were no strong constituencies, and the institutional locus — DHS and congress — were a weak force in inducing cohesion. These findings fit with the theoretical implications of a disintegrated regime that is, in turn, unsuccessful at implementation. However, the more puzzling outcome was that the regime was inefficient, yet the overarching structure prevailed as institutional capacity expanded in different sectors.

May and Jochim's work raises the question of whether the Homeland Security regime could be better conceptualized as the CIP regime changing its core defining idea, reinventing itself within the existing institutional structure. This question is particularly relevant given that the institutions and the organizational and interest communities behind the CIP and Homeland Security regimes had almost perfect overlap despite entailing different ad hoc focusing lenses.[6] These differences and how they played out across the various sectors depended first and foremost on the lens of problem formulation, e.g., terrorism, all-hazards, or cybersecurity (Cavelty, 2007).

Second, they depend on internal political dynamics and the institutional inertia at the creation of the DHS. Roberts (2005) and Patashnik (2008) explain how "the business of Homeland Security has become well ingrained in the American system through the provision of technology contracts, intergovernmental grants, and government activity" and that some regimes are "so deeply rooted in political practice and culture over time that its dismantlement becomes all but unthinkable" (Roberts, 2005; Patashnik, 2008). We need better explanations for such outcomes. Fluid regime boundaries impede our ability to recognize when evolving policy problems can better be conceptualized as distinct or evolving regimes.

Lewis (2020) provides a broader typological demarcation of CIP as governance issues evolve through various ideational phases. In the initial phase, a growing sense of

[6] While the CIP regime was borne out of long-term necessity the Homeland Security regime was a post hoc reaction to a large shock to the nation. Since public policy decision-making incentives are skewed towards short-term results instead of rewarding a long-term approach that hedges risk, adds system resilience, and devises mitigation plans, the reinvention of Homeland Security using the cyber-threat frame was necessary to preserve institutional momentum.

awareness of the security problem's intractability emerges as motivated by the all-hazards threat-frame, i.e., the combined threat of terrorism and natural disasters. Next is the era of public-private cooperation (or lack thereof). The middle phase includes contention around the governance structure between states and the federal government and is not addressed in this work. The two final stages are more informative to the analysis. The first is driven by the concept of resilience and risk-based decision-making, the second is by cybersecurity threats. These stages are best understood as motivated by threat-frames, a complementary concept to policy ideas used in this work.

Securitization theory posits that threat frames allow the deployment of extraordinary measures to cope with risk as traditionally non-military issues get shifted to the military domain (Buzan et al., 1998). Threat-frames are considered rhetorical devices embedded in policy ideas originating in actors' belief systems and characterized by a specific transference pattern across sectors.[7] For example, while the Bush administration and Congress did not use the label of a policy "regime" after the terror attacks of 9/11, discourse and policy action emphasized the need for an integrated approach to address the problem, using a new threat frame. As a result, the newly formed Homeland Security regime was now driven by the 'war on terror' as the 'all-hazards' approach could no longer serve as a coalescing idea across sectors.[8] The threat of terrorism facilitated the

[7] Threat-frames are addressed by securitization and communication theory generally. Both approaches are compatible with the PRF and can also be interpreted using similar methods.

[8] The question of overlap between theHomeland Security and CIP regime is beyond the scope of this work.

boundary-spanning aspect of the problem into multiple established policy areas (Dunn-Cavelty, 2009).

Using threat-frames as the fundamental unit of analysis, Dunn-Cavelty (2007; 2009) explored how threat construction affects politics in various security policy arenas, including cybersecurity, CI protection, and HS. Her research shows how cyber-threat frames became a matter of national security and high on the political agenda. She labeled that process as part of "threat politics," an ongoing political tussle over competing threat frames (Eriksson, 2001).[9] Drawing conceptual equivalence between threat-frames and "problem-solution" dyads is helpful, given the threat-politics focus in this work. Another reason for making this equivalence is that the regime lens focuses on how politics, or in this case, threat-politics, can affect implementation. Of particular interest is Dunn-Cavelty's finding on the vital role of non-governmental actors, issue-experts, and policy entrepreneurs, in setting the agenda of ideas and framing threats (Ibid).[10]

As a policy problem with international ramifications, cybersecurity has no shortage of literature tracking its long-standing emergence from the Morris worm onwards (Healey, 2013; Valeriano and Maness, 2015; Gorwa and Smeets, 2019). Cyber threats have today replaced the risk hyperbole that was once common of terrorism.[11] The defense establishment and mainstream media have perpetuated cyber threat inflation since early

[9] Threat frames are defined as "specific interpretive schemata about what counts as threat or risk, how to respond to this threat, and who is responsible for dealing with it" (Dunn-Cavelty, 2007).

[10] The disagreements on the nature and severity of the level of insecurity that Dunn-Cavelty points out were also later confirmed by May (2016).

[11] Terrorism was removed from the GAO's high-risk list for threat information sharing in 2017 (GAO 17-317).

in the millennium. A rampant and overinflated cyber rhetoric proliferated as the NSA warned of cyber-Armageddon, the FBI of an existential threat to the US, and congressional representatives warned of "cyberwar" (Thibodeau, 2010; Schneier, 2010; Vijayan, 2010).[12] Historically, the cybersecurity problem has enabled an environment where practitioners often forget that security is not a high-level goal by itself rather than a productivity enabler. The tension between balancing extreme risk-aversion with open technology systems continues today as politicians forgo complex solutions to wicked problems, relying instead on one-sided and often self-serving approaches. The intersection of CI and cybersecurity is increasingly salient today and continues to mobilize and engage diverse interests with an ample supply of experts from various disciplines.

5.3 The Information Sharing Environment (ISE) for Critical Infrastructure Protection

The topic of cyber-threat information-sharing (IS) has no shortage of ink spilled, especially in the CIP context. While cyber-threat information sharing remains the most salient CIP issue of the last decade, disintegrated policymaking and institutional problems have translated to many cybersecurity failures in the USG while information sharing remains one of the more persistent and challenging problems the federal government faces (GAO-03-760; Kean and Hamilton, 2004).[13] This section presents a summary

[12] The criteria for "criticality" and threats constituting an "existential threat" evolved as described in this work.

[13] Information sharing feature on the GAO's 'high-risk' list. For a review of notable cyber intrusions including federal networks see (CSIS, 2021).

account of institutional and organizational problems to IS from 2000-2010 to the extent that they can help understand dynamics related to the CISA restructuring in 2018.

The US government provides national security as a public good, supplied by the collective efforts of its military, intelligence community, and through private contractors dubbed the Defense Industrial Base (DIB). The provision of national security involves significant overlap with CI protection in practice.[14] However, since most CI is owned and operated by the private sector, legislative and regulatory demarcation of authority and responsibility for security provision remains the most challenging aspect of CI governance (Carr, 2016).[15] As threat-frames evolved, a loose institutional structure referred to as the PPP was slowly brought into existence, not by comprehensive strategic design but through a series of continuous top-down mandates orchestrated by the USG.

Starting with PDD-63 in 1998, the Clinton Administration called for a voluntary partnership and created Information Sharing and Analysis Centers (ISACs). after the USG understood the concerns of stove piping critical intelligence. After the 9/11 Commission Report, the dangers of stove piping of critical intelligence due to agency competition was made apparent, and the institutional and organizational capacity for IS was formalized with the creation of the Department of Homeland Security.
The initial CIP structure was superseded after 9/11 by Homeland Security Presidential Directive (HSPD) 7, which made the DHS responsible for protecting CI and coordinating PPPs (Bellovin et al., 2011). PPPs were referred to as the "cornerstone of America's

[14] Carr (2016) highlights how while CIP and national security are inexorably linked, cybersecurity is instead regarded as linked to the national *interest*.

[15] By most accounts, 85-87% of CI is owned and operated by private actors (Lewis, 2019).

cybersecurity strategy" at that time (National Strategy to Secure Cyberspace, 2003). After the Homeland Security Act, the Federal Enterprise Architecture (EA) explicitly mandated procedures for transferring and sharing information between government agencies, subject to accountability reviews by the Government Accountability Office (GAO).[16] However, as early as 2003, the GAO reported that "Information on threats, methods, and techniques of terrorists is not routinely shared; and the information that is shared is not perceived as timely, accurate, or relevant (GAO-03-760; GAO-05-207)." Per the 9/11 Commission recommendations, Congress passed the Intelligence Reform and Terrorism Prevention Act of 2004. The comprehensive framework for counterterrorism information sharing was established (Kean and Hamilton, 2004). Congress also established a new office with government-wide authority – the Office of the Program Manager for the ISE (PM-ISE) in 2004, later consolidated into the Office of the Director of National Intelligence (ODNI). The White House issued a National Strategy for Information Sharing in 2007 and worked through the OMB to provide information sharing guidance, creating comprehensive reform to handling the newly created category of controlled unclassified information (CUI).

The issue of failing public-private partnerships arose again in 2009 with the 60-day Cybersecurity Review conducted at the behest of President Obama (Bellovin, et al. 2011).

In 2010, the GAO concluded that public-private partnerships were failing to meet expectations regarding timely and actionable cyber threat information and alerts (GAO-

[16] The Federal EA is a policy framework at the core of intra-agency knowledge transfer and information sharing. It ensures investments in IT are tied to the President's agenda and sets out knowledge management as one of the four capabilities under its services component reference model.

10-628). According to private sector stakeholders, the problem was with federal partners failing to provide the capacity to share timely information in a secure setting. Confusion included scope and responsibility concerns regarding which federal office should be distributing information. Figure 6 below outlines the relevant institutional structure of critical infrastructure protection.

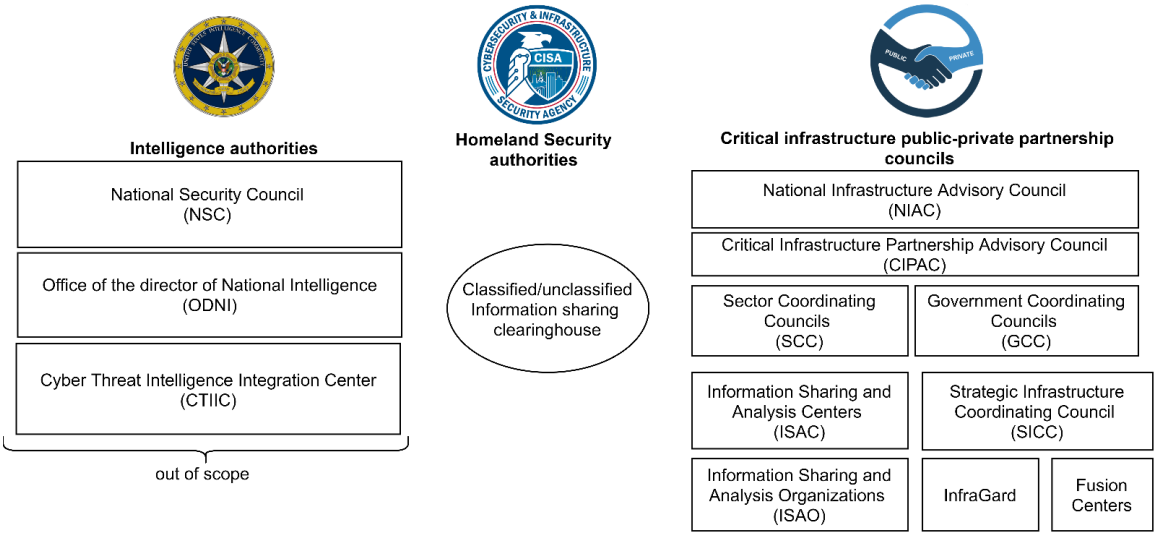


Figure 6:The institutional structure of Critical Infrastructure Protection

Harmonizing information sharing remains a significant institutional hurdle and collective action problem. The determining factor for a PPP's success often involves the proper assignment of control and property rights, especially given the underlying incentives they create (Rausser and Stevens, 2009). Security information is often framed as a 'commons' despite when lack of trust can often turn it into a 'bad' with the potential to ruin corporate

reputations. Further, timely and relevant information sharing is costly in resources despite efforts to automate the process.[17]

The ISE was expected to facilitate the distribution of various subtypes of relevant and timely cybersecurity information throughout the partnership while keeping nefarious actors in the dark.[18] However, non-cooperative and free-riding behaviors abound in the ISE as PPP stakeholders exhibited diverging preferences for control rights, responsibility, and resource allocation.

The cybersecurity regime is inexorably intertwined with 'top-down' PPPs established by the DHS mandate. For over 20 years, the federal government has leveraged the Office of the Director of National Intelligence, ISACs, and now DHS's CISA to orchestrate IS across the cybersecurity regime. In the private sector, capacity for 'bottom-up' inter-organizational peer-to-peer exchanges of a more limited mandate and scope such as Sector Coordinating Councils (SCCs) were made available to enable sharing of open-source and commercial threat intelligence (Green, 2021). Today, a capacity exists to channel information from the public sector to the private and vice versa. However, throughout its tenure, this "partnership" was tenuous and dysfunctional, given persistent

[17] DHS's Automated Indicator Sharing (AIS) program leverages existing technical standards (STIX language and TAXII protocol) to provide the automated sharing of unclassified machine-to-machine information.

[18] The term "information sharing environment" is defined and established under section 1016 of the Intelligence Reform and Terrorism Prevention Act of 2004 (6 U.S.C. 485). On a technical level, cyber information sharing relies on the exchange of Indicators of Compromise (IoC), which involve many standardization initiatives. For more details about IoC standards efforts see Skopik and Fiedler (2016) and Bakis and Wang (2017).

ambiguity over authority and responsibility between the public and private sectors (Ibid).[19]

Institutional problems are addressed in chapter 7 first at the planning level in terms of governance structures and rules, for example, the structural issue of how ISACs should be merged or layered. Second, they are addressed at the implementation level, i.e., information management techniques by the DHS, which acts as the "clearinghouse, integrator, analysis engine, and national source of cyber-threat information and defensive measures (Bakis and Wang, 2017). Other recurring issues involve the lack of a standard basis for translating classified data into actionable, non-classified information, the over-classification of information, and the automated sharing of information devoid of context.

[19] Carr (2016) has argued the need for replacing the term "partnership" with "relationship" to highlight those joint interests need to be leveraged instead of using ambiguous rhetoric that flattens complexity.

CHAPTER 6. THE CHINESE THREAT: IT TRADE WAR AND STRATEGIC COMPETITION

6.1 Introduction and chapter outline

The US government's assumptions about China's threat within the last decade require disaggregation if its potential effect on ensuing cybersecurity policy is to be evaluated. As nationalistic Republican and Democratic voices congealed around a unified narrative, China's threat became less differentiated, especially during the Trump administration. However, as this thematic analysis will describe, the root of the present-day idea of a monolithic Chinese threat stems from a combination of political-economic and national security aspects of US-China relations, i.e., trade and industrial policy.[20]

It is worth briefly recalling the late 1990s to help understand the US reaction to the rise of the Chinese ICT and telecommunications sector. [21] During this period, fledgling Chinese ICT companies set up mutually beneficial joint ventures with foreign partners where market access was exchanged for technology transfers.[22] The CCP acted to bolster Chinese national champions for the domestic market to relieve dependence on foreigners

[20] This work's focus on the civilian USG implies that geo-strategic concerns of military regional expansion in Hong Kong, Taiwan, and the South China sea are set aside.

[21] Chinese mercantilism on the other hand dates to the 1800s during the opium wars (Subramanian, 2011).

[22] The Chinese telecommunications market was highly competitive in the mid-1990s as emerging private firms and SOEs struggled to capture market share from their foreign counterparts. The Chinese demand was not sufficient to sustain the growing market as these domestic firms expanded outwards to remain competitive. Huawei, for example, was significantly engaged in international markets in the late 1990s and by the early 2000s, had contracts in Russia, eastern Europe, Africa, and Asia. It established cooperative arrangements with U.S.-based telecommunications and manufacturing firms such as Texas Instruments Inc., Lucent Technologies Inc. and Motorola Inc. By comparison, SOEs which were not export-oriented such as Datang Telecom Technology Co., were subject to a 94 percent profit loss in 2002 with the falling demand for phones in China (Bloomberg, 2021).

or better leverage technology transfers by taking advantage of the openness of global financial systems (Subramanian, 2011).[23] That said, while mercantilist policies are part of China's threat, this analysis focuses more on China's capacity to affect cybersecurity and critical infrastructure protection policy in the US. The idea of a Chinese threat facilitates distinct political and institutional regime convergence while involving trade, industrial, and national security policy. The range of policy problems outlined in this chapter reflects diverse political interests reacting to a Chinese ICT governance ecosystem, which involves tacit bargains with the Chinese state. As a result, IT trade heavily influenced US cybersecurity policy as a proxy battleground for geostrategic competition.

In the early 2000s, the USG recognized the Chinese threat but only alongside a lengthier threat litany dubbed earlier as 'all-hazards.' As previous chapters showed, much of the cybersecurity legislation revolved around critical infrastructure protection, creating a liability framework more conducive to threat-information sharing. For example, the PLA's modernization was noted but not overblown and never at the forefront (Clapper, 2011). Between 2009-2015, before Congress passed the Cybersecurity Information Sharing Act, distinct interest groups with separate motivations attempted to establish legislative cybersecurity frameworks to address 'all-hazards' threats. While the cyber institutions created during this era reaffirmed the pre-existing PPP structure and set the

[23] The President of the Information Technology and Innovation Foundation (ITIF), Robert Atkinson is a recurring issue-expert considered in this analysis. He argues the CCP's techno-mercantile policies have autarky as an end-goal for their economy. He contrasts a tension between the "Washington consensus" around what *competitive advantage* and the Beijing consensus on *absolute advantage* (Atkinson, 2012). This analysis discusses the distribution these ideas among interest groups in the synthesis section.

legislative and regulatory baseline for cyber-threat information sharing, political motivation did not focus solely on the Chinese threat.[24]

6.2 Overview of the China threat idea

Today, China's threat is a function of three distinct ideas that expanded the cybersecurity regime's institutional scope.[25] These ideas brewed for years and later provided a legitimating basis for regime expansion in the form of a whole-of-government response to Chinese ICT firms. Process tracing Congressional hearings uncovered vital distinctions between causal themes and their functions in promoting the overarching ideas. In tracing these foundational ideas on China's threat, we can explain how foreboding apprehension turned into whole-of-government implementation at critical regime junctures. The analysis will detail how characteristics of the Chinese threat evolved to induce differentiated levels of regime coherence, and integration as policy junctures evolved and institutional processes overlapped.

Figure 1 summarizes and expands the three implicit high-level ideas about China's threat and their associated causal themes. The three ideas are explicitly represented through sub-themes that provide the problem-formulation edifice supporting the overall narrative. Policy entrepreneurs have used these causal themes through various logical, empirical,

[24] Warning calls about Chinese ICT may have been unofficial at the time. In its reply to FCC WC Docket No. 18-89 *In the Matter of Protecting Against National Security Threats to the Communications Supply Chain Through FCC Programs* in June 2018, the Telecommunications Industry Association (TIA) referred to "specific suppliers in those countries that are believed to have ties with those governments" claiming that "quiet phone calls to major U.S. service providers [dates] at least as far back as 2010" (TIA, 2018).

[25] For this analysis, ideas combine an implicit problem-solution dyad. Themes are defined as the subcomponents of an idea providing evidentiary basis or causal association between the problem and its solution. The identification of a theme required two criteria, first the theme must appear in at least three separate hearings, second, the theme must provide causal elements essential to the problem-solution dyad.

and rhetorical devices to inform Congress and impact legislation.

The overall outline of this chapter follows the flow set in figure 1, which, for the most part, fits a chronological pattern from 2008-2020.[26] The description of causal themes proceeds from left to right in the next section. It should be noted that causal themes are additive. For example, the theme that Chinese ICT firms create supply chain dependencies presupposes that they are CCP-controlled untrustworthy.

6.2.1 Chinese ICT firms facilitate IP theft and are untrustworthy

The first idea presents Chinese ICT firms as untrustworthy based on their record of misappropriation of intellectual property and the lack of clarity surrounding their ownership structures. The thematic breakdown of this idea starts a series of causal claims serving to "poison the well" of Chinese ICT firms, where adverse information legitimizes more radical ideas in the future. Themes that associate Chinese ICT firms with abuses of human rights and the export of authoritarianism to developing nations appear later in the decade and are discussed in the final iteration of the China threat idea.

[26] A few exceptions to this rule were necessary given that logical and categorical fits were given priority over the order in which ideas appeared in Congress and elsewhere. Lumping together certain causal themes was necessary to maintain consistency in the overall narrative. For example, [insert example of lumping] [example of generalization] Chinese ICT firms' *opaque corporate governance structures* is only relevant in the context of Huawei but generalized across all categories of Chinese ICT firms and was included in the first idea.

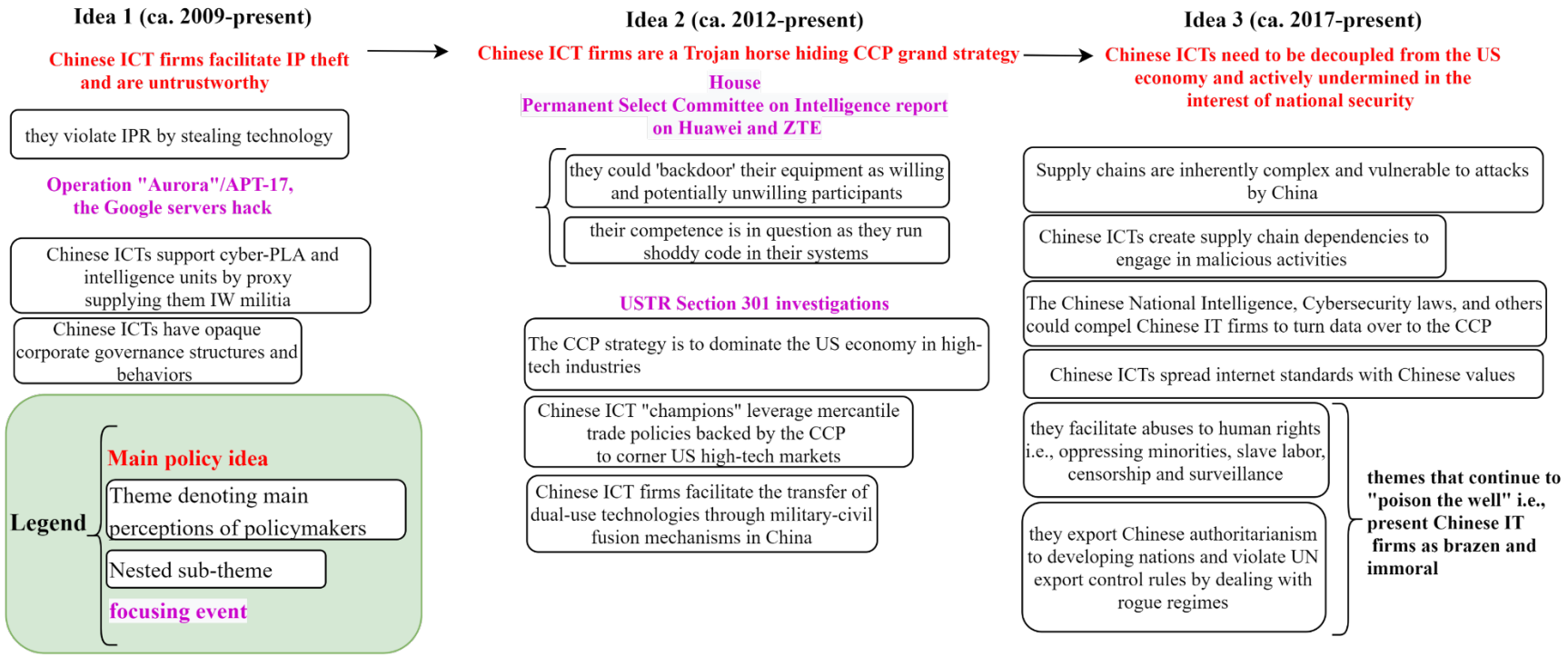


Figure 7: Evolution of ideas of a Chinese threat in the cybersecurity regime[1]

[1] For complete version refer to appendix.

6.2.2 Chinese ICT firms are a Trojan Horse hiding CCP grand strategy to dominate the US economy in high-tech industries through long-term and integrated mercantilist policies

The second idea presents Chinese ICT firms as a *Trojan horse hiding CCP grand strategy,* elevating them from mere economic competitors to a geopolitical battleground by proxy. This analogy draws on the ancient Homeric saga in that Chinese ICT's US market entry through equipment and information services are part of a CCP grand strategy to dominate the US economy. The relevant themes are listed below and systematically addressed in the USG policy response at critical regime junctures. The themes first involve an amalgamation of Chinese firm types:

- *Most Chinese firms, including SOEs, publicly-listed private firms operating through VIEs, and other structures like "employee-owned" hide CCP strategy. All Chinese capital is a tool of CCP strategy. Military and economic CCP goals are complementary.*

Causal themes then subdivide between those addressing Chinese FDI and those about inbound US capital and domestic Chinese market dynamics. In the former category, themes include variations on Chinese mercantile policies:

- *The CCP props up Chinese ICT firms as national champions and uses them to corner global markets.*
- *They use aggressive pricing (in the rural US and the developing world), unfair subsidies, and are backed by the state.*

In the second category, the lack of reciprocity towards inbound US capital is highlighted:

- *The CCP uses opaque ownership and licensing restrictions and the siren-song of its domestic market to promote its technology transfer goals*

As for domestic Chinese market dynamics, the relevant themes include so-called Chinese military-civil fusion (MCF)[1] and information sharing dynamics:

- *Chinese ICT firms have porous boundaries with cyber-PLA and intelligence units, supplying IW militia that supports the PLA by proxy.*
- *Chinese ICT firms facilitate the transfer of dual-use technologies through MCF mechanisms, i.e., a coordinated knowledge transfer system between political ministries, PLA cyber-units, research universities, national grant programs, and returning US-educated Chinese students.*
- *Chinese authorities have established engineering research centers, enterprise-based technology centers, state laboratories, national technology transfer centers, and high technology service centers to facilitate the Introduction, Digestion, Absorption, and Re-innovation of foreign intellectual property and technologies (IDAR).*

[1] Commercial-military integration, military-civil fusion, and civil-military integration are all used synonymously depending on the referred source.

6.2.3 Chinese ICT firms need to be decoupled from the US economy and actively undermined in the interest of national security

The third and final idea is that *Chinese ICT firms need to be decoupled from the US economy and actively undermined in the interest of national security*. While this third idea predated the Trump administration, it latched to a political environment of protectionist policies and animosity to China that tied the overarching narrative together and became synonymous with the solution to countering China's threat. The analysis will show how ideas and causal themes evolved to provide a legitimating basis that weaved various political interests together in a unified public interest national security rationale. While leveraged for different purposes by regime actors, this rationale helped converge the regime as it helped implement comprehensive and radical legislation to counter China. The themes of the final idea subdivide into two categories. The first themes follow an "appeal to motive" pattern whereby Chinese firms are aligned with the CCP. They are:

- *Supply chains are inherently complex and diverse. They are therefore vulnerable to attacks by China.*
    - *Chinese ICT firms create supply chain dependencies to engage in malicious activities (detailed in previous ideas).*
- *The Chinese National Intelligence, Cybersecurity laws, and others could compel Chinese ICT firms to turn data over to the CCP.*
    - *They could 'backdoor' their equipment as willing and potentially unwilling participants.*

- *Their competence is in question as they run shoddy code in their systems.*[2]

The second category continues a previous pattern of themes that "poison the well" of Chinese ICT as brazen and immoral agents. They are:

- *They export Chinese authoritarianism to developing nations and violate US/UN export control rules by dealing with rogue regimes (Iran & DPRK).*
- *They facilitate abuses of human rights, i.e., oppressing minorities, slave labor, censorship, and surveillance.*

As the final iteration of the China threat idea, decoupling from and actively undermining Chinese ICT now represented a robust rallying cry for the different political interests and created a legitimating basis for regime convergence.[3] While initially emerging from loud, peripheral voices in the regime, it later achieved mainstream bipartisan consensus during the Trump administration, which overtly leveraged the logic of threat-politics.

The following section analyzes the origins of the first China threat idea. The first part details how ideas transferred from military circles to civilian governments. Following that, the analysis outlines the causal themes used by policy entrepreneurs to provide an

[2] This theme applies to the third idea in the context of supply chain security but also to the first idea as it serves to "poison the well" of Chinese ICT firms.

[3] The inflection points between the second and third idea is subtle as both are predicated on logically additive causal themes that involved different policy responses. The distinction is made clear when considering whole-of-government practices and the political economy of 5G telecommunications and the semiconductor supply-chain in juncture 2.

evidentiary basis for articulating the problem, limiting evidentiary sources to the most representative manifestations.[4]

6.3 First Idea: Chinese ICT firms facilitate IP theft and are untrustworthy

An overarching question debated among US policy experts today is whether the CCP follows a cohesive and integrated whole-of-society approach that includes the Chinese private sector in their pursuit of great power competition. This idea has its origins in a 2005 Rand Corporation report commissioned by the US Air Force to examine Chinese ICT firms. Rand Researchers conceptualized a Chinese defense-industrial paradigm called the "digital triangle" (Rand, 2005).[5] This triangle comprises growing Chinese ICT firms, state Science & Technology (S&T) and Research & Development (R&D) funding, and finally, the People's Liberation Army (PLA). Through this digital triangle, Rand argued that four 'major players' of Chinese ICT firms were benefiting from the military supply chain (procurement, acquisition, R&D) by process of "civilianization," which introduces the profit-seeking motive to boost the military's IT readiness via public contracts (Rand, 2005).[6] Rand claimed this techno-nationalist behavior 'fuses' the centralized governance structure of the CCP with the nimble and dynamic market-forces of IT firms. The Rand report connected the telecommunications firm Huawei with the

[4] For an itemized mapping of ideas to policy experts in congressional hearings refer to the appendix

[5] This idea later contended with what Northrop Grumman put forward in a report to Congress as a "hybrid defense industry". This notion is arguably more accurate than Rand's reductionist approach to describing China's defense industry which was modelled after the US DIB. In the interest of objectivity, the "digital triangle" will later be revealed as overly reductionist given that one of the major IT firms, Juling, collapsed a year after the reports' publication and that other, more complex Chinese financial governance dynamics seem to explain the relationship between Chinese ICT firms and the CCP.

[6] Civilianization" serves as a precursor to civil-military fusion which was elaborated in more detail at a later stage.

PLA by associating the company CEO's military career with the "civilianization" processes. 'Civilization' and military-civil fusion are part of the second idea, i.e., Chinese ICT firms are a Trojan horse hiding a *CCP grand strategy*. Overall, the Rand report was seminal in formalizing the US military and defense establishment's wariness of Chinese ICT, a precursor to many themes and ideas yet to come. The genesis of the ideas and themes eventually transferred to the civilian government through Congress and the US-China Commission.

The first two ideas that *Chinese firms are* untrustworthy and *Chinese ICT firms are a CCP Trojan horse* co-existed throughout the 2010-2020 period, primarily as the securitization of IP and standards unfolded. Both ideas evolved into a more radical formulation in the third idea that tied the narrative together and mobilized a coherent, whole-of-government political response to China's threat by targeting their IT firms.

Early in the decade, Congressional reports on foreign cyber threats and IP theft were abundant. Concerns over alleged Chinese penetrations of private and public networks intensified as organizations voluntarily provided media disclosures of successive incidents.[7] What was once the purview of the military was now encroaching on various civilian government and industry sectors.

As early as 2009, Chinese IP theft was linked to a broad network of state-backed Chinese entities, among them IT firms. During this period, Congress started associating cases of IP theft with Chinese ICT firms whose trustworthiness was rapidly decreasing. This

[7] As the Northrop Grumman report notes, the media's portrayal of Chinese cyber penetrations as "advanced" was hyperbole as many victim organizations were simply ill-prepared (US-China Commission, 2012).

theme also laid the foundation for claims of porous boundaries between Chinese ICT and the Ministry of State Security (MSS). In a U.S.-China Economic and Security Review Commission hearing, commissioner Wortzel attributed network exploitation attempts on Google servers in Chinese universities to various institutional and individual Chinese actors.[8] Testifying experts presented state elements as coordinated and distributed between the Ministry of State Security, the Public Security Bureau, and the Chinese Communist Party organizations such as the Party's Central Propaganda Department.[9] Commissioner Wortzel noted that not all Chinese cyber espionage activity is conducted by government intelligence. Such activity is often proxied through a coordinated network of entrepreneur and militia hackers.[10] By stealing valuable intellectual property (source code) while obtaining access to the Gmail accounts of activists involved in human rights issues, Operation Aurora, also known as Advanced Persistent Threat (APT) 17, later reinforced the theme that Chinese ICT firms support espionage operations by proxy.[11]

[8] Created by the US Congress in October 2000, the U.S.-China Economic and Security Review Commission, (henceforth referred to as the US-China Commission), is mandated to produce annual reports to Congress and provide recommendations based on testifying issue-experts on the national security implications of the bilateral trade and economic US-China relationship.

[9] In this report, commissioner Larry Wortzel first distinguishes three distinct types of intents behind Chinese cyber operations: "Those that strengthen political and economic control in China; those that gather economic, military or technology intelligence and information; and those that reconnoiter, map and gather targeting information in U.S. military, government, civil infrastructure or corporate networks for later exploitation or attack" (The google predicament, 2010). As evident in this typology, OCOs are in essence intelligence operations that target corporate US networks and civilian network infrastructure and US military networks indiscriminately.

[10] VeriSign's iDefense intelligence service had claimed the attacks were perpetrated by undetermined proxies of the Chinese state (Paul, 2010). The Whistleblower site WikiLeaks similarly disclosed how "The Google hacking was part of a coordinated campaign of computer sabotage carried out by government operatives, private security experts and Internet outlaws recruited by the Chinese government" (NY Times, 2010).

[11] In 2017, the white-hat hacker group Intrusion Truth identified a connection between the MSS and four Chinese ICT companies (ZDnet, 2019; CFR, 2021). The group had also previously allowed DoJ to indict

That way, a monolithic Chinese threat was built on the technical difficulty of attributing and demarcating the origins of cyber attacks. The assumptions prevailed as attribution capabilities later gained more precision.[12]

In June 2011, the Recommendations of the House Republican Cybersecurity Task Force published its report. The recommendations notably lacked overt references to specific Chinese cybersecurity threats, including links to CCP grand strategy.[13] Instead, the report focused on presenting a political need for a public-private information-sharing framework to improve cyber defenses through security incentives and the use of targeted regulations around critical infrastructure. The lack of overt references to China corroborates the thesis that the regime had up to that point mainly been focused on gaps in the information sharing environment and bureaucratic competition between the DHS and other agencies, as described in the previous chapter.

In March 2012, Northrop Grumman Corporation prepared a special report for the US-China Commission.[14] The report delivered a theoretical threat analysis on Chinese ICT based on the open-source record and provided many themes that would become

---

members of APT 3 and APT 10 by identifying the Chinese Internet security firm affiliated with the hack (DoJ, 2017).

[12] The previous chapter discussed the cyber threat information sharing environment from PPD-8, the lead up CISPA and eventual passage of CISA which granted certain immunities to firms engaging in systematic information sharing. Commissioner Wortzel and the Internet Security Alliance discussed potential anti-trust exemptions for private sector firms sharing CIP information suggesting reforms in the ISE are also partially motivated by foreign nation-state actors.

[13] This finding is notable since the House Permanent Select Committee on Intelligence (HPSCI) investigation was being conducted in parallel that year. The Task Force report does not mention the threat of Chinese ICT despite including a member of the Permanent Select Committee on Intelligence as an author in the report.

[14] "Chinese Capabilities for Computer Network Operations and Cyber Espionage"

prevalent. Notably, the report asserted that future strategic partnerships between U.S. and Chinese firms in IT security would pose no more significant threat to network security or overall national security than any other IT partnership.[15] The Northrop Grumman report provides a marked separation between the first category of threat ideas, i.e., Chinese ICT firms should not be trusted, from the more radical position that presents them as national security threats.

However, a more radical stance emerged as IP theft issues started converging with national security concerns. In a hearing before the Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies of the Committee on Homeland Security in March 2013, Ranking Member Yvette D. Clarke (D-NY) presented cybersecurity as "the most prominent national security issue" faced in the 113th Congress and going forward (Clark, 2013). This declaration echoed the Director of National Intelligence's Annual Threat Assessment to Congress, which named cybersecurity the top threat to the US in 2012.[16] In that same hearing, the President's National Security adviser singled out China as the "place where cyber intrusions are emanating on an unprecedented scale" (Meehan, 2013). Mandiant Corp., which was present in the hearing, contributed to the Obama administration's elevation of the Chinese threat's priority by providing details of specific Chinese military units responding to IP theft.[17]

---

[15] In November 2011, the joint venture between Huawei Shenzhen Technology Company Ltd and Symantec, Inc. dissolved after four years of operations, with Huawei acquiring Symantec's portion. This should be noted as the last joint venture of the decade between a Western information security firm and Chinese high technology company at the time of writing.

[16] The report presents the position of entire US intelligence community (IC).

[17] The first major exposition of Chinese-based IP theft was released in the Ghostnet report 2009 (Deibert, 2009). A few years later Computer security firm McAfee documented in 2011 operation *Night Dragon*, an APT attributed to China against petrochemical companies. In February 2013, Mandiant the first APT1

Chinese IP theft was thereby associated with a predominant and severe cybersecurity threat (Alexander, 2012).[18] The theme of IP theft and the securitization of IP generally remained strong throughout the decade. A well-founded Congressional consensus held that Chinese entities siphoned off extensive economic and industrial data through espionage. However, congressional discourse amalgamated the theft of classified military secrets with indiscriminate, large-scale data exfiltration attempts, which targeted anything from widget factories to large financial networks (Halbert, 2016).[19] This tendency is indicative of how the securitization of IP would later contribute to the trend of cyber-threat-politics.

The second theme presents Chinese ICT firms as untrustworthy because of their *opaque corporate governance structures and behaviors.* This theme was set by the Investigative Report by the Permanent Select Committee on Intelligence chaired by Rep. Mike Rogers

report identifying the PLA's cyber espionage division referred to as Unit 61398 as one of approximately 20 groups targeting intellectual property from global private sector firms. Verizon's 2013 *Data Breach Investigations Report* concluded that one-firth of data breaches in their data set comprised efforts at IP theft and that 95% of those industrial espionage cases were attributed to threat actors in China (Verizon, 2013).

[18] General Keith Alexander famously referred to Chinese IP theft as the "greatest transfer of wealth in history" (Rogin, 2012).

[19] The impact of Chinese IP theft remains a contentious topic. While General Keith Alexander famously proclaimed regarded Chinese IP theft as "the greatest transfer of wealth in history" the true value of IP theft remains hard to measure due to the complicated nature of measuring trade in IT services, the indirect effects on US employment and innovation (IP Commission Report, 2013). A notable example of military IP theft involves Chinese targeting of U.S. Air Force's Joint Strike Fighter (also known as the F-35 Lightning II) project at Lockheed Martin. Despite similarities between the Chinese J-20 and the F-35, the Chinese espionage operation's overall success remains unclear. According to Libicki et al., (2016) reverse engineering hardware acquired from Russia may have been more effective for the development of advanced Chinese fighter jet programs. As for the private sector, many firms have historically underreported data breaches and IP theft for fear of reputational harms. Further, as China's economy gets bootstrapped by forced technology transfers, the ensuing growth in consumer purchasing power on the Chinese and US side is seldom reported in accounting figures.

(R-MI) on the U.S. National Security Issues Posed by Chinese Telecommunications Companies Huawei and ZTE.[20]

6.4 Second idea: Chinese ICT firms are a Trojan horse hiding CCP grand strategy to dominate the US economy in high-technology industries using integrated mercantilist policies

This section introduces the relevant critical regime junctures motivated by China's threat. These junctures represent coherent solutions by the USG (the third idea and policy solution) that emerged to respond to the Chinese Trojan Horse (the second idea and policy problem).

6.4.1 A note on critical policy junctures

Chapter 4 detailed how critical policy junctures are historical conceptions whereby a specific interplay of ideas, interests, and institutions accounts for swift, all-encompassing changes in outcomes. While these junctures do not constitute clearly defined events such as individual cybersecurity legislation, they can be regarded at a higher level of analysis as the product of a sequence of events traced and synthesized until a causal mechanism for an outcome emerges.[21] Observable regime outcomes at these critical junctures are contextualized as per the dependent variable, i.e., whether the distinct departure in USG policy (the junctures) presents a convergent or divergent regime trajectory.

From this perspective and comprehensive analysis of the Congressional Record, the cybersecurity regime enacted policy solutions through institutional alterations and expansions at two distinct critical junctures. The first involves *ad hoc* defensive and

[20] Not to be confused with Ranking Member of the House Armed Services Committee Rep. Mike Rodgers (AL-R).
[21] In other words, until data saturation was reached, and the evidence was repetitious.

offensive responses, and the second includes efforts to integrate disparate policy solutions in a whole-of-government approach. The following section describes the first juncture as a series of defensive and offensive measures coherently designed by the USG to respond to China's threat. These measures are manifest in institutional expansions of pre-existing authority and legislative amendments.

6.4.2 Juncture 1: The USG mounts a coherent defensive and offensive response to a Chinese Trojan horse by securitizing IT trade

The first juncture presents defensive and offensive regime measures as motivated by various ideas about China's threat, including sub-themes and their patterns of association. The defensive blocking of inbound Chinese capital centers around a coordinated response of multiple USG agencies and independent regulatory authorities, including the DoC, the DoJ, and the FCC. After Congress legislated defensive measures, offensive measures soon followed with DoC's new export control legislation. The analysis will track how specific ideas, i.e., themes of China's threat, motivated institutional expansion of pre-existing authority and legislative amendments. The following section addresses how specific themes morphed Chinese ICT firms' untrustworthiness into a *Trojan horse hiding CCP grand strategy.* Given perceived institutional gaps, the analysis details how this idea and its associated themes motivated the FIRMMA expansion and other defensive measures.

6.4.3 A coordinated defensive response to Chinese national champions centering around the Committee on Foreign Investment in the US (CFIUS)

The Committee on Foreign Investment in the US (CFIUS) was created in 1975 to investigate and determine whether incoming transactions may compromise national security through their affiliation to a foreign government (CSR, 2018; 2021). National

security concerns within the purview of CFIUS have traditionally involved acquisitions or majority ownership of US firms that holds special significance to the military because of an ongoing contractual relationship or sensitive intellectual property. Today, CFIUS acts as a multi-agency statutory committee chaired by the Treasury Secretary and includes the input of multiple coordinating agencies. CFIUS follows a similar mandate to its sister committee at the FCC, Team Telecom.

Starting with the Foreign Investment and National Security Act of 2007 (FINSA), Congress refined the CFIUS mandate from a procedural standpoint while maintaining a relatively narrow regulatory scope (DoS, 2008).[22] FINSA included transparency requirements and Congressional oversight, setting a legal precedent for concerned private sector entities and allowing them to preempt investigation by proactively reaching out to CFIUS. These requirements established a direct line of communication between the private sector and the inner workings of government before the committee sends final recommendations to the President for adjudication. Despite these transparency requirements, a distinct pattern emerged whereby Chinese investments often failed to assuage CFIUS concerns through any mitigation measure satisfactorily.

In 2008, CFIUS blocked Huawei from acquiring and merging with American network manufacturer 3Com. Despite partnering with American private investment firm Bain Capital, Huawei had to withdraw its offer after they failed to agree to mitigation terms with CFIUS over the acquisition of 3Com. The networking firm had supplied Intrusion Prevention Software (IPS) to DIB firms (Jackson, 2018; Mulligan, S. and Linebaugh, C.,

[22] For a detailed review of FINSA expansion as motivated by the Dubai ports controversy, see *The Committee on Foreign Investment in the United States (CFIUS)* by the Congressional Research Service (CRS, 2018).

2021). The 3Com deal generated bipartisan criticism by drawing on the “civilianization” of the Chinese military, as the Rand report had uncovered just a few years earlier. The USG now regarded Chinese ICT firms like Huawei to be central to that process.

After the blocking of the 3Com-Huawei merger, Senator Charles “Chuck” Schumer proposed expanding the CFIUS mandate to block the foreign acquisition of companies in “economically strategic areas” (New York Times, 2008). By rejecting Senator Schumer’s proposal, the Department of the Treasury (DoT) was still drawing clear boundaries between economic security and national security at the time. However, evidence of CFIUS weariness with Chinese mercantile practices dates since at least 2012. When asked whether Chinese FDI is treated differently from other countries, former CFIUS-lead and Deputy Assistant Secretary of the Treasury Nova Daly conceded that they afford particular focus to Chinese-based FDIs (US-China Commission hearing, 2012).

In February 2010, CFIUS blocked Huawei’s attempted acquisition of the server virtualization firm 3Leaf (Reuters, 2011). A red flag was raised as 3leaf owned patents on Quality of Service (QoS) management processes in virtual servers, a manifestly commercial application of technology in a highly competitive market at the time (PTO, 2010). However, the benign nature of the transaction did not stop Senators Jim Webb (D-VA) and Jon Kyl (R-AZ) from warning that the sale 3Leaf to Huawei "could pose a serious risk" to America's national and economic security (Sens. Webb, Kyl, 2011). The Senators also cited Huawei’s “well-established” ties with the PLA and the fact that Huawei was transferring “advanced U.S. computing technology” to China (Ibid).

In an August 2010 letter by a group of Republican representatives addressed to the Director of National Intelligence, the Treasury Secretary, Commerce, and Administrator

of General Services, Huawei's planned bid to supply equipment to Sprint Nextel Corp was similarly flagged. The letter combines all the themes of the first idea and emphasizes the "troubling" connection of the firm's founder to the PLA as outlined in the Rand report. The letter adds the novel theme that Huawei receives "substantial financial assistance from the Chinese government," consolidating the idea of Chinese firms as a Trojan horse of CCP strategy.

6.4.4 From techno-nationalism (2012-2017) to digital mercantilism (2017-present)

The US government and its IC provide information regarding sources of potential threats in the supply chain space (Castro, 2012). Early in the decade, the intelligence community prioritized determining whether relationships existed between a supplier and a foreign intelligence service instead of relying on whether a product had a foreign provenance (GAO-ODNI and NSA representatives). However, throughout the federal government, IT governance lacked a coherent response plan for addressing supply chain risks, a problem called out in the IT Supply Chain Security hearing as early as 2012 (Stearns, 2012). The GAO uncovered how civilian branches such as the DoJ, the DoE, and the DHS had made limited progress in accounting for supply chain risks compared to the DoD. In that hearing, China was not mentioned as a threat leveraging supply-chain-related vulnerabilities. However, the military and intelligence community maintained their stance.[23] Congress was also poised to act. Sec. 6004 of the "Spectrum Act" prohibited

[23] In its 2011 "Annual Report to Congress on Military and Security Developments Involving the People's Republic of China", the Department of Defense stated that, "China's defense industry has benefited from integration with a rapidly expanding civilian economy and science and technology sector, particularly elements that have access to foreign technology. Progress within individual defense sectors appears linked to the relative integration of each, through China's civilian economy, into the global production and R&D chain (…) Information technology companies in particular, including Huawei, Datang, and Zhongxing,

'barred' entities from participating in certain activities under FCC authority. According to the TIA, Congress intended to prohibit Huawei or ZTE from formally participating in FirstNet; i.e., receiving FirstNet and state implementation funds, participating in a spectrum auction, or receiving a grant[24]

The House Permanent Select Committee on Intelligence (HPSCI) report in October 2012 was a radical departure in the US IT trade and cybersecurity posture. It implied that any ownership or provision of telecommunications hardware and ICT services with a Chinese origin constitutes a *de facto* breach of national security.[25] The report demanded the exclusion of Huawei and ZTE's equipment from federal systems and contractors.[26] The private sector was "strongly encouraged" to refrain from transacting with both firms. The HPSCI report first linked a Chinese Trojan horse idea with IT decoupling as a necessary policy solution to enhance US national security. This connection accounted for the validity of targeting Chinese ICT firms as a policy response.[27] However, while the report

maintain close ties to the PLA (H.R. 4747, 115th Congress)." After the Pentagon report, the DoC barred Huawei in September from participating in FirstNet as part of a nation-wide public-safety wireless network for first responders stating they were a "security concern" (Kan, 2011).

[24] The "Spectrum Act" was a spectrum reform provision incorporated into Sec. 6004 of the H.R. 3630 (112th): Middle Class Tax Relief and Job Creation Act of 2012.

[25] The CAA of 2017 requires the Inspector Generals of multiple branches of the civilian government to conduct acquisition audits to ensure risks of cyber intrusion associated with hardware manufactured, directed, or subsidized by China among others are mitigated.

[26] While it could be argued that the report makes a reasoned claim that sensitive federal networks should avoid the inclusion of Chinese-owned hardware to hedge against advanced forms of supply chain compromises, the proposed solution legitimized the idea that Chinese ICT was fundamentally untrustworthy across-the-board, paving the way for specific targeting.

[27] The report also further consolidated older "poisoning the well" ideas that combined the untrustworthiness of Chinese ICT firms with their use as a CCP Trojan Horse. For example, the report recommends the US "view with suspicion the continued penetration of the U.S. telecommunications by Chinese technology companies" (Rogers, 2012).

urged CFIUS to block any FDI from Huawei and ZTE to the US, the need for coherence between the defensive measures lobbied for and the later use of export controls as an offensive foreign policy tool was not yet made salient. The interplay of ideas and causal themes over US-China trade dynamics had yet to impact the regime. Overall, the HPSCI report was seminal as policy entrepreneurs often echoed its themes and evidentiary basis in Congressional hearings following similar patterns.[28]

In March 2013, the Commerce, Justice, Science, and Related Agencies Appropriations Act barred the DoC, DoJ, NASA, and the National Science Foundation from purchasing IT systems "produced, manufactured or assembled" by entities "owned, directed, or subsidized by the People's Republic of China."

Congress passed the CISA Act in 2015 as an imperfect solution to cyber-threat information sharing on an entirely separate front. As great power politics intensified between 2015-2020, the cybersecurity regime's main threat factor shifted from resilience in the face of 'all-hazard' risk to countering nation-state actors. As techno-nationalism paved the way for trade weaponization, the USG shifted ICT policy into the strategic domain.

The East-West institute defined techno-nationalism as: "Government policies or actions that directly or indirectly favor ICT products and services sold by companies headquartered domestically or in allied states over those headquartered in states seen as competitors or adversaries (Kuehn and McConnell, 2020)." The implicit question that

[28] The HPSCI report remains the only comprehensive Congressional review of Chinese ICT firms to date. The lack of any significant investigative update into Chinese ICT in the open record was decried by the Competitive Carriers Association (CCA) in FCC regulatory proceedings years later. This includes annual reports of the US-China Commission to Congress and the USTR Section 301 report.

presents itself when IT becomes closely associated with its national origin is whether suppliers headquartered in untrustworthy nations can be secure from influence by their host governments, either via binding domestic rules or direct tampering by domestic intelligence services. This ideas' implication is to 'weaponize' commercial IT trade competition in a way that only reinforces tendencies toward self-reliance, protectionism, and a state-centric model of Internet governance, i.e., techno-nationalism.[29]

In February 2016, the FBI published a list of *Best Practices in Supply Chain Risk Management for the U.S. Government*, in which it advises shifts from ties to foreign intelligence to "the location of a service provider" (FBI, 2016). The FBI advised identifying potential dangerous associations between telecommunications manufacturers and the domestic laws of foreign governments, which may allow the request of sensitive US-based information from equipment suppliers.

S.1635 of the 114th Congress enacted in December 2016 is an early example of how the USG used the inherent vulnerability of the global supply chain as a basis to explore country-of-origin restrictions on telecommunications equipment or services in federal networks. Relying on the IC community's annual Worldwide Threat Assessment series dated February 9, 2016, Sec. 707 of S. 1635 required the GAO to report on critical telecommunications equipment or services obtained from suppliers closely linked to leading cyber-threat actors, where China appears first on the list (GAO-17-688R). The bill and report defined what constituted a "close link" between a leading cyber-threat-

[29] The section on the political-economy of 5G describes how the rise in techno-nationalism was catalyzed by Trump-era exogenous politics i.e., an increase in nationalist and isolationist tendencies that undermine trust in the multilateral system.

actor and foreign suppliers.[30] Therefore, the two documents continued to transfer ideas from the IC to the federal government by broadening the national security threat rationale to foreign vendors, as first suggested in the HPSCI report.[31] For example, suspect foreign suppliers would 1) have ties to the military or intelligence forces of said actor, and 2) be the beneficiary of financial support of the usual mercantile variety, and finally 3) is incorporated or headquarters in the threat actor's jurisdiction.[32]

S. 1635 confirms how ideas diffused from the IC to other civilian branches by associating supply chain risks with a manufacturers' country-of-origin. While the statute's applicability was limited to foreign IT usage in US government networks, the overall risk tolerance for country-of-origin as a level of security analysis starts gaining traction because of how these specific ideas combined.

In late 2017, a leaked memo by a National Security Council member (NSC) Brigadier General Rob Spalding revealed the prevailing gravitas in Washington around 5G. Given the perceived severity of security threats and the need to keep up an ambiguous race with Huawei, now considered synonymous with the CCP, General Spalding wanted the government to build its own 5G network and rent capacity to private operators. He

---

[30] The term ''leading cyber-threat actor'' means a country identified as a leading threat actor in cyberspace.

[31] The Consolidated Appropriations Act of 2017 (H.R. 244) later that year would name China explicitly and create a country-of-origin security requirement by calling for an interagency audit to ensure no funds are used to acquire information systems with "any risk of cyber-espionage or sabotage associated with the acquisition of such system, including any risk associated with such system being produced, manufactured, or assembled (…) by entities (…) posing a cyber-threat including but not limited to, those that may be owned, directed, or subsidized by the People's Republic of China.

[32] The term ''closely linked'', with respect to a foreign supplier, contractor, or subcontractor and a leading cyber-threat actor, means the foreign supplier, contractor, or subcontractor— (A) has ties to the military forces of such actor; (B) has ties to the intelligence services of such actor; (C) is the beneficiary of significant low interest or no-interest loans, loan forgiveness, or other support of such actor; or (D) is incorporated or headquartered in the territory of such actor.

argued that the deployment of a nationalized network would "reflect[s] our [US] principles" (Graff, 2020). While promptly rejected by the FCC, this extreme proposal illustrated the extent to which great power competition with China underlay the US 5G telecommunications environment (Pai, 2018).

As the following section describes, the Section 301 hearings against China in 2017 were a significant inflection point in US trade policy and relevant to this analysis in two important ways. First, the hearings represent the pinnacle of the idea that Chinese ICT firms are a Trojan horse hiding CCP grand strategy. Second, while providing a comprehensive analysis of US-China competition in high-technology and industrial policy matters, the report was seminal in tilting trade policy into national security space.

6.4.4.1 The United States Trade Representative (USTR) Section 301 hearings

The USG has historically used Section 301 authorities to build cases and pursue dispute settlements as a last recourse that bypasses the WTO dispute settlement process.[33] The Trump administration claimed unilateral use of its statutory means on China due to a perceived inadequacy of the WTO rules and its dispute settlement procedures in addressing their mercantile trade practices.[34] The report follows a pattern familiar to other Congressional hearings whereby testifying experts regard *Chinese FDI* and *inbound US capital to China* from the standpoint of a coherent and integrated Chinese mercantilist

[33] Section 301 of the Trade Act of 1974 (19 U.S.C. §2411) empowers the USTR with authority to investigate and implement countermeasures against foreign trade practices that 1) violate U.S. trade agreements, 2) engage in acts that are "unjustifiable" or "unreasonable", and 3) that burden or restrict U.S. commerce (CSR, 2021).

[34] The Trump administration USTR initiated 5 other section 301 investigations.

policy.[35] In the category of *Chinese FDI*, practices that burden or restrict US Commerce include the state-funded strategic acquisition of US assets combined with cyber-enabled theft of US IP and trade secrets. In the inbound US capital to China section, the report broaches mercantile behaviors, including forced technology transfer requirements and discriminatory licensing practices.

The Trump administration initially leveraged the theme of IP theft to justify the initiation of Section 301, stating that Chinese "laws, policies, and practices (…) encourage or require the transfer of American technology and intellectual property to enterprises in China" (Section 301, p.4). The final USTR report provides a practical example of how the USG perceives the CCP's grand strategy, including its implicit account of the Trojan horse idea. The strategy aims to displace US global industrial leaders "so that China may achieve global market dominance" (Section 301, p.47). The CCP aims to achieve its goal of dominating the US economy in high-technology industries through an integrated mercantile doctrine that combines strategic outbound investments (the Trojan horse) coupled with complementary MCF practices in the Chinese domestic market.[36] However, the narrative falls short of articulating an assumed end goal for the CCP. After the CCP achieves import substitution, i.e., when it replaces foreign suppliers with domestic

[35] The evidence used in the final report includes expert testimony, Chinese policy documents, and a record of US-China economic transactions.

[36] The CCP is reported undergoing the convergence of long-term, state-led industrial policies, from the *National Medium- and Long-Term Science and Technology Development Plan (2006-2020) (MLP),* the *State Council Decision on Accelerating and Cultivating the Development of Strategic Emerging Industries,* to the Made in China 2025 (MIC) policy. The MLP outlined a strategy of import substitution to be achieved through the Introduction, Digestion, Absorption, and Re-innovation of foreign intellectual property and technology (IDAR), a foreign technology transfer policy whose support continues with Xi Jinping's tenure. The MIC similarly preserves the arc of the CCP grand strategy by reaffirming the state's central role in economic planning and calling on a whole-of-society approach to achieve 70% self-sufficiency in strategic industries like telecommunications by 2025.

Chinese ones, it remains unclear whether the USTR regards the CCP as aiming to shift its trade balance towards autarky in all sectors of the economy or strictly in those 'strategic emerging industries.'[37]

As per the Chinese FDI category in figure 6, most global Chinese firms and investments are considered CCP intermediaries to transfer technology and dominate the US economy in high-tech industries.[38] A minority of hearing participants argued that market considerations drive Chinese FDI in the US instead of a grand CCP strategy. The USTR regarded these dissenting opinions as "not persuasive (USTR, p. 149) ." As a centrally managed economy, the report concludes that the Chinese state plays a "vital role in shaping and facilitating outbound investment activity." The USTR committee qualified most Chinese transactions as aligned with state objectives. The report describes many Chinese companies in the US operating at a loss and negatively impacting the US competitive environment given indirect CCP subsidies.[39]

As a planned economy, the CCP supports Chinese national champions by controlling development banks and sovereign wealth. Given this economic reality, the assumption put forward is that the CCP can direct their national 'champions' on the qualities of their

[37] China recognized strategic technologies in the 2010 Decision on Accelerating the Cultivation and Development of Strategic Emerging Industries (SEI Decision).

[38] The report itself does not single out IT firms. However, the notion of "state-sponsored" cyber intrusions implicitly targets Chinese ICT firms where the evidence of sponsorship put forward is extensive state support. The fact that Chinese national champions are globally competitive IT firms preserves their status as a Trojan horse. This status is maintained regardless of organizational structure (SOEs, private firms, or any form of "state-backed" enterprise).

[39] However, the assumption that Chinese firms are operating at a deficit often relies on imperfect measurements exacerbated by Chinese mercantilism. Within the WTO framework, antidumping measures are allowed after procedure determines "material injury" by calculating the "normal" value of a good through marginal cost and revenue. This calculation is based on comparing Chinese production costs with that of an equivalent nation (Krugman et al. 2018). Chinese mercantile practices distort data on Chinese goods and services with indirect subsidies, perpetuating a *de facto* assumption of foul play.

investments. Since many of the implementing firms happen to include SOEs, among others, this evidentiary basis is said to leave "no room for doubt concerning the role of the Chinese government (USTR, p. 149)." Even in cases where the government does not own a stake, such as private firms using Variable Interest Entities (VIEs), transactions appear to follow an almost pre-defined narrative. For example, the report notes that "(…) even when undertaken by companies in which the government does not own an observable controlling stake, the transactions identified are frequently guided and directed by the state (USTR, p. 103)."

The grand strategy narrative extended beyond the USTR. For example, in a statement to the U.S. Senate Subcommittee on East Asia, the Pacific, and International Cybersecurity Policy, the Senior Fellow and Director for the Center for Chinese Strategy at the Hudson Institute argued that China's leaders are continuing to implement a largely secret set of policy decisions made about 40 years ago for their regional plans. In response, he emphasized the need for a holistic approach, led by the President to "coordinate the Defense Department, USTR, Commerce, Treasury, and important elements in the State Department in designing new strategies to deal with the issues of trade, security cooperation, and multilateral coordination" (Pillsbury, 2018). The Department of State expanded this theme by assuming outbound and inbound capital flows as a unified Chinese strategy. For example, the Assistant Secretary at DoS' Bureau of International Security and Nonproliferation argued that certain Chinese entities must "ultimately take orders from the Communist Party" (*Chinese ICT firms are agents of the CCP)* and urged US firms to find the appropriate balance between the economic and strategic advantages of an open economy and the "allure of the Chinese market" (DoS, 2018). In a hearing

titled “Made in China 2025 and the Future of American Industry” on February 27, 2019, the President of the Information Technology and Innovation Foundation (ITIF) characterized China’s “innovation mercantilism” as outside the traditional framework of a welfare-maximizing, positive-sum game.

Another relevant example involves a Defense Innovation Unit Experimental (DIUx) report arguing that China “aims to displace the U.S. in key industries using its large market size to promote domestic champions which can become global leaders through state subsidies, access to low-cost capital, and limiting China’s domestic market access to foreign companies” (Brown, M. and Singh, P., 2018). [40] This theme invariably transferred to Chinese ICT firms. For example, knowing that ZTE and *Huawei* charged less than their competitors in rural Michigan implied they were not operating according to a profit motive. A policy entrepreneur in that hearing assumed this tactic allows the Chinese the ability “to collect vast quantities of information and to create leverage against adversaries in a potential conflict” (Keiser, 2018). As such, the reality of the Chinese economy renders the distinction between SOEs and private IT firms moot, given that they all contain a CCP element or influence. Further, according to the State Department, firms “aligned with Beijing’s industrial policy” were re-structuring transactions to bypass CFIUS’s jurisdiction (before the passage of FIRMMA) (DoS, 2019 Ashley Ford).[41]

[40] DIUx is a Department of Defense (DOD) unit that was established to foster a Silicon Valley technology innovation and business culture to the military.

[41] The claim put forward was those financial instruments such as Variable Interest Entities (VIE) were leveraged to allow Chinese private IT firms technology-access rights.

6.4.4.2 US outbound investments and domestic Chinese market dynamics

The themes outlined in this section complete the narrative of how the Trojan horse idea operates and are part of the mercantile practices described in the previous USTR section. After China's ascension to the WTO, "unfair" technology transfer requirements to inbound US capital persisted despite repeated commitments to the contrary (Section 301). The section 301 report argues these requirements have shifted towards informal restrictions in the guise of implicit *quid pro quos* for market access. The US Chamber of Commerce and other policy entrepreneurs have detailed how inbound capital to China is subject to technology transfer policies achieved through *ownership* and *foreign licensing restrictions* in defiance of the WTO regime. The USTR considers these practices to weaken US firms' competitiveness and stunt their investment in R&D. In the former case, foreign investors are only allowed to operate in key industries unless partnering with a Chinese firm.[42] In the latter, US capital is subject to administrative burdens imposed in selective and nontransparent manners. At the regional and local level, "thousands of other regulations, rules, and regulatory documents related to foreign investment (…) are issued by central government authorities, as well as a [sic] countless local government regulations and restrictions" (Section 301, p. 24).

The report sets a theme in which the Chinese government continues its use of *opaque ownership and licensing restrictions and the allure of its domestic market to promote its technology transfer goals (theme)*. A 'siren-song' metaphor was presented initially verbatim in the Rand report as denoting the "irresistible" allure of the Chinese market for

[42] China's system for administering inbound foreign investment is specified in the Foreign Investment Catalogue and a "negative list" for restricted industry areas.

US-based multinationals where market access is contingent on technology transfers. The 'siren-song' metaphor evolved in the section 301 hearings to portray the CCP as a mob boss that is "making an offer multinationals cannot refuse" (Section, p. 35). The evolution of this metaphor is revelatory of dynamics relating to inbound US capital to China. First, the CCP lures US firms into its domestic markets, where they sign a secret pact with the Chinese "mafia" in the form of equity or contractual joint ventures. Once the Chinese counterpart transfers the technology from the US firms, local producers can now produce near-equivalent products. In the final stage, Chinese SOEs (in cahoots with the mafia) are compelled towards local procurement, preventing US competitors and their superior products from competing fairly. As per the mobster metaphor, the report claims US firms were reticent to speak out, risking a loss of market access and "punishment by a powerful and opaque Chinese regulatory system" (Section 301). Finally, the USTR report parallels other hearings regarding civil-military fusion as a complementary policy to Chinese FDI to promote indigenous innovation.[43]

While more hawkish USG representatives may consider military and economic CCP goals isomorphic, the Trojan horse idea is not about a feared military takeover. Unlike the Homeric saga, it simply represents fear of an economic takeover designed to undermine the US edge in high technology industries.

6.5 Third idea: Chinese ICT firms need to be decoupled from the US economy and actively undermined in the interest of national security

[43] The State Administration for Science, Technology, and Industry for National Defense (SASTIND) is considered the domestic information sharing platform facilitating domestic knowledge transfers.

6.5.1 CFIUS's scope expands with FIRMMA 2018

Between October 2017 and March 2018, the USTR section 301 hearings legitimized a defensive response against inbound Chinese capital. The idea of a Chinese Trojan horse reached its apogee, and IT trade was now fully weaponized as "strategic technology." Given the strong techno-nationalism prevalent in Washington, Chinese FDI, particularly strategic technologies, represented most CFIUS reviews (Brown, M. and Singh, P., 2018). Given the urgent USG need to mount a coordinated response to the Chinese Trojan horse, CFIUS was the natural institutional pick to mount a defense as Congressional representatives earmarked it for reform. In a House Financial Services subcommittee hearing on December 14, 2017, the former Assistant Secretary for DoC's Export Administration described areas within the purview of the CFIUS mandate. These areas include "co-location issues, transactions that may involve espionage or security vulnerabilities, those that can reduce the benefit of US government investment, transactions that would reveal contain PII, those that create security and supply issues for DoD and other government agencies, those that would implicate law enforcement issues, and those that create exposure for the critical infrastructure such as telecommunications" (Wolf, 2017).

The Foreign Investment Risk Review Modernization Act (FIRRMA) passed the House on June 26, 2018, and was later enacted through the John S. McCain National Defense Authorization Act (NDAA) of 2019 on August 13, 2018.

Driving the Trojan horse point home, in a Washington International Trade Association conference, the Assistant Secretary of the Treasury and head of CFIUS justified the FIRMMA expansion based on "foreign governments using investments to meet strategic

objectives" (WITA, 2018). FIRMMA significantly broadened the purview of CFIUS to include all sectors of the economy compared to what used to be *ad hoc* considerations of capital transfers.[44] For example, Alibaba's attempted acquisition of MoneyGram International, a financial technology sector transaction, was blocked (IGP, 2020).[45]

However, setting aside the perceived need for increased defensive capacity was a political motivation as part of the impetus behind FIRMMA. CFIUS's blocking of strategic technology acquisitions predated FIRMMA. For example, CFIUS blocked Lattice Semiconductor Corp's acquisition by the Chinese investment firm Canyon Bridge Capital Partners in 2017 (Baker, 2017). It followed suit by blocking Singapore-based Broadcom from acquiring US-based Qualcomm in 2018. After the FIRMMA expansion, however, CFIUS interventions appeared to stretch the definition of strategic technologies to its limit.

The opaqueness and ambiguity of Chinese capital investments in domestic markets were perceived as aggressive tactics by the CCP to corner US markets with unfair mercantilism. Congressional hearings revealed how opaque Chinese FDI combined with a lack of reciprocity for US investments prompted calls for a more aggressive US posture by China hawks. For example, one extreme proposition debated in CFIUS hearings urged to add outbound US investments to China to its mandate as a buffer against the 'siren-song' effect of forced technology transfers through joint ventures (CRS, 2018). However,

[44] FIRRMA was passed through the John McCain National Defense Authorization Act 2019.

[45] Mueller (2018) argued the merger would have resulted in mutual gains and consumer benefit, first by expanding Alibaba's reach through MoneyGram's access to 200 countries, second by expanding Moneygram's portfolio to include the mobile payment space by combining with AliPay.

stark opposition from venture capitalists ensured FIRMMA would only cover inbound capital instead.[46]

The impetus for FIRMMA appeared to be partly motivated by a bargain between China hawks in Congress and the Trump administration's isolationist trade stance. At the start of the Trump administration's trade war with China, officials at DoT and DoC were concerned that the Trump administration would use IEEPA powers to apply a blanket restriction on Chinese FDI (WITA, 2018).[47] Around that time, the House Financial Services Committee and the US-China Commission were increasingly concerned with the rise of China as a foreign direct investor. The Assistant Secretary for International Markets and Investment Policy at DoT confirmed how the Trojan horse idea was operative, stating that FIRMMA was passed "based on two major trends, (…) the rise of China as a foreign direct investor and secondly (…) the issue of strategic technology" (WITA, 2018). Senator Crapo and Cornyn achieved this tacit arrangement, enabling FIRMMA to pass with a bipartisan Congressional majority and later lobbying the President to leverage FIRMMA instead of IEPPA powers to block suspicious Chinese FDI. At the same time, and as addressed in the next section, Sen. Royce and Engel were

[46] That said, the subsequent scope expansion was regarded as a positive step towards outright economic decoupling by some hardliners. China hawks such as Rep. Brad Sherman (D-CA30) presented his views on soft power in a hearing: "I, for example, am worried that the Chinese control a big chunk of the movie screens in the United States—AMC in particular. What that means is that if you make a movie that Beijing doesn't like, not only can't you get it shown in China, you can't get it shown in the United States… To give China control of the minds of Americans by controlling the media of the United States was a mistake that we can reverse, perhaps in this bill [referring to FIRRMA] (Govtrack, 2018*)."* The Trump administration took a different stance claiming that CFIUS would protect American jobs (The Hill, 2017).

[47] Seasoned public servants that were part of the Obama administration tacitly disapproved of the Trump administration's isolationist stance and can be regarded as aligned with group 1.

able to pass the first export control reform in decades as part of a coordinated effort to create a coherent USG response to China.

The expansion of CFIUS' mandate from strict national security investments to include economic-strategic investments furthered the securitization of IT trade based on an investment's national origins. The FIRMMA expansion was part of a coordinated, defensive policy response enacted due to a perceived institutional gap as the USG was faced with the need to address the CCP grand strategy to dominate the US economy in high-tech industries and political bargaining, as further highlighted in the section on the political-economy of 5G and the semiconductor supply chain.

Many USG concerns over Chinese FDI first highlighted in the USTR Section 301 hearings remain outside the official mandate of CFIUS. In a hearing titled *Risks, Rewards, and Results: U.S. Companies in China and Chinese Companies in the United States* in February 2019, Chinese firms, IT included, are described as indirectly subsidized since the state has been willing to absorb the losses that state banks incur on lending to their *Strategic Emerging Industries*.[48] The Public Company Accounting Oversight Board (PCAOB) had reported ambiguities that hampered their ability to attribute the source and quality of Chinese investments.[49] [50] For example, Chinese firms can list on the US stock exchange through VIEs but not *vice versa*. Chinese companies

[48] In many cases, the support has been provided by government-backed investment funds and development banks rather than through the official government budget, which complicates the case for legal trade action (Setser, 2019).

[49] Current US trade law allows trading partners to offset the impact of subsidies that can be proven to have a caused a material injury to their business. Chinese subsidies to domestic industries are not considered a violation of China's WTO commitments since the burden is in proving those subsidies.

[50] The PCAOB is part of the Securities and Exchange Commission (SEC).

are not subjected to the same quarterly disclosure rules in the US as US firms.[51] The PCAOB is also banned from doing inspections in China and cannot audit Chinese firms in the US due to the nature of VIEs. China regarded the accounting implications of Sarbanes-Oxley as an infringement on their national sovereignty. Since then, the SEC and PCAO initiated changes over the handling of general FDI from China after Congress passed the Holding Foreign Companies Accountable Act of 2020.[52] Such perceived gaps motivated further coordination between CFIUS, the Treasury, and DoJ after FIRMMA was passed and Team Telecom later formalized.

6.5.2 Offensive export controls complement the defensive measures

The section starts with a brief review of export controls as an institution. Export controls are a direct, offensive response to the threat of Chinese national IT champions such as Huawei and ZTE. It then explains new export control statutes and regulations through a political need for coherent institutional expansions. The unprecedented application of export controls whereby the USG opted to forgo its positive trade balance with China in the semiconductor industry in a quest to undermine Chinese ICT firms is outlined. Finally, the section explores how the USG framed its response to cyber supply chain threats, focusing on China.

[51] A policy initially designed not to discourage Greenfield investments due the doubling the number of regulations (home and foreign).

[52] The Holding Foreign Companies Accountable Act of 2020 amends Sarbanes-Oxley by promising to ban Chinese companies from US exchanges after three unsuccessful attempts to be inspected by the PCAOB. The ban will take place in 2023. Ownership disclosure requirements will become mandatory. These include disclosure of government ownership, whether the articles of incorporation contain the charter of the Communist Party, and the naming of CCP board members or operating entities.

After World War Two, the US military required export controls to remain technologically superior by ensuring adversaries did not offset their advantage via commercial acquisitions. However, the efficacy of export controls was fraught with contention as the balance between preserving national security without overly restricting US competitiveness abroad is often debated in Congress (CRS, 2018; Jackson, 2020).

The typical view on export controls pits military strategy, including defense and foreign policy, against economic considerations such as the US competitive advantage in high technology and maintaining a trade surplus. However, the more accurate view is less binary. In FY 1992, the Technology Reinvestment Project (TRP) was an extensive commercial investment program undertaken by DoD as an effort to promote the "Commercial-Military Integration (CMI)" of the commercial and military-industrial bases (Richardson et al. 1999). Its purpose was to enhance weapon systems' production efficiency through dual-use technology investments. The US also uses economic competitiveness as a direct instrument of national power and an indirect means to bolster national security through government tax revenue, innovation transfers, and synergies between the DIB and DoD (White et al., 1995; DoD, 2017).[53]

The Export Administration Act (EAA) of 1979 (US code 50 App. 2401-2420) regulated dual-use technologies from a statutory standpoint.[54] The EAA provided the legal

[53] For example, the Doctrine for the Armed Forces of the United States states: "Nations exercise their power through diplomatic, informational, military, and economic means (…) "As a nation, the US wages war employing all instruments of national power— diplomatic, informational, military, and economic (…) All forms of statecraft are important, but as the conflicts approach the requirement for the use of force to achieve that nation's interests, military means become predominant and war can result" (DoD, 2017).

[54] Dual-use technologies are US exports that are not strictly munitions but may have military applications. The EAA included a sunset provision that was bypassed for reauthorization in different administrations using the International Emergency Economic Powers Act (IEEPA) (Govtrack.us, 2021). The regulations

authority to control exports for reasons of national security or foreign policy.[55] The Export Administration Regulations (EAR) administered by the DoC's Bureau of Industry and Security (BIS) specified how the law was implemented by use of the Commerce Control List (CCL). The regulatory implementation of those controls was also fraught with jurisdictional disagreements and poor coordination between agencies. These problems caused delays, inefficiencies, and an inability to evaluate the controls' effectiveness (GAO, 09-310, 2010). Pressure by the business community to narrowly specify export controls lest they stifle US competitiveness abroad undermined any political consensus to enforce effective coordination between agencies (Brown, M. and Singh, P., 2018).

Dual-use exports involve technologies with both civilian and potential military applications (Fergusson & Kerr, 2020). Historically, the inherent tension between stifling early-stage technology and agreement over what technologies must be controlled led to poor implementation and incoherence.[56] The intersection of dual-use technologies and trade has been particularly problematic in the IT sector. For example, technologies like encryption were initially regulated as munitions (Diffie & Landau, 2010).[57] Before

---

meant to implement those statutes are the Export Administration Regulations (EAR).

[55] Items deemed as munitions are covered under the Arms Export Control Act (AECA) of 1976 (US code 22 titles 2571-2794) and implemented through the International Traffic in Arms Regulations (ITAR).

[56] Nuances in the definition of dual-use technology are often deliberately avoided at the statutory level. This functional statutory ambiguity leaves implementing regulatory agencies with the burden of providing a flexible interpretive criterion.

[57] Intelligence and law enforcement agencies pushed for curtailing domestic encryption and stopping its export for national security purposes. However, as economic incentives for the use and distribution of encryption grew in the newly privatized commercial internet, cryptographic libraries were differentiated and turned into a controlled dual-use export allowing broader civilian use. The computer industry had to version their encryption services into separate domestic and export compliant products. The EAR

Congress passed ECRA, the dual-use designation involved a process of diffuse responsibility in the USG. The DoS determined the dual-use status and transferred implementation to DoC's BIS as per the EAA. However, as the following section outlines, policymakers expanded the scope of export controls and designed them to cohere with defensive measures motivated by the need to beat China in the 'race' for strategic technologies and exogenous political considerations.[58]

6.5.2.1 The Export Controls Reform Act of 2018: statutory expansion of the dual-use designation

The Export Control Reform Act of 2018 (ECRA) and its implementation process presents ample evidence of increasing regime coherence motivated by China's threat. However, the ECRA's implementation also shows discrepancies between statutory intent and agencies' coordination over the controls' deployment. These anomalies reveal differences in the underlying interest groups with implications for regime integration.

The ECRA reform repealed the EAA of 1979 and broadened the legislative authority to implement dual-use export controls (Fergusson & Kerr, 2020).[59] Rep. Ed Royce, the original bill sponsor, claimed the reform would "reflect the realities of modern international commerce and the national security threats of the century we are in right now" (C-span, 2021). As described in Section 109, the bill aims to control for

---

requirement to "assess the foreign availability of equivalent products in deciding whether to grant or deny an export permit", contributed to lifting the controlled versioning of encryption services after it became clear that foreign customers were acquiring cryptography from non-U.S. businesses or developing their own regardless.

[58] Addressed in the second juncture.

[59] The relevant provisions were passed as part of the John S. McCain National Defense Authorization Act for Fiscal Year 2019. The interagency process is outlined in detail in the text of the ECRA bill.

"emerging" and "foundational" technologies that are "essential to the national security of the United States" (ECRA, 2018). While the reform could be regarded as motivated by the need to match changes in the evolving technology environment more broadly, a closer inspection of the bill presents the makings of an *ex-ante* technology control regime.[60] The definition of dual-use technologies is expanded and allows more flexibility in implementation. This expansion is achieved by adding the notion of "foundational information and know-how" to the law's scope, including "commodities, software, technology, and services" (ECRA, 2018).[61] The new law shifts control upstream of the innovation process by including the ambiguous provision of "emerging" technology as applying to software. In addition, it can now apply to foundational source code, a measure designed to dynamically preempt the transfer of any technology that may benefit US adversaries. With this reform, a bipartisan political consensus shifted the balance of export controls away from a pro-business US stance towards a more risk-averse position using a national security rationale that stemmed from the threat of China.

The Trump administration leveraged the vague statutory label of "emerging technologies" and paired it with an overly broad regulatory interpretation at DoC in an apparent effort to undermine Chinese ICT firms via hardware restrictions. After ECRA's passage in August, the BIS followed in November with a broad list of 14 "emerging technologies" proposed for regulatory control (Federal Register, 2018). To illustrate that

[60] The commoditization of industrial manufacturing supply has led to a downstream 'servitization' strategy whereby industries shift from a product offering into an integrated product and service offering. This ongoing change in commerce is an alternative hypothesis explaining the need for reform (Wise & Baumgartner, 1999).

[61] ECRA stopped short of including patents and "telemetry data".

policy's impact, in a Senate Committee meeting on Banking, Housing, and Urban Affairs titled *Export Control Reform Implementation: Outside Perspectives* on July 18, 2019, representative Patrick J. Toomey (R-PA) raised a concern on behalf of a manufacturer and supplier of piston-aircraft engines aiming to supply a Chinese Unmanned Aerial Vehicles (UAV) company with piston engines. Despite the obsoleteness of piston engine technology and that the strategic nature of UAVs is only relevant to the software and AI that powers them, that company's bid for a license to supply the Chinese firm was rejected by BIS.[62] As a testament to the strength of the China animus prevailing at DoC, representative Toomey was told by DoC that "an American company could not sell a screwdriver to the Chinese effort to build these UAVs"(Toomey, 2019).[63] Further, the former Under Secretary for Industry and Security at DoC reaffirmed doubts that any administration would ever change its controls policy should a US export be construed as contributing to the modernization of the Chinese military.

These examples further validate how the USG indirectly justifies an overly broad application of export control categories due to the perception of a monolithic techno-nationalist Chinese state where a cabal of commercial, defense, and intelligence interests seamlessly share information and coordinate activity to further CCP grand strategy.[64]

---

[62] As further indication of complicating factor of exogenous politics to IT export controls, UAVs, are still subject to legacy regulations part of the missile control regime which labels them as munitions. However, Air China can import from Boeing (a US national champion) with vastly more advanced technology for general aviation.

[63] After the Tiananmen Square massacre, Foreign Relations Authorization Act for FY 1990 and 1991 applies prohibited the sale of military or dual-use exports to the Chinese military. Public Law 101-246-Feb. 16, 1990.

[64] The lack of evidence for formal coordination between Computer Network Operation (CNO) teams and the PLA was first pointed out by the Northrop Grumman report. Any large state-based intelligence apparatus requires sophisticated bureaucracies and coordinative bodies to orchestrate efforts cohesively (Lindsay et al., 2015). Just as the US cybersecurity regime has been struggling with means to integrate its

Using the new ECRA authority, the BIS list amounted to a tit-for-tat response to China's MIC2025 and strategic technology targets (Daly, 2019). The Trojan horse idea portrayed a strong and coordinated CCP-led economy against which traditional mechanisms for ensuring fair trade were deemed inadequate. The USG's answer the lack of reciprocity is to adopt a series of tit-for-tat mercantile trade policies. As an exposed arm of CCP strategy, the Trojan horse of Chinese ICT makes an ideal target and effective motivator for a concerted USG response.[65]

6.5.2.2 The FIRMMA and ECRA reforms are designed to cohere

The ECRA requires the President to establish and lead an interagency process to identify "emerging critical technologies" that are not identified in any previous list, thereby establishing a broad coordinative basis for the relevant agencies to leverage (CRS, 2018). Both FIRMMA and ECRA were designed from the ground up to achieve a coherent US response in tandem. In a Senate Committee meeting on Banking, Housing, and Urban Affairs titled *Export Control Reform Implementation: Outside Perspectives* on July 18, 2019, Chairman Crapo stated that "these two important, hugely bipartisan bills [FIRMMA and ECRA] were intended, in no small part, to ensure that with proper controls in place to establish highly guarded inward and outbound regimes, a productive relationship between the US and China is not only possible but could be of the highest value in terms of global prosperity and security" (Crapo, 2019). Senator Cornyn

---

own ISE, it is difficult to hide an integrated organizational structure from scrutiny despite any attempts at classifying the information outside the public record (Lindsay, 2020). One could argue the USG to have over-estimated the Chinese coordinative capacity for MCF by simultaneously dismissing their profit motive and assuming a prodigious capacity to integrate their techno-nationalist apparatus.

[65] Chinese ICT firms attempting to function in US and international markets are more exposed to US policy initiatives than Chinese firms whose capital remained in China.

confirmed coherent policy design on both the defensive and offensive fronts. He argued in *a Senate Committee on Banking, Housing, and Urban Affairs Hearing to Examine CFIUS Reform* on January 25, 2018*,* that the FIRRMA expansion did not represent regulatory overreach since export controls are not sufficient to address the threat of outbound technology transfers as a standalone measure, thereby emphasizing both policies' complementarity.[66]

Given the inability of CFIUS to leverage the multilateral system as an inbound regime, the export control reform, it was hoped, would fill that gap.[67] A consensus emerged that such a measure would have duplicated and undermined the existing export control system without significantly benefiting national security. That consensus was reached after many hearings despite minor dissenting opinions over the CFIUS expansion.[68] The former Under Secretary for International Trade and Assistant Secretary of Commerce for Export Administration stated in a trade panel: "The Obama administration did a lot of good things in export controls but they didn't update the [control] lists. There are a lot of technologies that weren't control that should have been. Artificial intelligence, quantum computing, potential implications of blockchain (…) the question is should these be controlled, and a number of us said they need to be looked at but not by CFIUS, they should be looked at by the export control system that we've had since the end of the

[66] In a Senate Committee on Banking, Housing, and Urban Affairs Hearing to Examine CFIUS Reform on January 22 and 25 2018.

[67] Unilateral controls of technologies are widely regarded in Congressional hearings to harm the domestic economy without preventing China and other adversaries from acquiring controlled technologies.

[68] Some witnesses expressed reservations about the economic impact and regulatory overreach of an expanded CFIUS jurisdiction. Arguments were presented against extending the CFIUS mandate to passive investments or investments in U.S. venture capital firms.

second world war that by-and-large, worked (…) the way this ultimately got resolved was the financial services and banking committee said yeah we think CFIUS should be strengthened to look at inbound investments but we also think we need to update and modernize the export control system and a bipartisan bill introduced by Mr. Royce and Mr. Engel was essentially attached to the bill and became law (…) the process worked, it produced a compromise through a bill that strengthens both CFIUS and the export control system in ways that everyone agrees needed to be done but it avoided at one of the most perilous times an outcome that could have been much substantially worse. It could have been completely unilateral, significantly discouraged investment in this country (Padilla, 2018)".

In other words, with ECRA, a bipartisan Congressional compromise with the executive enabled defensive and offensive measures to cohere. Congress regarded ECRA and FIRMMA as complementary measures to limit outbound technology transfers. After the proposed FIRMMA provision to cover outbound transactions was redacted as part of that compromise, concern with the potential overlap between inbound and outbound institutions was set aside. The nature of the compromise is further discussed in the political economy of 5G in an upcoming section.

Given that Huawei has been scrutinized for more than a decade, the timing of USG attacks against it requires careful consideration. The USG's ongoing campaign against Huawei and ZTE is evident from the targeted nature of its employed measures, especially in how it intended to target vulnerable portions of the firms' supply chain, i.e., the semiconductor supply. With the Export Controls Reform Act of 2018 (ECRA), the USG response to China's threat becomes more cohesive given the gaps and inconsistencies that

would have occurred by relying on inbound restrictions as a standalone measure. However, the USG's differentiated treatment of national champions and other IT firms indicates tit-for-tat digital mercantilism (a response to the Chinese ICT Trojan horse), which later evolved into a whole-of-government response.

Following the defensive measures and a more aggressive trade stance, the USG response also involved an offensive response targeting Chinese ICT champions. While the offensive measures' efficacy remains contested, this solution was prompted by the need for a coherent USG policy response given the perceived complementary goals of decoupling trade while actively undermining Chinese ICT champions. Regime convergence was not without constraints given different stakeholder interests. Despite inconsistencies in the USG response, however, themes of Chinese compromise to the 5G supply chain were strong enough to compel convergent regulatory schemes that achieve regime goals. [69]

6.5.3 Juncture 2: The integration of defensive and offensive measures forms a whole-of-government response motivated by the need to counter China through strategic IT

The previous junctures outlined how policymakers combined defensive and offensive measures through coherent policy making. This next juncture involves new institutions devised to foster regime integration, such as interagency and whole-of-government

[69] There can be little doubt of the almost exclusive focus on China when it comes to export controls. The Assistant Secretary of Commerce for Export Administration stated in a panel: "if you're going to have a regulatory system that is intended to protect national security you should say who the target is (…) in the export control world there's no ambiguity about who the target is (…) if the goal here is to strengthen national security because you're concerned that somebody is doing something with foreign investments that you don't like, you should say who you're concerned about. And let's be honest, this debate was almost exclusively about China (WITA, 2018)."

responses to China in the cybersecurity regime. This section also explores the regime's efficacy at integrating a whole-of-government response motivated by the China-threat idea's final stage, i.e., that *Chinese ICT firms need to be decoupled from the US economy and actively undermined in the interest of national security.* It also addresses how the need to create new authorities had to reconcile the isolationist stance of the Trump administration with Congress's struggle to adopt a multilateral approach to counter China's threat.

6.4.5 The Federal Communications Commission

As the nations' communications regulator, the FCC used its public interest mandate to further a national security rationale. The FCC is one of the USG's principal independent agencies contributing to the securitization of 5G telecommunications equipment and international submarine cables. The FCC achieved this securitization process by furthering the convergence between infrastructure security and trade in the digital economy. As previously described with CFIUS, the same fundamental logic applies in the regime, i.e., incoming IT transactions by foreign adversaries pose an undue risk compromising national security. Moreover, since the ICT supply chain is pervasive and critical to every aspect of the US economy, the national security mandate can supersede free trade principles.[70]

[70] For example, while the FCC's delicensing of Chinese telecommunications firms violated WTO commitments in the Basic Telecommunications Services agreement of 1997, they were legitimated on national security grounds.

Relevant FCC efforts to the cybersecurity regime include the ICT supply chain, submarine cable landing rights, and the Universal Service Fund (USF) management.[71] This section focuses on how the FCC reinterpreted its legal authority under the Communications Assistance for Law Enforcement Act (CALEA) to further cybersecurity regime goals.

In April of 2018, the FCC published a Notice of Proposed Rulemaking (NPRM), *Protecting Against National Security Threats to the Communications Supply Chain Through FCC Programs*. After a period of comment submission and review (explored in the political-economy section), the eventual Report and Order made domestic firms using telecommunication equipment vendors or services from "designated" entities (Huawei and ZTE) ineligible to receive deployment subsidies.

Submitted comments (including those from Huawei) argued that the reinterpretation of the CALEA statute was an unprecedented, extra-legal move. However, after Congress passed the Secure and Trusted Communications Networks Act of 2019, the FCC argued they had "sufficient authority under section 201 (b) and 254 of the Communications Act and the Secure Networks Act" in requiring the removal of covered equipment and services by Eligible Telecommunications Carriers, i.e., rural operators, that receive USF support. [72] The FCC later issued a rip-and-replace order for rural operators singling out Huawei and ZTE as targeted Chinese ICT equipment manufacturers (FCC, 2019). The FCC later argued that the "Communications Act provides the Commission broad legal

[71] Section 201 (b) and 254 of the Communications Act.

[72] A government payback program provided compensation after USF recipients were certified free from Chinese ICT.

authority to require removal of covered equipment and services by ETCs that receive USF support" (FCC, 2020). The FCC's Public Safety and Homeland Security Bureau issued final designations on June 30, 2020, barring Huawei and ZTE from transacting in the US *communications sector*, including any US firm within the FCC's jurisdiction is barred from transacting with them.[73]

As a testament to the potency of the China threat idea, the FCC was willing to break precedent in an aggressive market intervention and risk inconsistency by regulating network and service providers alike. The FCC required all providers and any corresponding portion of their networks to certify they are not using equipment, services, or software from Huawei and ZTE. the telecommunications industry, in collaboration with the FBI, has been developing CALEA technical standards for the lawful interception of communications and the handover of user retained data following a legal warrant for the past six years (Rutkowski, 2020). However, the FCC engaged in a controversial market intervention by forcing vendors to develop their local enclaves and non-standard 5G specifications that ensure they are compliant and not using designated vendor equipment.

The following sub-sections describe the Team Telecom interagency processes and contrast it with the CFIUS. The section concludes with a regime-based explanation for why coordinative interagency processes overlapped in certain areas.

[73] The FCC, DoS, and other agencies were also involved in international efforts to further regime goals in the Prague Proposals. Conference recommendations emphasized [discuss with MM] promoted Open RAN solutions

6.4.5.1 Team Telecom

Team Telecom is a broad interagency working group advising the FCC on ICT risks to the cyber supply chain, including incoming ICT investments and licensing decisions based on referred applications (DoJ, 2021; CSR, 2021). The FCC's broad "public interest" regulatory mandate authorized Team Telecom informally since the early 2000s to secure critical telecommunications transactions through a cross-agency team from the FBI, the DoD, and later the DHS.[74]

Reviews begin after the FCC refers to Team Telecom cases where specific licenses and authorizations consist of 10% or more direct or indirect foreign ownership (Weimer and Witt, 2020). However, the committee's due process involves a lengthy and opaque deliberative procedure. For example, China Mobile was denied its application in April 2019 following eight years of indeterminacy (FCC, 2019). The timing of the decision is evidence of political pressure that confirms a coordinated defensive regime against Chinese ICT. Team Telecom later confirmed the Trojan horse idea that China Mobile would "be highly likely to succumb to exploitation, influence, and control by the Chinese government" if Team Telecom allowed it to provide international telecommunications services (DoJ, 2019).

With *EO 13913* on April 4, 2020, the White House formalized Team Telecom.[75] The Trump administration broadened the public interest mandate to include "national

[74] 47 U.S. Code § Section 214 Extension of lines or discontinuance of service; certificate of public convenience and necessity.

[75] *EO 13913: Establishing the Committee for the Assessment of Foreign Participation in the United States Telecommunications Services Sector* formalized and redesignated Team Telecom as the Committee for the Assessment of Foreign Participation in the United States Telecommunications Services Sector

security, law enforcement, foreign policy, and trade policy concerns," confirming a government-wide securitization of IT trade (DoJ, 2021). Chinese ownership was then systematically targeted as Team Telecom denied entry to telecommunications services and revoked authorization to international cable landing rights (FCC, 2021).[76]

An interagency process of committee members and advisory agencies now coordinated the newly formalized Team Telecom.[77] However, as one of two defensive interagency processes leveraged by the USG against Chinese ICT, Team Telecom suffers from "regulatory overlap" with CFIUS (Fitzgerald et al., 2016). The two committees' missions are formally distinct, CFIUS's scope is financial transactions that carry a national security risk, and Team Telecom addresses telecommunications transactions in that same vein. While both committees differ in their authority, they overlap in practice, membership, and staff.[78] The DoJ acquiesced, stating that while both agencies are

(CAFPUSTSS). Unsurprisingly, the informal designation prevailed. The FCC followed in October 2020 with the Report and Order *In the Matter of Process Reform for Executive branch Review of Certain FCC Applications and Petitions Involving Foreign Ownership*

[76] The FCC revokes the domestic authority and international authorization of China Unicom Americas, Pacific Networks, and ComNet i.e., they were denied from providing inbound and international services.

[77] The Committee is chaired by the Attorney General and includes the Secretaries of Defense and Homeland Security as members. The advisory board includes the Secretaries of State, Treasury, and Commerce; the Director of the Office of Management and Budget; the United States Trade Representative; the Director of National Intelligence; the Administrator of the General Services Administration; the Director of the Office of Science and Technology Policy, and certain Assistants to the President. The president can also add committee members from the executive.

[78] For example, the Director of the Foreign Investment Review Staff (FIRS) for the National Security Division (NSD) at the DoJ which serves as Chair of Team Telecom oversaw "the DoJ's participation in CFIUS, including the review of over 1,000 acquisitions and efforts to prohibit multiple transactions on national security grounds" (Sofield, 2021). The Principal Deputy Chief overlaps in his role as well. CFIUS and Team Telecom are also treated as a monolithic entity in conference proceedings. The national Conference on CFIUS & Team Telecom which is currently in its sixth iteration completes the involvement of all members from both working groups together.

independent of each other, “some transactions will trigger a filing with the FCC and [are] also (…) subject to CFIUS jurisdiction (DoJ, 2021).”

As per the operationalization of coherence, inter-organizational programs in Team Telecom, the FCC, DoJ, and CFIUS appear to consistently serve the same overarching China threat themes and ideas. While the DoJ states that “the Executive Order [EO 13913] is company and country agnostic,” the implementation of rules focused almost exclusively on Chinese ICT since their formalization (FCC, 2021). The DoJ states the formalization was intended to provide “clarity and reliability to applicants, the public, and the FCC about the review and recommendation process.” The formalization of Team Telecom tentatively appears to have replaced the opaqueness of its deliberative process with a blanket restriction on Chinese telecommunications.

Despite formalization, both CFIUS and Team Telecom still involve surprising regulatory overlap. The puzzling question of why both agencies were not unified remains. CFIUS is not affected by FCC rulemaking and can follow its mission by imposing requirements on financial transactions with no mandate to coordinate with other agencies. The formalization of Team Telecom involved process reforms, but more importantly, the interagency working group now followed a policy mandate designed to cohere with CFIUS in decoupling the US economy from Chinese ICT. Given Congress’s increasing calls for a whole-of-government regime in countering the Chinese Trojan horse, the question of why CFIUS and Team Telecom were not unified in a single agency remains open.

Given the revolving door between both agencies, the fact that they are not actively competing for cases, and the typical organizational instinct towards self-preservation, a

plausible hypothesis is that of institutional and structural inertia (Hannan and Freeman, 1977). Team Telecom and CFIUS were not borne out of necessity due to the pervasive and sector-spanning nature of ICTs, as is the case in whole-of-government councils. Instead, they were allowed to endure in tandem due to the perceived severity and ubiquity of the China threat and the lack of an integrative cybersecurity czar.[79]

As explained in the next juncture, whole-of-government councils such as the FASC, the Cybersecurity Maturity Model Certification (CMMC)[80], the OMB's IFR rules were more explicitly designed out of a perceived sector-spanning nature of ICTs, given China's threat. As national security considerations intrude on every commercial transaction, the USG's *de facto* regulatory treatment of the digital economy as space for great power competition appears to overcome the fragmentary nature of the USG under specific conditions. The second juncture explores these conditions in detail.

6.4.5 The Federal Acquisition Security Council

The Federal Acquisition Security Council created another whole-of-government intra-agency process on supply chain risk management. This process was first proposed in June 2018 with S.3085, the Federal Acquisition Supply Chain Security Act of 2018 (FASCA), and later enacted in December with H.R.7327, the 'Strengthening and Enhancing Cyber-capabilities by Utilizing Risk Exposure Technology, or "SECURE" Act.

Title 2 of the SECURE Act, the FASCA, creates the Federal Acquisition Security Council (FASC), an interagency process concerned with security threats to ICT hardware

[79] Parallels can be drawn to the Federal Trade Commission (FTC) and the DoJ.

[80] An out-of-scope standard for implementing cybersecurity in the 300,000 companies in the DIB supply chain.

and software to be chaired by the OMB.[81] The order applies to federal and non-federal networks when involving contractors to the extent that interconnections are made with the federal government.[82]

The council aims to provide recommendations for acquisition and supply chain risks to federal networks. OMB published Interim Final Rule (IFR) outlining procedures used to recommend country-of-origin restrictions. The impetus for this council, according to the bill's sponsor Rep. Will Hurd (R-TX) was "to move away from an ad hoc approach to dealing with unacceptable products offered to the Federal Government by companies such as Kaspersky, ZTE, and Huawei." (Congressional Record, Dec. 19, 2018). Rep. Hurd's comments can be explained given the perceived regulatory inadequacy after DHS used FISMA powers to issue a binding directive that excluded Kaspersky from government networks (Kuerbis, 2018). Legal befuddlement occurred as FISMA powers were not designed to address specific products or companies, hence the need for new regime authorities.

However, the criteria listed in the IFR were broad by design as they allow the FASC with "the needed flexibility to evaluate additional consideration and information on a case-by-case basis" (IFR, 2020). FASC is authorized to issue "exclusion orders" that prohibit or remove certain contractors. In addition to country-of-origin restrictions, the FASC embeds a localization criterion by evaluating the security of products based on whether

[81] Currently as an interim rule. It includes representatives from: the GSA, DHS, including CISA, The ODNI, including the National Counterintelligence and Security Center, DoJ and the FBI, DoD including NSA, and DoC including NIST.

[82] However, non-federal entities are not yet required to share supply chain risk information or abide by the removal and exclusion orders.

the product transmits data outside of the United States. The interim rule also focuses on sharing supply chain risk information, assigning the task to CISA's Supply Chain Risk Management (SCRM) Task Force program, as addressed in the next chapter.

6.4.6 Cyber Supply Chain Risk Management: How the USG framed its response to cyber supply chain threats

Supply chain threats are typically broadly defined to encompass counterfeit products, compromised hardware, and software after delivery, vulnerabilities in the networks of third-party partners, insider threats (including non-adversarial), poor quality manufacturing, development, maintenance, or disposal practices (CISA, 2021).[83]

In October 2018, Bloomberg published a story about the Chinese compromise of Super Micro Computer Inc microchips affecting Apple servers and other companies, citing anonymous government and corporate sources (Robertson and Riley, 2018). The source of the article suggests a possible strategic press leak as Apple, Amazon, and members of the intelligence community later discredited the story. Then-Secretary of the Department of Homeland Security Kirstjen Nielsen stated we "do not have any evidence that supports the article." Then-Director of National Intelligence Dan Coats also stated "we've seen no evidence" of manipulation of Supermicro products (Otto, 2018). The ex-FBI Director Christopher Wray cautioned to "be careful what you read" (C-Span, 2018). Apple CEO Tim Cook declared "it [the Bloomberg story] is 100 percent a lie, there is no truth to it" and called on Bloomberg to "do the right thing" and "retract their story (CNN, 2018)." Bloomberg strengthened their commitment to the story by publishing another article that

[83] Efforts to secure the IT supply chain security date at least to 2003 when GAO expanded its report 03-121 on Protecting Information Systems Supporting the Federal Government and the Nation's Critical Infrastructures to include cyber critical infrastructure.

alludes to an ongoing counterintelligence probe. Its status remains contested at the time of writing (Bloomberg, 2021). Whether fabrication or coordinated counterintelligence probe, regime agents had re-focused USG attention on China and the risk of nation-state compromises to the ICT supply chain.[84]

Cyber Supply Chain Risk Management (C-SCRM) became an all-encompassing acronym for securing the supply chain. It is defined as "the process of identifying, assessing, preventing, and mitigating the risks associated with the distributed and interconnected nature of ICTs including IoT and iIoT product and service supply chains at the entire life cycle (Ibid)." On a technical level, hardware-level backdoors on a silicon chip impede any efforts of adding software level protection hence the severity of the potential threats (Skorobogatov, 2012). Furthermore, given that nation-states are the only possible actors that can introduce vulnerabilities and compromise a supply chain, C-SCRM became synonymous with country-of-origin-based demarcations, i.e., increased security requirements or an outright ban.

With EO 13873 *Securing the Information and Communications Technology and Services Supply Chain (ICTS)* signed in May 2019, the White House added further regime coherence by aligning multiple federal agencies — Treasury, State, DHS, DoD, Attorney General, USTR, ODNI, GSA, FCC — to the DoC mandate drawing on the International Emergency Economic Powers Act (IEEPA). The order lays out defensive measures to

[84] For example, in a November 14, 2018 hearing on *Interagency Cyber Cooperation: Roles, Responsibilities and Authorities of DOD and DHS* Rep. Jody Royce (R-GA) stated: "I place some emphasis on the issue of supply chain risks and that of course is a big concern to many of us particularly in recent weeks as there have been some reports [Bloomberg article] of at least possible compromise in some microelectronics."

oust Chinese investors and suppliers from CI operators. It defined an ICTS "transaction" as any "acquisition, importation, transfer, installation, dealing in, or use of any information and communications technology or service, including ongoing activities, such as managed services, data transmission, software updates, repairs, or the platforming or data hosting of applications for consumer download." China features along with a list of six "foreign adversaries" China (including Hong Kong), Cuba, Iran, North Korea, Russia, and Venezuela. The DoC's ensuing Interim Rule outlined a broad regulatory framework that continues the USG's regulatory treatment of the digital economy as being on par with critical infrastructure security. For example, the DoC rules are set to apply to almost any conceivable category of ICTs.[85]

The DoC was therefore now empowered on an *ad hoc* basis to prohibit or restrict transactions conducted by any person, or involving any property, subject to penalties under the IEEPA, if they involve ICTs "designed, developed, manufactured, or supplied by persons owned by, controlled by, or subject to the jurisdiction or direction of a foreign adversary; and [may] pose an undue or unacceptable risk" to the national security of the United States". (IFR/DoC, 2020)

[85] The ICTS list includes first "critical infrastructure": ICTs that will be used by a party to a transaction in any of the sixteen CI sectors as designated by PPD-21, including any subsectors or subsequently designated sectors. Second, Network Infrastructure and Satellites i.e., any ICTs part of wireless local area networks, mobile networks, satellite payloads, satellite operations and control, cable access points, wireline access points, core networking systems, or long- and short-haul systems are included. Third, ICTs involving PIIs, or, any hosted data or computing services that uses, processes, or retains "sensitive personal data" of greater than one million U.S. persons at any point over the 12 months preceding an ICTS Transaction. Fourth, and in an unusual regulatory assortment surveillance, monitoring, home networking, drones "where one million units of the ITS item at issue have been sold in the 12 months prior to the ICTS Transaction" are included. Fifth, Communications Software**:** any desktop, mobile, web-based, and gaming applications that uses the Internet. Sixth**,** Emerging Technology, or, any ICTs that may include artificial intelligence and machine learning, quantum key distribution, quantum computing, drones, autonomous systems, or advanced robotics.

The following section outlines how a public interest national security rationale was leveraged by various political interests to steer the cybersecurity regime in specific ways.

6.4.7 A monolithic Chinese threat for political mobilization

This section describes how the first idea continued perpetuating later in the decade and served to anchor assumptions for a more united whole-of-government front. In the later part of the decade, Congressional hearings would perpetuate implicit themes that anchored old ideas by present Chinese ICT firms as brazen and immoral. For example, these themes bolstered the idea that Chinese ICT firms were untrustworthy because *they export technology that facilitates authoritarianism in developing countries or violates US and UN export control rules* (theme).[86] The following two examples are more explicit examples that would appear later in the decade. In a June 2018 hearing of the House Committee on Small Business titled "ZTE Threat to America's small business," a former staffer for House Intelligence Committee Chairman Mike Rogers (which spearheaded the HPSCI effort) claimed China exports its authoritarianism through ZTEs' technology being used to suppress dissent in African countries. The assignment of political value to networking technology is fallacious from a technical standpoint because the CCP was known to have used Cisco products to facilitate domestic surveillance before they started using Huawei (Sydney Morning Herald, 2011).

The next theme is that Chinese firms are *untrustworthy* because they abuse human rights. The Department of State was more explicit in proposing that Chinese ICT national

[86] Huawei had violated of US sanctions and export controls by selling to countries like Iran and North Korea (DoJ, 2019). ZTE was more brazen as they later admitted to 380 violations to mask evidence relating to its dealings with Iran.

champions such as Huawei and ZTE have built the modern model of the authoritarian police state (DoS, 2019). They achieve this by powering the technocratic surveillance model, including the social credit system and facial recognition. That way, Chinese ICT firms oppress minorities (notably Uighur Muslims, Falun gong worshipers, and Tibetans), engage in slave labor, and censor information from their citizens. Calling attention to the rhetorical functions of this argument should not be misconstrued as a normative endorsement of oppressive and tyrannical CCP tactics. However, these *ad hominem*-type claims can hijack strategic discussions. For example, discussing Uighur oppression muddies debates about managing the semiconductor supply chain strategically for long-term US interests and how to apply an appropriate mix of competitive and cooperative trade tactics. This fusion of multiple foreign policy areas serves to add cohesion to a whole-of-government regime by providing political legitimacy through shared values.

In *Assessing the Role of the United States in the World*, a hearing before the Committee on Foreign Relations, February 27, 2019, Senator James E. Risch provides a valuable summary of how the first two ideas on the China threat are additive: "It is no secret that China seeks to surpass us both economically and militarily. One of the primary ways they have attempted to do this is by stealing our technology and intellectual property. (…) Whether or not Beijing is currently using tech firms like Huawei or ZTE to spy, it certainly could demand it and no court ruling or constitutional check would be necessary for them. This is a serious threat to our national interest (…)". Chinese ICT firms are portrayed as the vehicles of CCP grand strategy as displayed in figure 6. The lack of questioning whether Chinese ICT firms are opportunistically serving their profit motive

or merely sidestepping regulatory hurdles through tacit bargains with the Chinese state is revelatory of the strength of associations between the first two ideas. The dominant narrative gains legitimacy by sidestepping such distinctions in favor of a more digestible monolithic threat. Therefore, the underlying theme in question can be reformulated as *all Chinese capital is a tool of CCP strategy*. In other words, any private or public Chinese enterprise from SOEs*,* publicly-listed private firms operating through VIEs, and other structures like "employee-owned" firms are hiding CCP strategy. This fundamental assumption is implicit to the report and prevalent across the USG. For example, policy experts at the US-China commission have similarly assumed that private Chinese firms and SOEs are equivalent. The amalgamation of various corporate governance types reinforces a monolithic threat by Chinese firms that hides CCP strategy.[87] In another February 2019 US-China commission hearing titled *Risks, Rewards, and Results: U.S. Companies in China and Chinese Companies in the United States*, themes set after the USTR Section 301 hearing further ossified. Testifying experts argued the opaqueness of Chinese firms hampers the US ability to determine the soundness of investments and the extent to which Chinese private capital ties to SOEs, which may facilitate the aims of the CCP.[88] The counter position that large Chinese private companies have their interests

[87] Wired magazine notably argued that the opacity of Chinese organizational structures is part of a functional ambiguity designed to confuse the Western observer by having "turtles all the way down" (Wired, 2018). That said, Hawes (2021) revealed how confusion around Chinese firms' ownership (including union-ownership, CCP party branches, and VIEs for foreign investments) stems from an innovative suite of corporate governance mechanisms designed to navigate the morass of Chinese regulatory and political requirement. Firms like Alibaba, Tencent, and Baidu are publicly listed, while ZTE has the CCP as its biggest shareholder. Huawei's structure on the other hand, is unique.

[88] The finance community has also complained that as an unlisted, and employee-owned company with a CCP element Huawei's lack of regular or full financial disclosures raises suspicions. Huawei may have later hired the global accounting firm KPMG to perform their audits to assuage some of these concerns.

aligned with the US political-economic system was in the minority. Professor William C. Kirby from Harvard University highlighted that China's stock exchanges are not friendly to privately held enterprises and that CCP policies discourage large IPOs of private companies in China, making them venture offshore through VIEs.

6.4.8 The political-economy of 5G and the semiconductor supply-chain: how isolationism and multilateralism clashed in countering China's threat

Both Congress and the Federal government have used a broad national security rationale as the impetus for their campaign against Chinese ICT. While the motivation for this crackdown has been described as ideological, a confluence of distinct political interests complicates the question of determining which ideology is operative (Mascitelli & Chung, 2019). As the following section outlines, a closer examination of the distributional outcomes ensuing from China-motivated institutional changes explains why sub-optimal regime outcomes were reached by a compromise between the protectionist Trump administration and China hawks in Congress.

Figure 7 below provides a summary of the relevant interest groups relevant to the cybersecurity regime. The categories include multilateral China hawks predominantly in Congress (group 1), the unilateral and isolationist Federal government of the Trump administration (group 2), business interests competing directly with Chinese ICT (group 3), and (group 4) businesses that co-produce services with Chinese ICT firms in a

mixture of cooperative and competitive engagements with Chinese labor, demand, and IT goods and services markets.[89]

[89] Though often impressing many policy problem-solution dyads in Congressional hearings, the category of academics and issue-experts from national labs is excluded as they do not constitute a well-defined interest group capable of lobbying government and exerting direct influence.

	Group 1: Multilateral China hawks within and outside the USG	Group 2: The unilateral and isolationist USG	Group 3: Business interests competing directly with Chinese ICTs	Group 4: Cooperative and ambivalent organizations
Categories of cybersecurity regime	Policy makers in Congress, cyber-threat firms, think-tanks	Executive and independent regulatory agencies	Telecommunications vendors (RAN, Core Network Vendors, optical communications)	The semiconductor sector (Qualcomm, Intel) parts of the IT private sector (Google, Microsoft) and telecommunications operators (Verizon)
Prominent members, firms, or lobbies	(R-ARK), Marco Rubio (R-FL), Rick Scott(R-FL), Edward Royce (R-CA), Michael Gallagher (R-WI), Gary Palmer (R-AL), Michael McCaul (R-TX), Joe Manchin (D-WV), Susan Collins (R-ME), Will Hurd (R-TX), Maria Cantwell (D-WA), Lisa Murkowski (R-AK)	Cabinet Secretaries of the Trump administration	ADTRAN, Arris, Calix, Cisco, Nokia, Erikson, Fujistu, Infinera, Juniper, Ribbon, Samsung, Tellabs, the Telecommunications Industry Association (TIA)	The Information Technology Industry Council, Nokia Shanghai Bell, the Semiconductor Equipment and Materials International, the Semiconductor Industry Association, the Competitive Carriers Association, the US Chamber of Commerce
View of Chinese ICTs	Highly negative	Moderately to lowly negative	Mostly highly negative	Neutral

Figure 8: Major interest groups of the civilian cybersecurity regime

Members of group 1, the multilateral China hawks, had reasons for concern about the radical isolationism prevalent in group 2, serving as further motivation for the new statutory authorities discussed earlier.[1] What inspires a strategic technology race can be answered by considering the naïve aim of export controls. The successful application of controls on any foundational technology, however broadly defined, can be assumed to depend on three criteria.[2] First, determining whether adversary militaries can leverage a given technology. Second, whether the technology is essential to the US domestic national security broadly defined; and finally, determining that the technology is not widely available elsewhere (S. HRG. 116–122, 2019). Therefore, the success of export controls depends on the coordination of implementing agencies and the USG's ability to leverage allies in enforcing the controls. However, the Trump administration ignored the third criteria and furthered its unilateral application of hardware-based export controls.[3]

Expert witnesses have also commented on the limits of export controls when applied to intangible products such as data and algorithms. To the extent that export controls are used to manage emerging strategic technologies such as AI and 5G, they are only feasibly applied to tangible products such as hardware chips and chip manufacturing equipment (Buchanon, 2020). To make matters worse, the fallibility of employing IT-based export controls on hardware products instead of services and applications becomes evident when considering that hardware is but a single part of a triad comprising an AI service.

---

[1] While Republican representatives of group 1 have a high percentage of voting in line with President Trump's position they tend to disagree with Trump on Defense and other appropriations.

[2] Naïve criteria exclude political considerations.

[3] The Trump administration's rationale for its isolationist stance and unilateral application of export controls is outside the scope of this work.

Labelling AI as "strategic" without accounting for scalable algorithms, and 'big data' sets, is tantamount to trade protectionism.[4]

The 5G telecommunications supply chain is arguably even more intractable than AI. It involves a diverse supply chain from Radio Access Network vendors (RAN)[5], core network vendors[6], telecommunications operators (e.g., Verizon and CenturyLink), and the semiconductor sector, which supplies the RAN market with chips (SIA, 2020). The semiconductor industry is also comprised of a diverse and global value chain dominated by US firms in many segments.[7] Globalized market where various countries enjoy different comparative and competitive advantages (Khan et al., 2021)

While other "strategic technologies" such as quantum computing and AI continue to be framed as part of an ambiguous technology race with China, 5G telecommunications were singled out as the preeminent competitive battleground because of the dependency of Chinese ICT on US semiconductors. The reason why export controls were still applied to the semiconductor supply of Chinese ICT firms can be explained by a concordance of political interests. The Trump administration (group 2) was concerned with its "tough on China" optics, while more aggressive China hawks (group 1) wanted to rally allies to "secure 5G" from China but had concerns with group 2's isolationism and incoherent

[4] While algorithmic innovation is often portrayed as IT company's 'crown-jewels', the positive feedback loops typical of networked economies are such that a firm's market dominance is often provided by the quality and availability of its data (Mueller & Farhat, 2020).

[5] Globally led by Samsung and Huawei, also includes Nokia, Ericsson, and ZTE.

[6] Globally led by Cisco and Huawei.

[7] The semiconductor market segments include electronic design automation firms, integrated device manufacturers, fabless designers, and foundries (Bown, 2020). The United States, Japan, and the Netherlands have a competitive advantage in the production of manufacturing equipment, itself a bottleneck for China's chip supply chain (Khan et al., 2021).

implementation. However, both groups had joint interests in decoupling and actively undermining Chinese ICT firms. The Executive branch wanted to use the US in isolation and Congress wanted to leverage allied countries.[8] That way, despite not satisfying the naive conditions for effectiveness, a broad application of export controls on the semiconductor sector was still applied. Their application accelerated the more hawkish political agenda of decoupling and actively undermining Chinese ICT. This reframing allows a better understanding of institutional reforms such as ECRA.

ECRA kept the definition of "foundational technologies" purposefully vague, allowing for flexible and dynamic implementation by regulatory agencies of future administrations. While this functionally broad definition was the litmus test of bipartisan support countering the Trojan horse, Congress clashed with the Trump administration in their approach to implementation. Congress was completely in line with the Trump administration's need to counter China but disagreed with the latter's trade policies. For example, in a Senate Committee meeting on Banking, Housing, and Urban Affairs titled *Export Control Reform Implementation: Outside Perspectives* on July 18 2019, the former Under Secretary for Industry and Security at DoC voiced his concern with the administration's approach to trade, stating: "As a policy matter, I don't think it's a sound idea to treat export controls— which are imposed for military security and foreign policy reasons—as an element of our commercial trade policy (…) It is even worse to treat the enforcement of export controls in that manner. Public horse-trading of national security and law enforcement for sales of agricultural commodities sends the wrong message to

[8] The Clean Networks initiative is an international initiative by DoS discussed in juncture 2.

those who would violate our laws and put our country at risk" (Hirschorn, 2019). This statement alludes to the bilateral tactics of the Trump administration whereby its campaign against Chinese ICT was traded-off for broader commodities trade concessions. Such political considerations are exogenous to the IT sector *per se* yet carry a disintegrative effect on the cybersecurity regime in the temporary incoherence of its response.[9]

Referring to Congress' disapproval of the implementation process, representative Chris Van Hollen (D-MD) stated in that same hearing: "If we make a determination that something is in our national security interest, for example if we think it's important to put Huawei on the entity-list for the purpose of preventing exports that could strengthen their 5G network (…) we should not then be making trade-offs with respect to those national security interests in order to get concessions on tariffs or other trade related issues" (Van Hollen, 2019). Witnesses and representatives agreed across the board. Senator Van Hollen continued deploring President Trump's move to remove ZTE from BIS's "Denied Persons List" after negotiations with China's Xi Jinping (Jiang, 2018). Van Hollen continued: "Huawei was also found to be in violation of sanctions and as a result we've asked for the Canadians to arrest the CFO of Huawei and then the President says that he would intervene in the interest of Huawei's CFO Ming if it helped secure a trade deal with China (…) I agree with a lot of the efforts that this administration is taking with respect to addressing Chinese theft of technology and the national security part. I agree

[9] The Trump administration had also mulled placing Huawei on DoT's Specially Designated Nationals (SDN) list, also known as the "nuclear option" which makes it virtually impossible for a company to transact in US dollars. Adding Huawei to the SDN list would have implied a host of logistical, diplomatic and economic difficulties for the USG given the impact on US allies that rely on Huawei for their 4G networks (Reuters, 2019).

with their Huawei policy. But it is very, very scary to start trading off national security issues and the rule of law and arresting people with respect to trade" (Ibid). In other words, proponents of a multilateral export control regime and the Trump administration had a joint interest in targeting the Chinese Trojan horse. However, their approaches were different given their different political motivations.[10]

On May 16, 2019, BIS amended the EAR by adding Huawei to its Entity List, stating there was "reasonable cause to believe that Huawei has been involved in activities contrary to the national security or foreign policy interests of the United States" (Federal Register, 2019). This designation lasting five years is an effective embargo that cuts Huawei from the US supply chain with an estimated material impact valued at $30 billion. Any firm is forbidden from exporting or transferring access to 152 Huawei affiliates at the risk of losing access to US markets. As a result, British semiconductor designer ARM was forced to comply with US regulations and retract its contracts with Huawei. Google was similarly forced to retract the Android operating system from Huawei phones within 90 days. Consequently, as global telecommunications and software vendors were forced to align themselves with the two major geopolitical blocks, the strategic technology battleground shifted to the EU (Merics, 2020).

[10] DoC's response has been inconsistent with its national security rationale. ZTE was removed from the entity-list after paying a $2 billion fine while Huawei's status persists at the time of writing. The fine was the largest penalty levied in an export control case. Meanwhile, firms such as Transsion are left free-reign to make inroads in the African telecommunications market. Transsion, a Chinese telecommunications manufacturer overtook Samsung in 2017 as top-selling phone maker in Africa (Gagliardone, 2020).

Interest group	Group 1: Multilateral China hawks	Group 2: The Trump administration	Group 3: Competing businesses	Group 4: Cooperative and ambivalent businesses
Joint interests that failed to intersect	With group 4: Mega FTAs regarded as appropriate measures to extract concessions from China to level the playing field and gain more domestic market access	With group 4: on facilitating outbound US capital in the domestic Chinese market	Not applicable	With groups 1 & 2: favors trade reciprocity including attempts to lift impediments to trade (localization requirements or restrictions on Foreign Cloud Service Providers) as well as gaining access to the Chinese domestic market
Joint interests that enabled a political equilibrium	With groups 2&3: **countering the Chinese Trojan horse via inbound and outbound restrictions**	With group 3: **to secure the supply chain via geopolitical blocks of "trusted networks"**	With group 1: **Setting up a whole-of-nation response to counter China's threat**	Not applicable
The proposed solution to counter the Trojan horse	Digital neo-mercantilism	Techno-nationalism	Trade protectionism and boosting domestic champions	Overhauling domestic industrial policy

Figure 9: Interest group majority position on IT trade with China

Per figure 9, a political equilibrium yielded a viable solution to the threat of China in the USG. Positions on China fell on a spectrum from cooperative to competitive, where extremist stances found no basis for trade in any technology industry with China. Milder stances aimed to limit it to the extent necessary.[1] This analysis found a functional conceptual demarcation that distinguishes multilateralist China hawks, group 1, from the isolationist Trump administration as group 2.

Group 1 (multilateral China hawks) had a similar conception of China as a policy problem to group 2 as they shared the same country-of-origin national security rationale; however, the two groups differed on their policy solutions, i.e., their willingness to work with allies, their implementation procedure, and finally, their political motivations. Some representatives such as Mike Rogers (R-ARK) or Marco Rubio (R-FL) leveraged the threat of Chinese ICT overtly, others on Congressional energy committees such as Maria Cantwell (D-WA), Lisa Murkowski (R-AK), or Joe Manchin (D-WV) leveraged IT/OT convergence (addressed in the next chapter) as worsening the threat of China but not the other way around. Group 1 was concerned with the Executive's potential use of emergency powers to further its agenda on the threat of China.

Group 2 prioritized their domestic political agenda by favoring trade protectionism first and foremost. Politically, the Executive branch used restrictions on Chinese ICT as a bargaining chip with group 1 for concessions on commodities trade while bolstering its domestic image as tough on China.

[1] Groups 1 & 2 can be further sub-differentiated to account for bipartisan politics. For example, democrats and republicans agree don ICT Supply Chain Risk Management programs but differed on assigning leadership and authority between DoE and the DHS. The distinction had limited relevance to the analysis and was therefore excluded.

Group 3, which involves businesses and interests competing with Chinese ICT, lobbied Congress for expansive protectionism and additional funds to cover self-serving rip-and-replace programs. Group 3 also lobbied for a whole-of-nation response to secure the IT supply chain to overcome government fragmentation. Group 4, which involves firms in more cooperative arrangements with Chinese ICT, favored trade reciprocity, attempting to lift impediments to trade such as localization requirements or rules on foreign cloud service providers to gain better access to the Chinese domestic market. They lobbied against export controls since it contradicted their profit motive arguing the economic and security future of the US to be more determined by domestic innovation policy choices than the ability to influence Beijing's economic policies. However, the pushback from group 4 was not sufficient to overcome the aligned interests of the remaining interest groups.

The Competitive Carriers Association (CCA) (group 4) argued that FCC proposals to extirpate Chinese ICT were flawed as they would cause "immense harm" to their members by shrinking the market, driving up cost and creating uncertainty that would harm millions of rural Americans (CCA, 2018).[2] They found the FCC's presentation of the national security threat motivating the NPR as ambiguous, claiming the Commission "failed to identify evidence supporting the broad prohibitions contemplated by the proposed rule" (CCA, 2020). The CCA continued by deploring the use of the seven-year-

[2] The CCA argued the FCC NPR would shrink the number of suppliers of core network equipment from five to three. The TIA responded claiming "many vendors provided end-to-end design solutions and customer service for carrier customers, not merely discrete components as CCA claimed.

old HPSCI report as the only source of critical evidence, itself severely lacking as persuasive evidence.

The CCA's means of exerting leverage threatened legal action by alluding to a legal violation of due process and suggesting potential compensation for their carriers should the FCC motion come to pass. The TIA argued that the rip-and-replace reimbursement process should come from Congress instead of the USF. The CCA was later less keen on speaking out after Congress passed the Secure and Trusted Communications Networks Act which included the pay-back program after Chinese ICT was ripped and replaced. This change indicates either within-group variation or a change in the CCA's overall political stance over Chinese ICT after Congress enacted the compensation program. [3]

In stark contrast to the CCA, the Telecommunication Industry Association (TIA) was an ardent proponent of expanding offensive measures against Chinese ICT (Andrews, 2020).[4] For group 3, the growth of the Chinese ICT threat litany involves a powerful trifecta, i.e., national security, jobs, and innovation. The TIA lobbied for the Congressional payback program and argued for a "surgical approach" that targets Huawei

[3] In a Senate Commerce, Science and Transportation Committee hearing on 5G technology and Cybersecurity on March 4, 2020, CCA spokesperson Steven Barry lauded representatives present for passing the Secure and Trusted Communications Networks Act. The challenge of 5G as he put it "is heightened by carriers that have equipment in their networks from companies deemed by federal agencies to pose a national security threat" (Barry, 2020).

[4] TIA is "the leading trade association for the information and communications technology industry, representing companies that manufacture or supply the products and services used in global communications across all technology platforms. TIA represents its members on the full range of policy issues affecting the ICT industry and forges consensus on voluntary, industry-based standards (TIA, 2020)." While Huawei and ZTE are part of the TIA, they were denied access to the public policy committee and internal deliberations.

and ZTE instead of overhauling supply chain management. Supporting the designation of Chinese ICT as covered entities on the DoC list. Urges the FCC to adopt a "whole of government approach to supply chain security," acknowledging the USG fragmentation and proposing a regime-level response to avoid "duplication of effort and conflicting outcomes (TIA, 2020)."

Group 3 have consistently lobbied for protectionism. For example, Infinera testified on the Chinese ICT threat in a US-China Commission hearing in 2012, lobbying for protection in an intensely competitive optical communications market. Infinera's counsel decried the rapid market share gains of Huawei and ZTE in the mid-2000s and leveraged the Trojan horse idea speaking against the "concerted efforts of the Chinese government and Chinese optical equipment vendors" (US-China Commission, 2012).

The interest group category 4, represented by the ITI, SIA, and the Semiconductor Equipment and Materials International (SEMI), are engaged in cooperative relationships with Chinese ICT firms despite inbound restrictions.[5] Since less than 15 percent of the world's manufacturing capacity resides geographically in the United States, these groups favor open supply chains and fewer trade barriers (Varas et al. 2020).[6] For example, after DoC threatened ZTE with a 7-year ban on sourcing US technology, US technology firms are reported to have lobbied in favor of ZTE (Capri, 2020).

[5] The US firms represented by these groups continue to lead the IT market in semiconductor sales. For a detailed historical exposition of the political economy of the semiconductor sector see (Bown, 2020).

[6] The reaction of group 4 from figure 2 is further discussed in response to the Federal Acquisition Security Council (FASC) and NDAA FY2021 in juncture 3.

In a Senate Committee on Commerce, Science, and Transportation titled *China: Challenges to U.S. Commerce* on March 7, 2019, the Information Technology Industry Council (ITI), speaking with the voice of its Executive Vice President of Policy, presented an alternate narrative by recognizing the need for nuanced competitive and cooperative behavior on IT trade, as captured by group 4.[7] For instance, they recognize that curtailing IP theft will not solve indigenous Chinese innovation. They instead consider US economic security to be determined by domestic policy choices instead of attempts to influence Beijing's trade and economic policies. On May 15, 2020, the President of the Semiconductor Industry Association (SIA) declared the rule would "create uncertainty and disruption for the global semiconductor supply chain" (Reuters, 2020).

On May 15, 2020, the President of the Semiconductor Industry Association (SIA) (group 4) declared that the implementation of export controls would "create uncertainty and disruption for the global semiconductor supply chain." However, the DoC and Trump administration more broadly continue citing national security threats as motivating factors as they continue to consider Huawei as beholden to the CCP. Minority voices at DoD also claimed Huawei hardware is not sensitive technology and that banning trade with them will harm the DIB's ability to remain competitive, indirectly affecting national security (WSJ, 2020; Purdy, 2020).

On August 17, 2020, DoC secretary Wilbur Ross further reduced the margin by which the entity-list applies to Huawei, claiming, "there has been a very highly technical loophole

[7] This position was also found more common among testifying academics.

through which Huawei has been able, in effect, to use US technology with foreign fab producers" (Reuters, 2020). The Foreign Direct Product Rule (FDPR) thereby shrunk the *de minimis* provision from 25% of US-made components allowed in a product down to 10%.[8] DoC's BIS further restricts Huawei's ability to use U.S. tech and software to design and manufacture its semiconductors abroad. It blocks any global company from using US-made hardware or software to design or produce chips for Huawei.

In December 2020, Representatives Michael McCaul (R-TX) and Marco Rubio (R-FL) sent a letter to Secretary Ross complaining that the inclusion of the Shanghai-based Semiconductor Manufacturing International Company (SMIC) on the Entity List was "done for show and parochial commercial interests at the expense of US national security."[9] In the letter, the representatives also state they expect companies to bypass the *de minimis* provision by altering their supply chains, as Huawei and ZTE had recently done. The Entity Listing of SMIC limits the presumption of denial to items required to produce wafers at 10 nanometers and below. The representatives argued that advanced chips below 10 nanometers could be retrofitted from older generations, a claim contested by manufacturers (Shilov, 2020; Zafar, 2021). As of Q4 2020, the Chinese domestic market for logic chip production is served at 67% by Taiwanese, Singaporean, and American manufacturers. SMICs, China's largest and most advanced foundry, produce only 19% of the demand The representatives urged in their letter to DoC to "ensure that SISC is unable to access semiconductor manufacturing equipment from any location the

[8] The *de minimis* provision pertains to a US-controlled content threshold allowed to be incorporated into foreign-made products. If an item contained more than 19% US origin by value, the product required an export license.

[9]

world." The inflated threat claims appear aimed at focusing on China's supply chain bottleneck.

6.5 Conclusion: the China hawk thesis emerges as a viable policy solution

The USG policy solution to the threat of China is based on the continued decoupling of Chinese ICT firms from the US economy while actively undermining their champions in the US economy and international arena. This emerged as the fundamental thesis by China hawks (groups 1&2).

The China threat idea was conducive to coherent USG cybersecurity policy making. That said disintegrative forces were present in the case of CFIUS and Team Telecom caused in one case by structural and organizational inertia. In another case, the political bargaining between groups 1 & over the appropriate policy response compromised policy coherence. Issues also appeared in executive implementation at endemic problems related to the DHS and federal information management policies as described in the next chapter.

The policy problem presented by China hawks is that Chinese ICT is a Trojan horse hiding a CCP agenda to dominate the US economy. While accounts differ and are seldom complete, the Trojan horse narrative first diffused from the US military and intelligence agencies to the civilian cybersecurity regime and tied the China threat idea to Chinese ICT and strategic technologies. It can be summarized as follows: the Chinese state leverages its ICT industry in domestic and foreign markets to consolidate power. Strategic ICT technologies grow domestic Chinese GDP via military-civil fusion mechanisms that allow dual-use technology transfers through obscure public-private institutional arrangements. Military-civil fusion is a policy problem especially given its

three main objectives: first, it grows the Chinese science and technology base through foreign and domestic dual-use technology acquisition, which are (somehow) also converted into military-grade technology. These acquisitions are achieved through industrial espionage facilitated by coordinated PLA and militia actors. Second, national "champions" are sponsored through direct or indirect investments such as favorable government contracts or forced technology transfers by requiring Western firms to set up joint ventures with Chinese counterparts as a condition for accessing the alluring domestic Chinese market. Third, military-civil fusion mechanisms help modernize the PLA through 'special' contracts between Chinese ICT firms and the PLA. The PLA then benefits from private sector expertise, given their revolving door policies. As a result, both the Chinese public and private sectors serve the same CCP grand strategy willy-nilly.

Since the US cannot be expected to counter the threat of China with its industrial policies given an unlevel playing field, it must play offense by furthering its brand of MCF. The solution is a tit-for-tat strategy of digital neo-mercantilism, i.e., the USG decouples Chinese ICT from the US economy and actively undermines their overall growth through joint defensive and offensive measures. The DoC levied the US comparative advantage in semiconductors and used mechanisms to limit their export to Chinese ICT firms. The DoC also hedged risk for future military applications by expanding the dual-use definitions to amalgamate Commercial Of-The-Shelf Technologies (COTS) with military-grade technology, further converging economic competition to the strategic domain

.

CHAPTER 7. THE PROBLEM OF IT/OT CONVERGENCE

Introduction

This chapter considers IT/OT convergence as another possible explanatory factor for cybersecurity regime integration, contrasting it with the threat of Chinese ICT addressed in chapter 7. The convergence of IT and OT is a phenomenon enabling the emergence of cyber-physical systems. The chief concern in this chapter is how the perceived nature of IT/OT convergence is reifying security threats and risk perception and how these threats may be used to drive cybersecurity regime integration.

The vulnerabilities created by IT/OT convergence are often framed and conceptualized from the standpoint of novel cybersecurity threats. While these new threats have yet to result in a "cyber-9/11", they are actively debated in the USG. Tracing how this family of problems is framed, including incumbent institutions' perceived adequacy to address them, will help us better understand IT/OT convergence as a driver of regime change, including policymaking mechanisms under ambiguity and uncertainty. At stake is finding the right balance in allocating resources to reduce public risk, i.e., building a secure federal risk management enterprise while avoiding the pitfalls of a security theater associated with cybersecurity risk hyperbole (Schneier, 2009).[1] Understanding how political interests leverage ideas and argue for solutions in this space may also pave the

[1] As many interdisciplinary authors on the economics of information security have noted, when it comes to secure information management, one can limit the attack surface but not get rid of it completely as resources are costly in terms of equipment and security implementation. Further, the security constraints on legitimate users also contribute to optimization between usability and security by making incremental incentive-based adjustments and changes in resource allocation. With critical infrastructure, however, this framework does not apply as the concern instead involves 'black swan' events those that do not fit the equilibrium framework (Odlyzko, 2019).

way to explore institutional innovations in the ongoing reorganization of the civilian US cybersecurity regime.

The challenges associated with IT/OT convergence are most prevalent in the energy sector given its intersection with ICTs and the blurring regulatory demarcation for CIP governance, i.e.., the smart grid.[2] The chapter proceeds as follows: in section 1, IT/OT convergence is disambiguated by considering the high-level operational and security requirements of IT and OT, first as distinct environments, then combined as a novel security problem compounding the threat of CI interdependence. Section 2 provides a brief historical overview of notable cases. It starts with Stuxnet in 2010, which illustrates how the problem framing of IT/OT convergence shifted from Public Policy to Foreign Policy given its ties to malware signatures associated with specific nation-state actors. Section 3 summarizes the main IT/OT convergence themes extracted from relevant Congressional hearings and in-depth interviews, including their pattern of association. Section 4 expands the themes of section 3 and addresses how an institutional vacuum created opportunities for government agencies and National Labs to compete in providing solutions for different IT/OT convergence variants, including regulations and networking architectures. Section 5 addresses interest group dynamics and how the threat of China encroached on the threats posed by IT/OT convergence but only affected sector-specific

[2] While some argue energy is the single most important critical infrastructure sector, CI is most critical at the "lifeline sectors" on which all others have more dependency. These include energy, water, communications, and transportation subsectors. The Director, Office of the Director of National Intelligence, National Counterintelligence and Security Center stated at a technical FERC/DOE conference that while telecommunications and financial systems are critical, adversarial intelligence officers typically appear mostly concerned with how military bases are powered, making energy the single most important CI sector in the US. Driverless cars and military robotics with mixed-initiative systems entailing shared decision-making present other potential case studies.

areas, such as 5G standards, networking architecture (in the IT sector), and CIP Reliability Standards (in the energy sector). The chapter concludes in section 6 with a synthesis of relevant findings and presents a pathway forward.

7.1 IT and OT in the energy sector

7.1.1 General-purpose Operations Technology (OT)

Supervisory Control and Data and Acquisition (SCADA) systems that monitor and control industrial networks are the quintessential form of OT (Meyers, 2013).[3] Such Industrial Control Systems (ICS) are used in water, gas, and electric power to control and monitor energy and material flow spread over vast geographical areas through hardware interfaces. With OT, information exchanged between two points depends on stringent networking requirements such as latency and packet loss ratios set by Application Programming Interfaces (API). A focus on operational data dependability typically characterizes OT environments, stemming from the time-critical nature of these machine-generated values such as volts, amps, bars, and breaker status (Farhat and Mueller, 2020). Since operational data are exchanged within and across industrial environments and need to be made available and routed for authorized personnel and machines in real-time, the requirements for constant availability of data often precede confidentiality or even integrity (Anton et al., 2017; Murray et al., 2017). OT's most notable distinguishing marker as far as security is concerned is its prioritization of 'uptime.' An unfortunate byproduct of this prioritization is a much longer replacement cycle for hardware and

[3] Other low-level class of systems include Programmable Logic Controllers (PLCs) and Distributed Control Systems (DCSs)

software, which have often led ICS to run environments with known vulnerabilities (Heritage, 2019).[4]

OT development and deployment currently revolves around twenty mostly analog and proprietary industrial protocols, with the most significant market share per vendor in 2019 at around 15% (Li, 2020). These legacy assets and devices were historically air-gapped from other networks, i.e., they mainly operated independently from IT systems.[5] Today, however, the demands for availability and productivity has shrunk those air gaps while the mitigation practices needed to counteract the increased risk posed by interconnectivity remain lacking in several technical, organizational, and institutional respects (Campbell, 2018).[6]

7.1.2 The introduction of IT in the energy sector

The Public Utility Regulatory Policies Act of 1978, 16 § USC 2601 set efficiency as a public policy goal for utilities and altered the return-on-investment calculus. Energy technology shifted towards efficiency models as Schweitzer introduced microprocessor-based digital relays in the 1980s, making IT integration feasible (Acromag, 2005).[7] The

[4] In fact, 20-year validation periods for new technology products are commonplace for risk-averse energy utilities seeking to fully depreciate their investments (Wirtz, 2019).
[5] Many proprietary industrial protocols lacked means of authentication and credential management capabilities due to their closed-loop nature i.e., hacking these systems would have required knowledge of specific architectures and physical access to components. The addition of remote maintenance interfaces connected via the internet has therefore increased firms' potential exposure of their 'crown jewels' i.e., their most valuable information-based assets to be protected.

[6] Further, the security provided by air-gapped networks is often overstated given the availability of technologies specifically designed to bypass them e.g., malware implants on EarPods inserted with a human agent (Anonymous, personal communication, 2016).
[7] A byproduct of Moore's law is the continued decrease in the manufacturing cost of microprocessor-based devices. For example, the decreasing cost of switches has allowed the targeting of a packet to a determined n ports (a hub in a star topology) rather than forwarding to the sum total N switch ports, thereby eliminating collisions and enabling more deterministic networking.

pressure of continuous expansion, market competition, and the modern requirements for safe and predictable energy distribution, such as two-way data communications, have accelerated public internet use in ICS networks and initiated a convergence between IT and OT in the energy sector (Eisenhauer et al., 2006).[8] This convergence has , increased the interdependence of cyber and physical while simultaneously creating vulnerabilities at the edge of the distribution grid for lack of two-way communication and regulatory oversight (FERC/DOE, 2019).[9] The use of a scalable and interoperable general-purpose networking technology for distributed computing meant that convergence on the internet, was almost inevitable.

As IT and OT continue to consolidate, functions that used to require separate hardware components were unified in one physical box while maintaining logical separation, therefore requiring a rethinking of information management at the enterprise level (Ibid). The early 2010s saw an uptake of internet of things devices, an environment notorious for insecurity. The industrial equivalent followed suit driven by the promise to improve operations' performance, including efficiency, reliability, productivity, safety, and the like. However, different market demands and regulatory requirements implied a differential convergence rate between both environments. That convergence continues today as microprocessor-based devices proliferate, aided by powerful new data management, machine learning, and other techniques for algorithmic scalability (Farhat and Mueller, 2020). While the convergence rate *per se* is an impractical question to answer, demarcating important industrial networking milestones allows for a pseudo-

[8]

[9] Critical Infrastructure Protection Reliability Standards do not apply at the distribution part and edge part of the grid.

treatment effect, especially in comparing how threat conceptualizations evolve in the USG. For example, proprietary buses such as Controller Area Network (CAN bus) were primarily involved with serial data communication. However, the advent of IP-based solutions such as Modbus TCP or DNP3 have facilitated convergence with the adoption of more open, low-cost, and minimum hardware requirement since at least 1997 (Swales, 1999). Affordable and off-the-shelf serial to digital convertors have been available since 2010, and the trend of integrated black-box solutions has accelerated from 2010-present.[10] The timing of many of these transformations, as will be made evident in this paper, is inconsistent with that of their associated threat conceptualization in the USG.

[10] Buses and gateways that convert from serial OT to digital IT and vice versa include 5201-DFNT-DNPM, Moxa NPort 6110, VLINX MODBUS, and PLX31-MBTCP-MBS (Shahzad et al., 2016).

Table 6:The security environments of IT and OT

	Secures	**Security priorities**	**Updates**	**Software**	**Type of data**[11]
IT	Software	Confidentiality & Integrity over availability	Frequent	Open-source, *de facto,* and standardized networking protocols. Proprietary data analysis software	Nonoperation-al e.g., digitized wave form, maintenance information on the circuit breakers.
OT	Hardware and software	Availability over integrity and confidentiality	Infrequent	Proprietary and/or standardized networking protocols and serial communications	Operational e.g., Volts, amps watts bars

Table 6 documents the mismatch between the security environments of IT and OT. The difference has been attributed to different security cultures (Murray et al., 2017). While many security issues plaguing IT, such as credential management, memory corruption, and missing encryption, are prevalent in OT, the mismatched security priorities and different compliance standards between both environments present challenging internal information management practices (Farhat and Mueller, 2020). IT/OT convergence impacts the consumer sectors i.e., botnets using lax security of cheap IoT devices as a

[11] See (Farhat and Mueller, 2020).

transmission vector to compromise other systems and the whole network loses usability as a consequence.[12] A variant of this problem is referred to as the monoculture issue, or, the downsides of having a single type of component or operating system dominating the market, which increases the likelihood of infection (Anton et al., 2017; Lewis, 2020; Roberts, 2014).[13] As such, IT/OT convergence presents a combinatorial explosion that greatly amplifies the number attack vectors and increases the potential negative network externalities. In an OT environment, 'uptime' or accessibility is prioritized due to the criticality of ongoing operations. In an IT environment, however, the security priority will depend on the application in question, such that integrity or confidentiality may supersede accessibility requirements. Table 4 provides a conceptual demarcation (modified from Murray et al., (2017)) of the general tendencies prevalent in both operating environments. The nuances in the differences and patterns of convergence are crucial to understanding how threats may be conceptualized.

7.1.3 Focusing cases behind IT and OT convergence as an emerging cybersecurity threat

The following account of cases is non-exhaustive; it includes only ICS-based incidents that help contextualize IT/OT convergence as a valid emerging cybersecurity threat to CI.

That said, it is essential to note that there has never been a loss of load in North America due to a cyber-attack (FERC/DOE, 2019; GAO 2019).[14]

---

[12] In a relentless race to find the most cost-viable product, many IoT manufacturers have skimped on security for their devices in terms of authentication, access control, and lack of support.

[13] PLCs running an underlying operating system will use modified IT modified for industrial applications, for example, the Windows operating system.

[14] Despite that fact, and as evidence of rampant Congressional threat inflation, Rep. Maria Cantwell (D-WA) erroneously claimed in Senate Commerce, Science and Transportation Committee hearing on 5G

US public attention was first captured in 2007 by Idaho National Labs (INL)'s "Aurora Generator experiment."[15] INL showcased how ICS for energy generators could be sent a series of on and off commands via open networking protocols to reverse their polarity while they operate, thereby causing their destruction (Di Stasio, 2017; Anderson and Fuloria, 2010).

Around the 2009-mark, media reports of ICS vulnerabilities intensified. The WSJ relayed concerns from current and former national-security officials that China and Russia were actively conducting reconnaissance to map the US electric grid and ICS networks (Gorman, 2009).[16] According to a Northrop Grumman report to the US-China Commission, media attention around that time stemmed from Chinese government-sponsored research into the analysis of US grid vulnerabilities (Wang, 2012; Wang and Rong, 2011, 2009a, 2009b). However, seeing as cascading failures of the power grid was an issue of interest to the academic community at the time and was not particular to Chinese universities, the open-source Chinese research was likely not a product of Chinese military or intelligence services (Krekel et al., 2014).[17]

---

technology and Cybersecurity on March 4, 2020, that “just recently an attack on our grid in the west was the first time an actor had actually brought down a power system for more than 12 hours. So it’s no longer just people searching around and looking at our power plants, now actors are starting to bring what are essential services to a halt (Cantwell, 2020).”

[15] While previous cyber-physical incidents existed, most were accidental and did not capture public attention, see (Hemsley and E. Fisher, 2018).

[16] In 2010, the WSJ also revealed how the NSA's increasing suspicion of Russian and Chinese surveillance efforts prompted the "Perfect Citizen" program, which sought to complement the EINSTEIN 3 federal network monitoring system in the private sector (Bellovin et al., 2011).

[17] The Northrop Grumman report also stated that despite the fact that Chinese cyber intrusion of US networks were based on stealing IP using common methods of network intrusion, media and industry reports over-inflated their threat because many US organizations were unprepared to deal with them. (Krekel et al., 2014).

The primary focusing event of the early 2010s remained the Stuxnet malware which targeted the Iranian uranium centrifuges at Natanz in November 2007 (Turner, 2010).[18] The Director of Symantec's Global Intelligence, which first discovered and analyzed the malware, called it "a wake-up call to critical infrastructure systems around the world" (Ibid). As the first ICS-specific malware deployed to effect, Stuxnet created a distinction between cyber-attacks with physical ramifications from the more commonplace ICT-based exploits used as means of gaining network access and enabling lateral movements for different ends.[19] This new category of cyber-attack was exclusively tied to nation-state capabilities since air-gapped systems isolated from the internet require the exceptional skill and extensive effort that only a nation-state can muster (Odlyzko, 2019).[20] In other words, cyber-physical attacks are not likely to cause wanton destruction and collateral damage unless purposefully intended by a nation-state actor. Despite pundits in the media continuing to refer to network intrusions as “attacks,” Stuxnet created a clear distinction between cyber-attacks with physical consequences and those whose effects are contained in the IT space.[21] As the race for improving attribution

[18] Other ICS-based attacks around the time include the “Night Dragon” operation which targeted global petrochemical companies (Kirk, 2011) and the Islamic Revolutionary Guard Corps (IRGC)’s forays into the ICS network of a New York Dam.

[19] The advanced nature of the reconnaissance effort behind Stuxnet i.e., the theft of highly secure digital certificates and the use of a previously unbeknownst software vulnerability known as a zero-day exploit made for a "smart" malware that does not deploy unless certain conditions are met, such as finding the correct model of Siemens Programmable Logic Controllers (PLC) (Hemsley and E. Fisher, 2018). Stuxnet and its other variants known as Duqu/Flame/Gauss have been attributed to a joint US-Israeli effort due to the advanced hacking techniques combined with the nature of the target and geo-political environment.

[20] That said, nation-states more commonly conduct less technically sophisticated infiltration techniques via proxies such as social engineering, spear-phishing, and other non-zero-day-based exploits.

[21] Bearing in mind that compromises to data confidentiality, integrity and accessibility can in the right circumstances be just as if not more consequential than physical destruction.

capabilities continued to intensify, Stuxnet opened strategic opportunities enabled by a new arsenal of tactical cyber capabilities ranging on a spectrum from covert with limited visibility to overt and destructive (Cole, 2019).[22]

7.2 IT/OT convergence threat idea breakdown

IT/OT convergence is a longstanding area of concern in many industry sectors. It amalgamates two different development paths in terms of economic, professional, and security cultures. At face value, IT/OT convergence is qualitatively distinct from artificial intelligence or quantum computing in that the phenomenon is not sought after as part of a competitive or strategic race. Instead, it is an unintended byproduct of technological evolution that demands reconceptualizing cybersecurity and public risk mitigation. However, since the word has yet to stabilize around an authoritative and functional definition of IT/OT convergence accepted and understood by all sectors, this chapter uses it to capture beliefs and perceptions of threats relevant to cyber-physical systems.[23] This vagueness is especially suitable since experts disagree on whether the complexity of decentralized control systems resulting from IT/OT convergence is conducive to more or less security (Enose, 2014; Meyers, 2013; Slayton and Clark-Ginsberg, 2018).[24]As a result, the distinction between beliefs and fact-based assertions is rendered moot for two

[22] For more detail about strategic considerations of offensive cyber operations (OCOs) see (Gartzke and Lindsay, 2015; Harknett and Smeets, 2020; Jensen et al., 2019; Valeriano et al., 2018).

[23] Ehie and Chilton (2020) proposed IT/OT convergence to be "the integration of information technology systems used for data-centric computing with operational technology systems used to monitor events, processes, and devices and make adjustments in enterprise and industrial operations." A more nuanced theory of technology's impact on society consistent with the PRF will account for political-economic effects and governance dynamics as complementary causal factors.

[24] The current state of ambiguous security applies to data managed on or off-premises via cloud services by third-party providers ((Farhat and Mueller, 2020; Slayton and Clark-Ginsberg, 2018).

reasons. First, despite many networking intrusions into US ICS, cyber-physical attacks have yet to cause a loss of load on the North American grid. Most threat concepts, therefore, are speculative. Given the ambiguous nature of the term and the uncertainty over the implications of the varying levels of CI security, analysis of proposed policy ideas and solutions reveals even more about the political bargaining behind policymaking. With continued convergence, ideas from the IT sector and the USG intruded on the energy sector as an internal tug of war was waged.

While the main ideas are chronological and cumulative, they cannot be demarcated by exact dates or administrations. Instead, many elements, including technological change, focusing events, and endogenous politics, will be shown to drive the problem-solution conceptualization. Dates are selected around focusing events that mark the clearest possible turning point. Figure 10 below demarcates how the idea of IT/OT convergence evolved as a threat presented by policy entrepreneurs and accumulated into three conceptual variants.

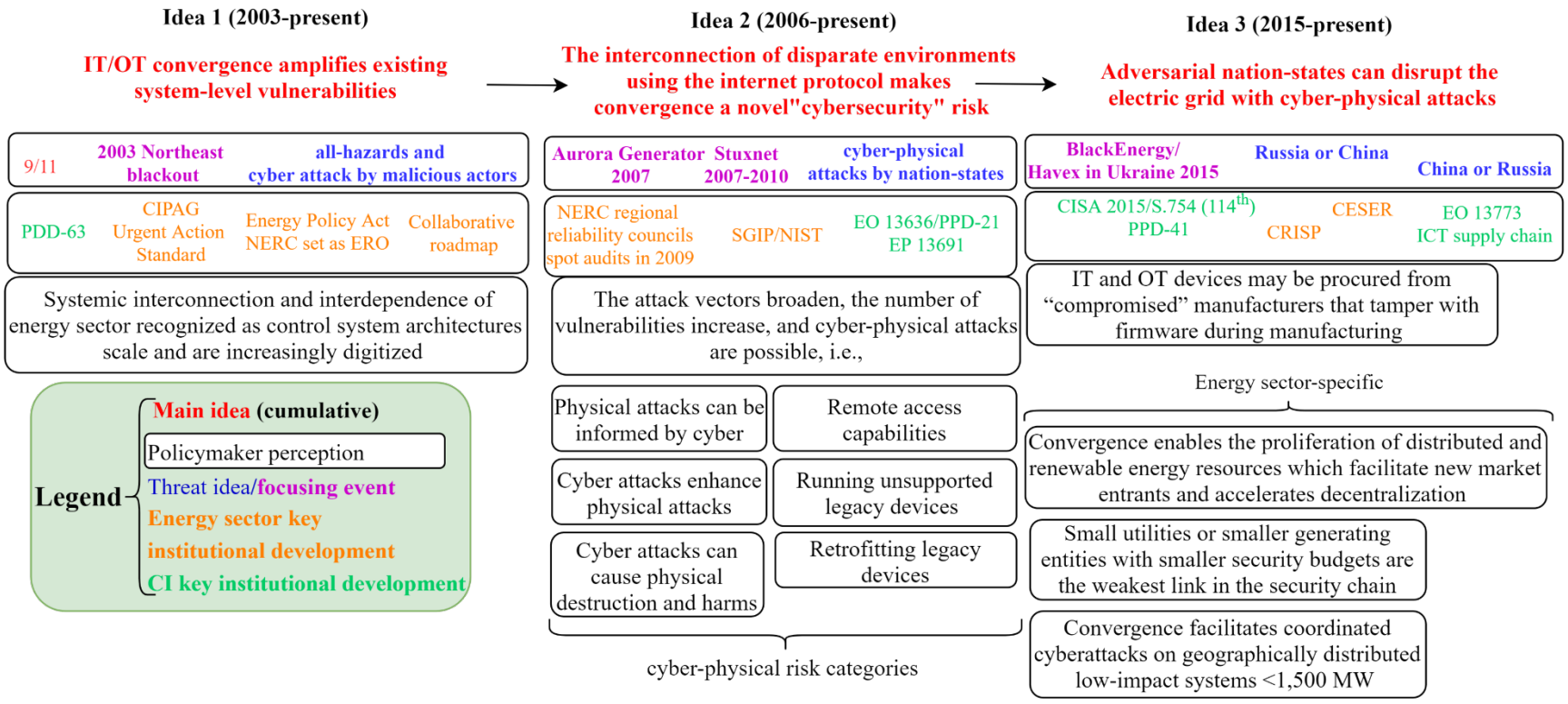


Figure 10: Two decades of ideas around IT/OT convergence

The themes shown below the main ideas follow the cumulative pattern and data collection method set in chapter 7 with the addition of in-depth, semi-structured interviews with energy firm executives and academics studying data analytics in the energy sector.[1] While many institutional changes can be easily determined, the proposed timeline is not a hard demarcation that traces how ideas accumulate. However, the threat ideas and themes behind those changes are more loosely associated with institutional change and closely tied to focusing events in red. The following section summarizes the themes; they will be explored in greater detail later as endogenous sector politics will be shown to bridge the gap between threat ideas and institutional change.

Phase 1: *IT/OT convergence amplifies existing system-level vulnerabilitie*s

In the first phase, all CI sectors, not the energy sector specifically, are conceptualized as having emergent interdependencies (PDD-63).[2] In phase 1, the different security priorities of networking and energy system engineering influenced the FERC/NERC regulatory model, especially after a combination of human and software error caused the 2003 Northeast blackout.

[1] As an example of how the themes are cumulative, the security and academic consensus maintains that the quantity and complexity of cyber-attacks on ICS are increasing and worsened by the proliferation of the internet of things devices first in the industrial market and more recently in the consumer space (Symantec, Dragos, Kaspersky).

[2] The energy sector being the most important, followed by the combined lifeline sectors including energy.

Phase 2: *IT/OT convergence is a novel "cybersecurity" risk due to the interconnection of disparate environments and the uniform reliance on the internet protocol.*

The evolution from phase 1 to phase 2 involves broader recognition in the energy sector and the USG that CI sectors are increasingly digitized and unified by IP. IT/OT convergence is now considered a problem involving qualitative change instead of scale and interdependence. In phase 2, decreasing hardware costs allow the deterministic networking requirements of energy sector OT to be increasingly resolved by IT as the electromechanical power grid accelerates towards a digitized "system of systems" (SGIP, 2010). Utilities start migrating towards digital substations, increasing perceived risk due to the combined systemic interdependence and unification by IP. As ideas accumulate, vulnerabilities are thought to be introduced by technological evolution, i.e., the interconnection of disparate environments and the uniform reliance on the internet protocol. As a result, the attack vector is thought to broaden, and the number of vulnerabilities is believed to increase.

Phase 3: *Adversarial nation-states can disrupt the electric grid with cyber-physical attacks*

In Phase 3, cyber attacks on the Ukrainian power grid captured Congress's attention and solidified the idea that adversarial nation-states can launch cyberattacks to disrupt the grid physically. In this phase, the energy sector remained more concerned with the operational and institutional/regulatory components of IT/OT convergence around grid interconnection points. Accelerating decentralization through the proliferation of Distributed Energy Resources (DER) and renewables created a perception of vulnerability with the energy sector, particularly around the distribution part of the grid,

since interconnection points escape federal regulations. Market entrants and small utilities with smaller security budgets are now the weakest links in the security chain. In this period, the energy sector generally considered its top threats in decreasing order, the rapid growth and use of digital technology, all-hazards defined as severe weather and storm, Electro-Magnetic Pulses (EMPs)), cross-sector dependencies, and finally, supply-chain compromises. However, ideas of China's threat on CI diffused from the White House, the ODNI, and the IT sector to energy. The USG starts focusing on Russian and Chinese-based compromises to the ICT supply chain but quickly reverts to China after the ODNI readjusts national security priorities. The novel threat during this period is that rival nation-states can compromise ICT supply chain and bulk power systems' equipment to mount cyber-physical attacks on the grid

As such, compromises in the ICT supply chain can facilitate cyber-physical attacks. A commonly cited example is how IT and OT devices may be procured from companies whose firmware is "compromised" during manufacturing.

Chapter 7 showed how ideas from the military and IC community encroach on the civilian cybersecurity regime. The intersection of both the Chinese threat and IT/OT convergence was hypothesized as borne out of military concerns of the asymmetric warfare capabilities of adversarial nations. As the analysis in this chapter will show, despite many focusing cases, mobilization in the cybersecurity regime around IT/OT convergence was mainly confined to the energy sector in the first and second phases. In the third phase, the resurgence of great power competition solidified nation-states with active offensive cyber operations capabilities as the only relevant actors able to leverage

increased digitization to mount attacks on critical infrastructure. However, those ideas are not sufficient to integrate the cybersecurity regime.

Despite a preponderance of Russian-based ICS-exploits revealed around the time, the threat of Chinese ICT encroached on the energy sector as policies diffused throughout the USG in the Trump administration, particularly concerning supply chain security. Generally, politicians in Congress and agency bureaucrats wanted more cyber-physical security while energy sector operators consider cyber-physical security appropriate. More importantly, as the analysis will show, the "all-hazards" resilience approach was unable to mobilize a whole-of-government response, especially when compared to the threat of Chinese ICT in the form of supply chain security. Similarly, threat vector variants of IT/OT convergence were insufficient to integrate the cybersecurity regime compared to China. Its effect was instead sector-specific.

7.3 How USG policy responded to IT/OT convergence

7.3.1 First idea: IT/OT convergence amplifies existing system-level vulnerabilities

In the formative days of critical infrastructure protection, PDD-63 was motivated by a broad scope of disasters as discussed in chapter 5 – but the interagency coordination body responsible for implementing PDD-63, the Critical Infrastructure Coordination Group (CICG), was convinced of the looming dangers of cyberspace.[3] CI sectors interdependencies were therefore thought to worsen by cyberspace and increasing digitization. As detailed in chapter 5, Lewis (2020) describes the governance issues of the

[3] Addressed in chapter 6.

initial phases of CIP, including how the original Homeland Security Act and the ensuing Bush administration Homeland Security Presidential Directive (HSPD-7), which sought to replace PDD-63, were the genesis of the institutional structure of CIP. While many of the early CIP governance issues are outside the scope of this work, it is worth noting that HSPD-7 did not assign a single sector-specific agency for energy and ICTs, clouding the issue of responsibility for CI. According to Lewis (2020), the purpose of HSPD-7 may have been to address a debilitating level of bureaucratic competition after the DHS amalgamated 22 different agencies in the USG and left other agencies out of the National Strategy. However, according to the Congressional Research Service, the Bush Administration may have enacted HSPD/7 to reflect a shift in motivational focus from cybersecurity to physical threats after 9/11, thereby causing "organizational instability" (Moteff, 2015). Regardless, HSPD-7 was an incoherent policy design effort for CIP overall. It left responsibilities unspecified and scattered across different departments. Unsurprisingly, terrorism was considered the likely source of risk instead of nation-states. However, as pointed out in chapter 5, while the threat idea was all-encompassing, sector stakeholders pursued their agendas in ways that reflected their historical ways of conducting business, and the Homeland Security regime remained "anemic" due to implementation discrepancies (May et al. 2011).

In energy, CI owners and operators have recognized the high degree of interdependency early on as raising the stakes of cascading and simultaneous failures (Anderson and Fuloria, 2010).[4] After the 2003 Northeast blackout, an institutional review at NERC

[4] Complexity was also cited as the intersection of interconnectivity and interdependence. As more business units gain access to operational and non-operational data, system-level security considerations include the

initiated the path of mandatory cybersecurity standards for energy generation and transmission (Slayton and Clark-Ginsberg, 2018). The design of CIP standards at the time proved to be an exercise in security cost avoidance that simultaneously allows the industry to maintain a state of self-regulation over federal regulations (Campbell 2011; Reilly 201; Jacobus & Waller 2016; Slayton and Clark-Ginsburg 2018). In all three phases, NERC debates around CIP standards revolve around a frame of return on equity for their security investments. The economics of information security are such that "technical feasibility" (i.e., the language of CIP standards) is designed to be compatible with "business judgment," i.e., OT cybersecurity costs that account for asset amortization. Overall, policymaking around phase 1 was disjointed and sector-specific, i.e., Congress and the federal government failed to propose integrated, cross-sectoral policymaking on cybersecurity, which was still an emerging issue at the time. The ensuing discussion of phase 2 starts with the evolving nature of the threat and then focuses on how DHS's ever-expanding authorities hijacked CIP debates and widened the gulf of disjointed policy implementation with the DoE on CIP oversight.

7.3.2 Second idea: IT/OT convergence as a novel "cybersecurity" risk that is leveraged by nation-states for physical effect

In the mid-2000s, the security of North American power is subject to oversight by the DoE and the DHS. While the threat conceptualization of IT/OT convergence influenced the development of cybersecurity policy for CIP in the energy sector from 2003 onwards,

diversity of stakeholders from utilities, OEM manufacturers, service providers, and consumers become relevant. While the "servitization" of the energy sector this offers multiple advantages for both efficiency gains and strategic business growth, a shift to services creates an environment where market segmentation introduces system-level security vulnerabilities. For more details refer to (Farhat and Mueller, 2020).

the energy sector has been aware of interdependence and unification by IP since at least 2006.

A critical networking requirement for industrial control applications is deterministic networking i.e., the ability of a communication protocol to guarantee that a message is sent or received in a finite and predictable amount of time (Acromag, 2005). As hardware costs continue to decrease, the deterministic networking requirements of energy sector OT are increasingly resolved by IT. The rate of IT adoption accelerates with the release of Modbus TCP (ca. the year 2000) and later with the standardization of the DNP3 suite as IEEE 1815 (ca. 2010), both enabling new functionalities, efficiencies, and services. As the electromechanical grid continued to digitize, IT/OT convergence was now considered a problem involving qualitative change rather than mere interdependence due to the interconnection of disparate environments and the uniform reliance on the internet protocol, therefore compounding the threat vector. Utilities start migrating towards digital substations, increasing perceived risk due to the combined systemic interdependence and unification by IP.

In 2006, the DoE and the DHS commissioned a sector-wide consensus study, the Roadmap to Secure Control Systems in the Energy Sector (henceforth referred to as the Roadmap). The central vision of the Roadmap was to lead the energy sector towards a state of resilience defined as the ability to "survive intentional cyber assault with no loss of critical function in critical applications" (Eisenhauer et al., 2006). The Roadmap reflects the deep understanding of owners and operators in 2005 of the technical, organizational, and institutional problems related to infrastructure protection, and many are still relevant today. The industry was aware of the risks of unifying the energy sector

through the internet protocol. The increased interconnectivity through IT creating new auxiliary connections from the operating system to the lower-level networking layer was considered a "fresh point of entry for prospective cyber attacks" especially given the inherent insecurity of legacy OT systems (Eisenhauer et al., 2006).

Similarly, the perennial problem of information sharing was emphasized along with the "uncertainty on how information will be used, disseminated, and protected." The Roadmap recognized that the PPP was "still clarifying their respective roles and responsibilities in this [CIP] area." While cross-sector mechanisms existed early in the form of SSCs, the lack of institutional capacity for a whole-of-government effort was regarded as detrimental. The operators explicitly called integration through a single federal office designated as a responsible entity for overseeing control system security within the energy sector. That designated agency would later become the DoE with the 2015 FAST act. However, the original silos of Homeland Security separating energy, information technology, and communications continued to manifest the disjointed implementation, particularly in terms of information-sharing.

In retrospect, the roadmap underestimated the industry's capacity to migrate past legacy systems. Such considerations are influenced by the economics of information security, i.e., balancing asset amortization against mandatory cybersecurity requirements.[5] IT/OT convergence also later initiated unforeseen changes at the organizational level of energy

[5] For example, deregulation the increased volume of energy transactions and ensuing competitive environment have created "narrower operating margins for energy providers" i.e., absent mandatory standards security standards, security budgets shrunk. When the NERC CIP regulatory regime was enacted, transmission operators were removing routable communications to avoid complying regulations and face hefty fines (Anderson and Fuloria, 2010).

firms around industrial data management.[6] Finally, the Roadmap expresses two broad concerns increasingly relevant today—first, the need for new "control system architecture" in providing needed network segmentation.[7] Second, operators flagged "offshore reliance" as a potential security concern in one of the earliest country-of-origin bases proxy for trust and hardware security.

The Roadmap was followed by the start of the audit-based enforcement of the NERC CIP Reliability Standards suite in 2009, setting a new institutional era of mandatory cybersecurity regulations for the energy sector (Anderson and Fuloria, 2010).[8] Around the same time, high-profile cases of cyber-enabled IP theft were documented, as detailed in Chapter 7. However, the US lacked a comprehensive legislative framework to address these mounting cybersecurity concerns. Instead, various enacted statutes addressed multiple aspects of it (e.g., the Electronic Communications Privacy Act (ECPA), the Computer Fraud & Abuse Act, the Homeland Security Act (HS), or the Federal Information Security Management Act (FISMA). As broad consensus formed around the specific areas that needed to be addressed in the 111th Congress (2009-2011), mainly related to the internet economy, legislators first proposed to amend pre-existing bills but failed to gain significant traction (Fisher, 2014). However, congressional mobilization on cybersecurity ramped up in the 112th Congress, with 38 hearings and four markups in the

[6] For more details about organizational-level changes brought about IT/OT convergence refer to (Farhat and Mueller, 2020).

[7] The lack of such valid operational architecture today speaks to [not insufficient market need really, it could be the momentum is too strong] the economies of scope and scale afforded by the internet protocol that would need to be overcome in implementing fundamental network upgrades to accommodate the industrial sectors.

[8] The DoE/DHS Roadmap stemmed from a workshop in 2005 involving energy sector CI operators and government representatives.

House and 38 hearings in the Senate (Fischer, 2014). Overall, the threat of IT/OT convergence was poorly defined in Congress and tacitly regarded as a mere quantitative expansion of dangers best addressed through the ICT sector. Relevant congressional hearings at the time also gloss over the nuance between CI sectors' growing interdependence *per se* with their increased interconnection by uniformly relying on the internet protocol as a risk *sui generis*. The first explicit Congressional reference to IT/OT convergence as a threat distinct from CI interdependence was referred to by an ODNI report. In a Subcommittee hearing on Oversight and Investigations for the House Energy and Commerce Committee in March 2012 titled IT Supply Chain Security, Rep. Degette references the ODNI referencing "network convergence (Clapper, 2011)." She brings the issue up with Lawrence Castro, CIO of DoD at the time, based on the concern that "everything are [sic] all converging on one common network (Energy and Commerce Committee, 2012) ." Castro defined convergence as a threat based on the weakest link in the chain argument "where we rely upon each of the devices in an integrated way (...) the problem there is that vulnerability on one part of that chain is easily introduced into the other parts of the chain (Ibid)".[9]

Despite the lack of explicit threat association with convergence in Congress, a series of proposals for comprehensive cybersecurity legislation was lobbied as cybersecurity concerns continued to gain salience. These proposed bills represented by figure 11 allow the demarcation of political interest groups and explain why frustrated with a

[9] In that same hearing, Rep. Stearns lamented the lack of policy integration in the federal government to address ICT supply-chain risk but did not allude to any specific nation-state actor. An expert witness representing a global security and risk management firm further corroborated that assertion stating that nation-states are the only relevant actors to supply chain compromises of ICTs at the manufacturing level.

compromising Congress, the executive passed EO 13636/PPD-21.[10] During this period, the protection of CI and the electric grid, including information sharing and cross-sector coordination programs, reveal a cybersecurity regime riddled with endogenous, sector-specific political tensions over the responsibilities and authority of federal agencies, especially given the lack of a unified national cybersecurity strategy in the face of a growing threat landscape.

7.3.2.1 PPD-8 - March 2011

Through its use of the notion of "resilience," the Obama administration's *PPD-8* in March 2011 set the assumptions and imperatives of CIP for the entire era. The directive is "aimed at strengthening the security and resilience of the United States through systematic preparation for the threats that pose the greatest risk to the security of the Nation, including acts of terrorism, cyber-attacks, pandemics, and catastrophic natural disasters (PPD-8, 2011)." The logic behind hardening critical targets against "all-hazards" is based on a recognition that systems have emergent properties and that resources are limited. Given the backdrop of consecutive natural disasters within the years before its passage, the motivating threat idea for CIP remained 'all-hazards resilience.'[11] The CI label now encroached on every sector of the national economy, numbering at 18. Further, by relying on the "all-hazards" approach to resilience, which includes cybersecurity risks to CI among a lengthier list of threats, PPD-8 reinforced the CI security partnership voluntarily. The directive's scope and language were kept broad, given the target

[10] A broader compromise between the executive and legislative branches was later reached in 2015 with the Cybersecurity Information Sharing (CISA) Act.

[11] In the few years before its passage the US witnessed wildfires, floods, hurricanes, and the Texas fertilizer plant explosion. Resilience was later operationalized by PPD-21 in 2013. The standard risk assessment methodology defined risk as a function of Threat, Vulnerability, and Consequences (Lewis, 2020).

audience's diversity, ranging across all government, private, and nonprofit sectors. However, within-sector inconsistencies prevailed, highlighting the diffuse nature of responsibility in the PPP. For example, while specific industries such as oil and gas were part of the energy sector, they were only indirectly regulated and consigned to a nebulous PPP structure. In contrast, the electric power industry followed more stringent self-regulation and government oversight.[12]

PPD-8 is germane to the cybersecurity regime for reasons of institutional path-dependence, i.e., understanding the political forces that were the genesis of a new era of CIP.[13] While the scope of PPD-8 spans all of CI, the inability of the "all-hazards" resilience approach to mobilize a whole-of-government response effectively when compared to the threat of Chinese ICT a few years later (a more closely bounded policy problem) provides further evidence of the requisite structural, and ideational forces required for political mobilization. The nascent conceptions of IT/OT convergence and its association to “all-hazards” failed to adequately recognize the extent to which CI sectors were becoming unified by the internet protocol at the time. This recognition will be achieved in phase 2. The following section considers PPD-8's mobilizing impact on the nascent cybersecurity regime.

Given the US's federalist system of governance, the enactment of PPD-8 presented complex analytic and organizational challenges for the PPP structure responsible for protecting the country's CI. PPD-8 replaces and expands the scope of HSPD-8 by establishing five mission areas labeled as Prevent, Protect, Mitigate, Respond, Recover.

[12] CI sectors would later consolidate to 16 in 2013 with PPD-21.
[13] It was regarded as vacuous wishful thinking by some experts and a step in the right direction by others (cite Kahan)

The areas expand into 31 target capabilities that the WH designed to be implemented using a prioritization basis to minimize public risk, i.e., low probability and high consequence risk, which private actions alone cannot readily address (May & Koski, 2013). The implementing agency, the DHS, was tasked to develop a National Preparedness System to set the risk priorities in coordination with executive agencies and the rest of the PPP, thereby achieving, at least in principle, an "integrated, layered, and all-of-Nation preparedness approach that optimizes the use of available resources" (PPD-8, 2011).

The shared goals of PPD-8 established a new multi-level and whole-of-nation framework for voluntary coordination between public and private sector stakeholders. However, since CI stakeholders lacked an explicit mandate for inter-organizational behavior, including information sharing procedures, the DHS was expected to guide coordinative activity. The Obama Administration proceeded on another front by appointing the first White House Cybersecurity Coordinator, the "cyber czar," a position established to coordinate the executive management of cybersecurity. “Cyber czar” was a misnomer, as the WH did not grant the position control over budgets, and more importantly, the new position was not cross-cutting CI sectors.

7.3.2.1.1 Policy incoherence and resulting implementation

In theory, CIP policies were designed to reinforce each other, as balanced governance between federal, state, and the private sector was a recurring normative theme throughout the order. In practice, however, the top-down requirements of PPD-8 applied to the federal government but failed to provide any direct incentives for compliance to private sector infrastructure operators. The private sector, which owns 87% of the infrastructure,

was expected to voluntarily adhere to the National Preparedness document guidelines driven by self-preservation instincts.

Part of the CI operator's complaints with PPD-8 was the incoherence by which resilience was operationalized. Different stakeholders use different risk methodologies to define and measure resilience (Lewis, 2019). State governments follow the all-hazards approach for low probability, high consequence but all-encompassing public risks, while the private sector uses advanced statistical modeling to hedge against private risk in a way that optimizes for their bottom-lines.[14] Since private risk stemming from logistics and supply-chain concerns is fundamentally different from systemic cybersecurity risk as a public-private, boundary-spanning externality, the lack of differentiation amounted to incoherent policy design.

The implementation challenge with PPD-8 was argued to be due to an incoherent approach in assessing risk and measuring resilience. For instance, the directive did not specify methods for integrating and aggregating PPP stakeholders' preparedness levels, leaving the task up to the DHS and the Federal Emergency Management Agency (FEMA) as later outlined in PPD-21.[15] Several non-governmental groups later pressured the Obama Administration to operationalize resilience better, given the apparent goal deficit. A report by the Homeland Security Policy Institute Preparedness, Response &

[14] Misaligned incentives in cyberspace also involve the cross-purposes between intelligence gathering from public agency perspective and private sector entities that strive to swiftly contain and remove threats lest they impact their reputations and bottom-lines. Private industry wants to preserve their own interest, whereas law enforcement and intelligence services situation to evolve to preserve an audit trail to better investigate and gather intelligence.

[15] The DHS is a behemoth cabinet-level agency that actively protects federal civilian government systems and collaborates with the private sector to secure critical infrastructure and information systems, among other things as described in section 5.7 For a detailed breakdown of DHS's organizational structure, refer to the chapter appendix. https://www.dhs.gov/secure-cyberspace-and-critical-infrastructure

Resilience Task Force had concluded in 2011 that "The White House and the DHS must advance US capacity for resilience or else a loss of momentum will result in resilience being little more than a buzzword" (Kahan, 2015).

7.3.2.1.2 Integration, implementation, and motivating factors: the organizational failure of the DHS

PRF assumes that both substantive and political forces work to drive a regime's trajectory, among other things. PPD-8 was a textbook case of endogenous politics having a significant influence on the policymaking process. Its language was designed to give President Obama full credit for advancing national preparedness, given the lack of recognition of work done during the Bush administration (Kahan, 2014). The White House sought to reinforce its locus of control around CI information security management by further legitimizing and expanding the DHS's coordinative authority and decision-making mandate.[16]

PPD-8 did not provide measurable criteria for preparedness capabilities, which limited the integration of a nationwide national preparedness target. There were no defined criteria for success in implementation either. As a result, agencies responsible for implementation were struggling to achieve evolving objectives. GAO-13-637 stated that FEMA was making progress towards implementing PPD-8. However, at a USG-level, the capability gaps remained unclear, complicating the case for appropriations (Kahan, 2015). To make matters worse, as described in section 5.7, the DHS was plagued by

[16] For example, the DHS is also one of the unique institutions with section 806 authorities to block individual ICT vendors from federal networks as addressed in chapter 7.

"severe mismanagement," according to a bipartisan report from the SenateHomeland Security Subcommittee on Investigations (Rubio et al. 2012).[17]

In 2012, the GAO pressed DHS to go beyond a resilience framework and develop an implementation strategy that includes "steps needed to achieve results, by developing priorities, milestones, and performance measures; responsible entities, their roles compared with those of others, and mechanisms needed for successful coordination (…)" (Kahan, 2015).

However, as the following section indicates, interest groups in Congress had different approaches to the role of the DHS, which was reflected in their proposed legislation. The next section outlines the main differences.[18]

7.3.2.2 Political interests and their motivating ideas in the 111th- 112th Congresses

7.3.2.2.1 The Cybersecurity Act of 2012: the genesis of the IT/OT convergence problem in Congress

Proponents of the "Lieberman-Collins" cybersecurity Act asserted that their approach leverages the incumbent PPP structure with "carrots instead of sticks" (U.S. Senate Committee on Homeland Security & Governmental Affairs, 2012).[19] The proposed bill

[17] The CEO of a major utility company stated in an interview that "Homeland security in general is a big bloated thing, in my opinion, you should separate it out, create a new agency, and really make it small and efficient (…) I could never get Jeh Johnson's attention. What was he worried about? (…) immigration. That's all they care about."

[18] For this analysis, the House and Senate are considered equivalent bodies encompassing various interest groups unless otherwise indicated. It should however be noted that the House focused on bills with a narrow focus, and the Senate pushed more comprehensive legislation that typically combined approaches proposed by the Homeland Security and Governmental Affairs Committee (S. 3480), the Commerce, Science, and Transportation Committee (S. 773) (Fischerkeller, 2014).

[19] The bill sponsors were Sen. Tom Carper (D-Del.), Chairman of the Subcommittee on Federal Financial Management, Government Information, Federal Services, and International Security, joined Sens. Joe Lieberman (ID-Conn.), Susan Collins (R-Maine), and Jay Rockefeller (D-WV).

would have granted DHS significant new authority to assess and serve civil penalties on owners and operators of CI that were in noncompliance with the newly proposed cybersecurity regulations (Fischer, 2014). The failure of this proposal illustrates the significant structural differences between the ICT and energy sectors. The energy sector is the only sector with mandatory CIP Reliability Standards. The ICT sector, due to its diversity of industry verticals and suppliers, e.g., platforms, telecommunications providers, cloud services providers, was successfully able to lobby against mandatory cybersecurity standards.

S. 2015 was therefore opposed by the US Chamber of Commerce and House Republicans except for the immunity-for-information provision, later adopted in the CISA Act. Despite its failure, the proposed bill was foundational in first defining the idea of "cyber-physical systems" as physical or engineered systems whose networking and information technology functions and physical elements are integrated and actively connected to the physical world through sensors, actuators, or other means to perform monitoring and control functions.

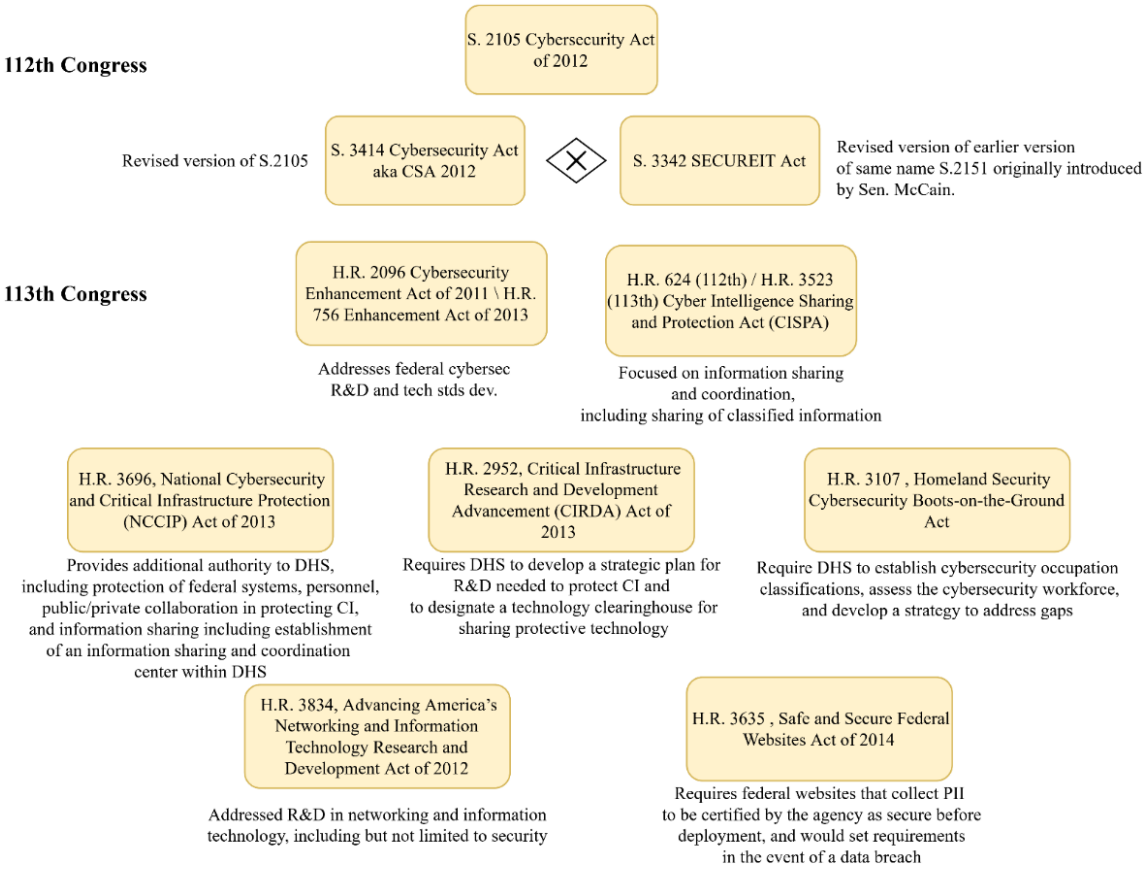


Figure 11: Proposed congressional action on cybersecurity, 111th-113th Congresses

7.3.2.2.2 The CSA 2012 vs. Secure IT Act: a sector-based and ideological interest divide

Disagreement over the different approaches to tackle cybersecurity continued as two major bills competed in the debates: Sen. Joseph Lieberman's S. 3414 and Sen. Hutchinson's CSA2012.[20]

[20] Both bills include a long list of co-sponsors however are only attributed using the main sponsor for brevity. The Secure IT act was co-sponsored by R Burr, Richard [R-NC] R Chambliss, Saxby [R-GA] R Coats, Daniel [R-IN] R Grassley, Charles "Chuck" [R-IA] R Hutchison, Kay [R-TX] R Johnson, Ron [R-WI] R McCain, John [R-AZ] R McConnell, Mitch [R-KY] R Murkowski, Lisa [R-AK]]. The CSA 2012 was sponsored by Sen. Joseph Lieberman and co-sponsored by Carper, Thomas [D-DE], Collins, Susan [R-ME], Feinstein, Dianne [D-CA], Rockefeller, John "Jay" [D-WV].

The original S. 2105. bill was heavy-handed, calling for mandatory cyber standards applying to all sectors of CI. The Lieberman group of representatives claimed that requiring mandatory standards was not onerous since they were developed "in consultation with the private sector" (cite hearing). After significant resistance from the Chamber of Commerce, privacy advocates, and other representatives, Sen. Lieberman et al. withdrew the regulatory framework that included mandatory provisions and amended their bill to provide incentives to adopt security practices and standards.

While both bills accounted for the need for antitrust immunities and information-sharing provisions, proponents of the Secure IT Act rejected S.3414 because regulations would be too burdensome on the private sector and that the DHS was not to be trusted with new authorities given their recent track record (cite testimony). The label of voluntary standards was thought to be a façade.[21] While the Lieberman bill allows the private sector to propose standards described as voluntary, the bill empowers federal agencies to make these voluntary standards mandatory. Given the lack of trust with DHS after the subcommittee on investigations report, their administration of a regulatory regime was thought to "lengthen and hamper the efforts to open information sharing (Hutchinson, 2012).

Early in the decade, one could expect smaller interest groups (constituents backing Lieberman et al.) to be more effective at mobilization than the larger groups (constituents backing Hutchinson et al.) endowed with a broader array of representational preferences (Olsen, 1965). Rent-seeking theory suggests that sectional groups such as Lieberman and

[21] If an agency does not make the standards mandatory, it would have to report to Congress the reason it had failed to do so.

Collins should be highly effective at exerting Congressional pressure in mobilizing political commitment and expanding DHS's authorities based on the perceived threat from cyberspace (Ogus, 2004). Collective action theory similarly predicts that small and easy to organize support groups such as those lobbying to expand DHS's capacity are likely to exert more significant influence on legislation than those representing consumers and other 'public' interests.[22] However, upon closer consideration of distributional outcomes, the larger interest group had a considerable advantage as it benefited a larger number of constituents with common interests. In this case, privacy advocates and civil society, along with Republicans in the Chamber of Commerce concerned with onerous regulations and ease of doing business, were united against the Lieberman bill. The transaction costs of self-organization and coalition-forming were worth overcoming.[23] In supplying information security as a public good, DHS was at the nexus of information control and security provision as a public good. The political bargaining was symptomatic of a broad array of constituent preferences that are historically useful to understand the conditions that allowed the eventual restructuring in 2018 with the Cybersecurity and Infrastructure Security Agency Act of 2018.

[22] It should be noted that Sen. Lieberman was foundational in the formation of the department of Homeland Security and along with Sen. Collins, a co-sponsor of his bill and served as the chairmanship of the Senate Committee on Homeland Security and government affairs for Sen. Collins.
[23] SECURE IT had support from businesses, nonprofits and business lobbies such as the US Chambre of Commerce, the national association of manufacturers, the American fuel and petrochemical association, the Petroleum institute, the internet security alliance and others.

7.3.2.3 Key takeaways from deliberations in the 112th Congress

7.3.2.3.1 Factors motivating coordination over information sharing

S. 2105 and S. 3414 would have permitted the sharing of lawfully obtained threat indicators among private-sector entities and the federal government. Federal entities could use and share such information for cybersecurity and law-enforcement purposes only.[24] A notable motivating factor prevalent with both bills is the urgency with which the cybersecurity threat was communicated. Part of the criticism of the proposed legislation by the US Chamber of Commerce, which stood in opposition to S. 3414, was that the bill "rushed to the floor without a legislative hearing or markup" (Josten, 2012). To further illustrate the over-inflated sense of risk urgency, Sen. Lieberman's claimed to be open to compromise because their group "didn't want to lose the chance to pass cyber legislation that could prevent a cyber-9/11 attack against the US before it happens instead of rushing amid mayhem after we suffer a major attack. (Lieberman, 2012)". The "all-hazards" threat frame traditionally used in framing CI protection debates and as used in PPD-8, was now married to cybersecurity as a policy problem used for mobilization purposes. Sen. Lieberman used a commonly cited threat list that first appeared in PDD-63: "the danger of cyber-attacks against the US is clear, present and growing with enemies ranging from rival nations to cyber terrorists, to organized crime gangs, to rogue hackers (Lieberman, 2012)". Sen. Durbin, Franken, Wyden, and others had instead argued the interests of advocacy groups who pressed for greater privacy protections in the Lieberman Bill.

[24] Sectoral coherence stemming from Congressional legislation has yet to be established because cybersecurity legislation had not passed in Congress yet. A minor exception involved China and foreign policy.

The WH was planning executive orders to that effect around September 2012; however, it had encountered opposition from Congress, still hoping to resolve its differences. At that point in the debate, the theft of intellectual property stemming from China was the only unifying policy problem related to cybersecurity that tied interest groups together.

On October 10, 2012, ranking Member of the Homeland Security and Governmental Affairs Committee, Susan Collins and others, urged the WH against issuing executive orders on cybersecurity policy citing transparency and legitimacy concerns and the need to further momentum with ongoing Congressional action on cybersecurity policy (Homel et al., 2012).[25] Another group of representatives directed similar preemptive pressure on the White House, warning not to exert regulatory influence over the internet in the name of cybersecurity (Rubio et al., 2012). The claim was that Russia, China, and Iran would be emboldened by a US cybersecurity regime with a top-down regulatory apparatus and thereby break away from the open private-sector-led multistakeholder internet. This surprising finding indicates that China's threat was used early in the regime by foreign policy-minded politicians concerned with the effects of domestic regulations as an excuse not to pass cybersecurity legislation. The irony is that the same representatives will openly advocate for a top-down decoupling from Chinese ICT a few years later. This position is a notable contrast to chapter 7, where the need for a better defense against the threat of China enabled a government-wide approach to cybersecurity.[26]

[25] Sen. Collins represented one of three major Congressional interest groups explored further in the section below

[26] Contrasting both positions will help better understand what factor contributed to this ideational leap, including how cybersecurity was associated with country-of-origin restrictions on IT.

7.3.2.3.2 The executive proceeds with EO 13636 and PPD-21

After several comprehensive cybersecurity bills were debated in Congress and failed, the White House issued PDD-21 and EO 13636 in February 2013 despite some Congressional opposition. The EO focuses on cyber threats to critical infrastructure while maintaining PDD-8's resilience approach.[27] At a high level, the White House directed the Federal Government to coordinate with critical infrastructure owners and operators to improve information sharing and collaboratively develop and implement risk-based approaches to cybersecurity. Presidential Policy Directive 21 (PPD-21), Critical Infrastructure Security and Resilience, expanded the scope of critical infrastructure protection. The perceived need for CI scope expansion was informed by "significant evolution in the critical infrastructure risk, policy, and operating environments (…)". The motivating threat frame was CI interdependence, evidenced by the updated 2013 National Infrastructure Protection Plan (NIPP).[28] The era of 'resilience' and risk-informed decision-making after PPD-21 continued to be informed by the threat of CI interdependence in phase 1. However, updates to the NIPP involved following an enterprise approach to risk management that includes cyber and physical security conceptualized as separate threat vectors. The NIPP highlighted the risk of cyber-physical dependencies and the need to integrate them holistically by generally focusing on

[27] The White House included similar provisions from Congressional bills with the notable distinction of proposing to restrict the authority of state and local jurisdictions with regards to where commercial data centers are located (WH cybersecurity proposal, 2012).

[28] The National Infrastructure Protection Plan (NIPP) 2013 was the resulting overarching framework that sets tone, definitions and a specific mandate for the current state of the Critical Infrastructure (CI) regime. The effort was intended to harmonize systems, technology and information sharing between government and private industry has given the perceived increasing interdependence between sectors of critical infrastructure.

resilience.[29] It designated "lifeline infrastructure" as encompassing the Water, Energy, Transportation, and Communications sectors. Lifeline sectors are essential to themselves and all other sectors (White et al., 2016).

PPD-21 expanded DHS's Enhanced Cybersecurity Services (ECS) program for the near real-time and automated sharing of cyber threat information to CI operators. Practically, the more coordinative aspect resultant from the White House orders involved requiring federal agencies to generate unclassified cyber threat reports to be shared with the private sector while simultaneously establishing a system to track the dissemination of classified information to CI operators authorized to receive them. This program includes a capacity for CI operators to share information voluntarily with the government via Commercial Service Providers (CSPs) which act as a secondary clearinghouse after DHS. This incentive program allows CI operators, once vetted, to receive ECS services from eligible CSPs i.e., they would receive threat signatures from any of Verizon, AT&T, Centurylink, or Lockheed Martin (DHS, ECS, 2013).

Structurally, PPD-21 re-identifies 16 CI sectors, thereby providing a coherent update to pre-existing institutional structure. The risk management framework (RMF) outlined is to be implemented in voluntary cooperation with industry through Sector Coordinating Councils representing the sixteen sectors. As part of the new approach of the federal government's risk management, DHS was tasked with setting up two national CI centers, one for physical infrastructures and another for cyber infrastructures. In January 2015,

[29] The consensus over absolute security being unachievable, the USG focused on resilience, which PPD-21 defined as "the ability to prepare for and adapt to changing conditions and withstand and recover rapidly from disruptions.
Resilience includes the ability to withstand and recover from deliberate attacks, accidents, or naturally occurring threats or incidents."

President Obama visited the NCCIC to promote proposed legislation aimed at private sector cyber-threat information sharing (Obama, 2015). However, as discussed in chapter 6, institutional problems endemic to the PPP hampered the conception of novel policy solutions or implementation of voluntary information-sharing practices at the time. Since information sharing was the *de facto* success criteria for CIP governance, notable cyber incidents such as the Office of Personnel Management (OPM) hack in 2015 coupled with repeated warning calls by the GAO meant that USG efforts at institutional readjustment would continue to be perceived as inadequate.

7.3.2.4 Influence of the National Institute of Standards and Technology (NIST)

Early in the decade, Congressional mandates for grid modernization allowed North American utilities to continuously add smart grid devices to an aging grid in areas escaping federal regulation (Campbell, 2011).[30] The energy sector was aware of the threat of unification by IP early on. The Energy Sector Control Systems Working Group (ESCSWG) updated its Roadmap in 2011 to focus on cybersecurity and outlined a multistakeholder framework for resilient infrastructure capable of surviving cyber incidents while maintaining critical functions.

Congress, however, took longer to follow suit given how IT sector politics involving the DHS detracted entrepreneurs from institutional innovation or re-evaluation of cross-sector initiatives in the PPP.

The American Recovery and Reinvestment Act (ARRA) in 2009 funded NIST's smart grid interoperability panel SGIP, which was established as a PPP that defines

[30] The Energy Independence and Security Act of 2011 (EISA) title 13.

requirements for communication protocols and other common specifications and coordinates development of these standards by collaborating organizations (Campbell, 2011). NIST published NISTIR 7628 Guidelines for Smart Grid Cyber Security in August 2010. However, the GAO reported that NIST had largely addressed cybersecurity elements in their work but remained lacking in combined cyber-physical attacks (GAO, 2011).[31] According to a principal Smart Grid Interoperability Panel member, the NIST SGIP process effectively transitioned from government to private partnership in 2012, stating, "2012 was the year of transition (…) in 2013 I had 80 dues-paying members already. And then we developed the NIST information reports, through 7628 which was the guidelines on cybersecurity."

PPD-21 directed NIST to build a framework published for the smart grid as part of a nascent recognition of IT/OT convergence in the cybersecurity regime. As a result, the Cybersecurity Framework, published in February 2014, was intended to serve as the first national-level sector-spanning framework for cybersecurity. NIST developed it on stakeholder input to help ensure that existing work within the sectors, including the electricity subsector. It recognized that the electric grid is changing "from a relatively closed system to a complex, highly interconnected environment." (NIST-IR, 2014). NIST indicated that

[31] The NIST has recognized and studied ICT-based supply chain risks to federal systems early in the decade but was agnostic to country of origin and never mentioned China or Russia explicitly. NIST provides a long list of guidance documents on SCRM. Starting in 2012, NISTIR 7622 provides an array of best practices intended to help mitigate supply chain risk to federal information systems. NIST Special Publications 800-161 published in 2015 is a consensus report with consultation from private sector that guides federal organization practices for supply-chain risk. NIST also emphasized criticality analysis is key to supply risk management, publishing NISTIR8179 in April 2018. SP 800-37 Revision 2 Risk Management Framework for Information Systems and Organizations: A life Cycle Approach for Security, Privacy, and Supply Chain Risk was published in December 2018. NIST followed with an Interagency Report (IR) 8170, The Cybersecurity Framework, Implementation Guidance for Federal Agencies in March 2020. Finally, SP 800-53 Revision 5, Security and Privacy Controls for Information Systems and Organizations in September 2020. According to a DHS webinar, NIST may be planning to consider external suppliers more carefully in the future.

the implementation of cybersecurity requirements is first a function of deterministic evolutions in the technology given rise to emergent system-of-systems properties, and second, changes in exploitation techniques.[32] In September 2014, NIST/SGIP published NISTIR 7628 Revision 1 Guidelines for Smart Grid Cybersecurity to provide an organizational system-level risk methodology to identify and mitigate cyber vulnerabilities for the smart grid. The SGIP defined the categories of threat to include: 1) Physical attacks informed by cyber; 2) Cyber-attacks enhancing physical attacks, and 3) Cyber-attacks causing physical destruction and harm. NIST states: "This approach recognizes that the electric grid is changing from a relatively closed system to a complex, highly interconnected environment. Each organization's cybersecurity requirements should evolve as technology advances and as threats to grid security inevitably multiply and diversify." As utilities migrated to digital substations, legacy grid devices were retrofitted with two-way communications capabilities to allow new functionalities or diagnostics. These legacy devices were either unsupported or involved challenging remediation techniques.[33] At the organizational level, the perceived threat vector was expanded by complexity, i.e., owing to combining the different security priorities in IT and OT.

The USG eventually caught on as cyber-physical attacks were demonstrated with Stuxnet and the Aurora generator experiment. The 2013 NIPP finally stated that: "[G]rowing

[32] Nation-states feature first on the list of adversaries. A few years later, nation-state adversaries and vendor country-of-origin will converge in meaning to become an almost synonymous category as the primary ICS cybersecurity threat-vector.

[33] Remediation for known vulnerabilities may not be feasible due to a lack of OEM support to provide firmware and software updates or a lack of willingness from operators to suffer downtime.

interdependencies across critical infrastructure systems, particularly reliance on information and communications technologies, have increased the potential vulnerabilities to physical and cyber threats and potential consequences resulting from the compromise of underlying systems or networks (NIPP, 2013)."

7.3.3 Third idea, 2015-present: Adversarial nation-states can disrupt the electric grid with cyber-physical attacks

The following section addresses how IT/OT convergence threat ideas evolved with the resurgence of great power competition and the attacks on the Ukrainian grid. In this phase, China 'hawks' in Congress discussed variants of convergence such as "digitization" as facilitating 'gray zone' warfare given new network entry points, outright military operations, or acting as a 'smoke screen' as part of a more significant invasion. The concern was that convergence would facilitate asymmetric warfare capabilities. The USG enacted EO 13636/PPD-21 and later PPD-41 to increase public-private cybersecurity coordination following the Ukraine events. During the Trump administration, the WH passes EO 13800, the National Cyber Strategy, and DHS releases its Cybersecurity Strategy. As the stakes of great power competition continued increasing, technical concerns around "strategic technologies" such as quantum computing, artificial intelligence, 5G standards, and networking architecture became salient in the cybersecurity regime. Around 2018, despite evidence of predominantly Russian activity on ICS systems, the threat of Chinese ICT prevails.[34]

[34] While the Chinese conducted an Intrusion Campaign on the US Gas Pipeline from 2011 to 2013, they have generally used more open-source exploitation tools, focused on IP theft and targeted espionage at government agencies (CISA, 2020).

7.3.3.1 ICS-based cyber incidents on the rise

Early in the decade, many nation-states with offensive cyber operations capabilities were catching up in developing the capacity to attack critical infrastructure (Hemsley and E. Fisher, 2018). The trend of cyber incidents reported on ICS increased more or less linearly, as the data in table 7 indicates.[35] The DHS presumed that 55% of attacks on ICS involved nation-state actors or proxies thereof leveraging APTs, a majority of which (around 80%) occurred in the energy sector (DHS, 2014).[36] Analysis of the Common Vulnerabilities and Exposures (CVE) list that tracks ICS vulnerabilities indicates that even though SCADA-based exploits are not as prevalent as purely IT-based compromises, they are an increasing concern for manufacturers starting around 2011 (Anton et al., 2017).

Table 7: ICS incidents and vulnerabilities[37]

Year	ICS-based cyber **vulnerabilities** reported	ICS-based **incidents** reported
2011	69 – 69	140
2012	192 – 79	197

[35] Sampling and underreporting biases notwithstanding, many breaches are either unknown by the victims or unreported given the associated reputational damages of disclosure. The incidents are self-reported by CI owners and operators and compiled by ICS-CERT, a unit within DHS. It remains unclear whether the linear increase in the number of vulnerabilities reported is proportional to the increased rate of convergence, attention paid to ICS security by security researchers deployments and their ensuing attack vectors and the increased attention.

[36] DHS stopped reporting incidents involving ICS vulnerabilities after ICS-CERT was integrated with NCCIC following restructuring with the CISA act.

[37] *Sources: Kaspersky Labs – DHS vulnerabilities advisories - ICS-CERT*

2013	158 – 85	257
2014	181 - 99	245
2015	189 - 142	295
2016	? - 140	290
2017	806 - 192	?
2018	223	?

Notable ICS-based exploits have been attributed to Russian nation-state-backed cyber actors. In 2013, US-CERT identified an advanced ICS malware suite with modular payloads and later attributed them to the Russian Civilian and Military Intelligence Services (RIS) group Grizzly Steppe / Dragonfly / Energetic Bear (Hemsley and E. Fisher, 2018; NCCIC, 2016). Like Stuxnet, the Havex/BlackEnergy malware suite uses information gathering about devices and resources within an ICS network before triggering further escalation at the command-and-control site.[38] In December 2015, the BlackEnergy 3 variant was used on 30 Ukrainian substations and left almost a quarter-million without power for around six hours, the first documented case of a cyber-physical attack of its magnitude.[39] Similar attacks followed next year. This suite of ICS-based

[38] Black Energy was ongoing since at least 2011 and Havex was discovered in 2013. Havex communicates with C2 server and can deploy a modular payload from espionage, persistent access, to sabotage as optional capability. Symantec observed its presence on the US, Turkish, and Swiss energy sectors (Hemsley and E. Fisher, 2018).

[39] The Ukrainian blackouts of December 2015 and 2016 are said to result from a coordinated attack, using Black Energy 3 (latter attributed to Russian RIS by the USG) and Industroyer/Crashoverride (Anton et al). The combined work of the Russian RIS (positively attributed by the USG) and a group called Electrum (third-party attribution). The RIS is thought to have used the BlackEnergy 3 malware (latter attributed to Russian RIS by the USG) while Electrum used Industroyer/Crashoverride as part of a long-term campaign (Anton et al; ("ELECTRUM | Dragos," 2020). A Dragos report stated asserted the link based on confidential sources. The Electrum group is also tied to the Sandworm team (Russian GRU), which was behind the 2015 Ukraine power system cyber-attack. Given the lack of apparent financial motivation,

malware was later attributed to a Russian Civilian and Military Intelligence Services group called Grizzly Steppe (DOJ, 2020; NCCIC, 2016). News of the malware rippled throughout the US security community as it targeted ICSs vendors in the US. The DHS, FBI, DOE, NERC, and many expert witnesses on Congressional hearings have since expressed concern about the significance of the Ukraine events as a new precedent in cyber-physical capabilities.[40] Before the events in Ukraine, the evolution of IT/OT convergence ideas and the coupling of solutions was subject to framing information under uncertainty seeing as threats had yet to materialize (Kahneman and Tversky, 1981; Kingdon, 2014).

As the events of Ukraine revealed concrete possibilities, they were called out in a Senate Committee hearing on Energy and Natural Resources *Cyber Technology Energy Infrastructure* on October 26, 2017 as a real and growing threat on the US grid.[41] The actions of the Russian Military Intelligence Services group on the Ukrainian power grid continued to grip the IC and cybersecurity regime and amounted to a watershed moment that motivated many upcoming adjustments to the offensive and defensive USG posture in cyberspace.[42]

Dragos' attribution of Russian RIS is based on Electrum's ties to the Sandworm team (GRU) and the ongoing regional geopolitical tensions involving the protracted conflict in Crimea (E-ISAC, 2017).

[40] For a more detailed account of high-profile incidents, see (Hemsley and E. Fisher, 2018).

[41] This hearing also continued a trend of great-power competition discussed in chapter 7 whereby any general-purpose high-technology such as ML is conceptually regarded as dual-use. In this case, ML was regarded as potentially enabling coordinated attacks against the grid

[42] According to the Republican Policy Committee the USG sent interagency investigative teams to Ukraine in March and May of 2016. A bipartisan bill for US-Ukraine Cybersecurity cooperation was later passed by the house on February 7, 2018. The bill reaffirms the joint strategic partnership particularly the cybersecurity of critical infrastructure.

Following the second wave of cyber-physical attacks on the Ukrainian grid, PPD-41 was passed on July 16, 2016, as one of the last Presidential Directives of the Obama administration. It notably focused on cyber incidents that include both cyber and physical effects. PPD-41 established another structure for public-private cybersecurity coordination, Cyber Unified Coordination Groups (UCG).[43]

After the Russian Information Operations on the 2016 US Presidential elections, the Obama administration aimed to retaliate with a cyber-based counter-attack deploying "implants" in Russian networks deemed "important to the adversary and that would cause them pain and discomfort if they were disrupted" (Miller et al., 2017). Developed by the NSA, the malware was designed to be triggered remotely as part of the administration's desire to expand the retaliatory menu of options in the face of ongoing and multifaceted Russian aggression (Ibid). The US cyber forays on the Russian power grid were consistent with a more aggressive cyber posture that transitioned to cyber-physical space.[44]

Around 2017, US ICS operators and the broader internet economy suffered several waves of spear-phishing, ransomware, and wiper attacks with the Petya, NotPetya, and WannaCry malware later attributed to Russian state-affiliated actors. NotPetya stood out

[43] These groups are to be headed by relevant SSAs and any supporting federal agency. The groups are triggered according to a new schema describing a cyber incident's severity from a holistic perspective, defining six levels, zero through five, in ascending order, whereby events over level 3 warrant group formation. Should a cyber incident mostly affect a private entity, they are to take the lead in remediation while coordinating with the federal government.

[44] The revelation of the logic bomb on the Russian grid came June 2019 however it remains unclear what specific behavior this incident was in response to. The behavior appears to fulfill a tit-for-tat strategy intended to either deter further information operations, or instead as a purely instrumental end to 'prepare the battlefield' consistent with the Trump administration's more aggressive cyber posture with Nakasone's Defending Forward strategy (Sanger and Perlroth, 2019).

as the "most destructive and costly cyber-attack in history" as it maliciously encrypted the networks of various sectors, including healthcare, without a ransom demand (DOJ, 2020). The following sub-sections address the influence of convergence on energy sector agencies.

7.3.3.2 The Department of Energy

The DoE conducts CI oversight through an undersecretary-level information management governance council (MGC) and influences the energy sector through incentives and regulations.[45] The MGC coordinates and implements cybersecurity for DoE based on the NIST risk-management approach (DoE, 2009). DOE underwent internal organizational changes partially motivated by IT/OT convergence, resilience, and cybersecurity.[46] In 2015, the Fixing America's Surface Transportation Act (FAST) amended the Federal Power Act, which designated DOE as the only statutorily defined sector-specific agency responsible for the cyber and physical security of infrastructure owners and operators in the energy sector.

This formal expansion of DoE authorities resolved an institutional vacuum and competitive concern between DoE and the DHS which was poised to take over CI in ICTs and energy.

[45] DOE also leads the Energy Government Coordinating Council (EGCC) along with the DHS.

[46] The last major restructuring of the Energy Sector involved Energy's Policy Act of 2005 which directed FERC to use transmission incentives to help ensure reliability and reduce the cost of delivered power by reducing transmission congestion. The $80 billion allocated to DoE added resilience to the transmission of energy. The 2015 restructuring was more oriented towards distribution resilience.

DoE was afforded new authorities to protect critical energy infrastructure from all hazards, including cyber and physical attacks.[47] In passing the FAST Act, Congress paid attention to industry needs by making DoE responsible for the entirety of the coordination effort for energy infrastructure protection. Industry's need for being accountable to a single agency stemmed from a desire to simplify the already complex regulatory ecosystem in various energy markets and their relationship with the FERC.[48] Motivation for energy sector legislation involved the simultaneously increased interdependence of all CI sectors on energy (energy is perceived in Congress as the most critical of all infrastructure sectors) combined with the expanding threat vectors due to digitization. The Committee on Energy and Commerce was responsible for debating upcoming amendments to Assistant Secretary functions at the DoE. In their report to accompany HR 5174, the committee argues the need for legislation stems from the highly interdependent nature of energy systems; advances in digital and information technologies are layered onto existing practices and energy infrastructures such that new risks vulnerabilities emerge. The report continues tying the third phase threat component: "recent high-profile attempts by foreign actors to infiltrate our nation's energy systems and infrastructure further highlight the need for legislation aimed at mitigating these significant and growing threats (…) the growing interconnectedness of energy systems and the national importance of ensuring the supply and delivery of energy against cyber

[47] Section 61003 of the FAST Act amends section 215 of the FPA, creating a new section 215A "Critical Electric Infrastructure Security" which allows the Secretary of Energy to take action without notice for immediate measures in the event of an emergency.

[48] Represented by the Energy Subsector Coordinating Council (ESCC), and the Oil and Natural Gas Subsector Coordinating Council.

threats, underscore the need to consolidate and elevate the Department's energy emergency functions."

According to the 2018 Multiyear Plan for Energy Sector Cybersecurity, the energy sector noted a "substantial progress on information sharing, particularly through ICS-CERT, the ISACs, EPRI, and CRISP" following the attacks on the Ukrainian grid. However, private operators were still rarely voluntarily reporting incident information. In an Energy and Commerce Committee hearing titled Energy Department Modernization on January 9th, 2018, the Deputy Secretary of DoE claimed that too often, expectations for countering cyber attacks on the grid exceed their authority despite access to classified information as part of the NSC. This problem further highlights the need for cross-sectoral collaboration with the DHS as part of an integrated regime.

Later next month, the Secretary of Energy established the Senate-confirmed Office of Cybersecurity, Energy Security, and Emergency Response, or CESER. The newly created Assistant Secretary position has jurisdiction over emergency and security functions related to the energy sector's infrastructure and cybersecurity. In effect, the new role was that of a new sector-specific cybersecurity integrator or energy cyber czar. In May, President Trump eliminated the National Cybersecurity Coordinator, and Congress finally enacted a major DHS restructuring in November 2018 with the CISA act.[49] These changes effectively created further disintegrated information sharing between the CESER and the CISA. Meanwhile, on the intelligence side, the role of the Cyber Threat Intelligence Integration Center in the civilian cybersecurity regime has yet to be

[49] H.R. 4120 (115th), Grid Cybersecurity Research and Development Act was the Democratic counterpart proposal to enhance interagency policy coherence for cybersecurity, only this time, under the DOE's leadership.

articulated as it awaits the assignment of a headquarters more than five years after its creation.

7.3.3.3 The Federal Regulatory Energy Commission (FERC)

The FERC is an independent and self-funded agency part of the DoE regulating interstate wholesale power generation and transmission in the energy sector, including rates, permits, terms and conditions, mergers, and acquisitions.[50] The Energy Policy Act of 2005 designated the FERC as primarily responsible for the reliability of the bulk power system (Campbell, 2011). The Energy Independence and Security Act of 2007 (EISA) added security and reliability requirements for the smart grid deemed necessary to prevent simultaneous and cascading failures from all-hazards and cyber threats given the increasing grid complexity. The FERC designated the North American Electric Reliability Corporation (NERC) as responsible for enforcing the CIP reliability standards, thereby shifting the industry from a voluntary basis to a mandatory regulatory apparatus for federal bulk power applications after 2009.[51]

FERC's authority excludes the energy sector's distribution portion, including power transfer agreements and defining the CIP standards themselves. FERC cannot issue security standards without consultation with operators, and any revision to existing standards is subject to stakeholder approval. Distribution utilities are instead under the purview of the NERC and regulated by state and local public utility commissions.

[50] NERC's scope also extends to natural gas, crude oil, and refined petroleum.

[51] NERC was the only entity that applied to FERC for the designation.

Utilities have a strong historical interest in self-regulation. As plainly stated by a utility executive: “Here's the deal. Private industry needs to be a pitcher, not a catcher (…) I don't want to get regulations from them [the government] I'm going to tell them what regulations I need in order to prevent and respond to threats most effectively. While CIP standards are mandatory in the energy sector, they only apply to industry-defined “critical cyber assets.” The issue of self-determining security standards was found to be strictly confined to the energy sector.

In 2013, FERC noted significant penetrations of small generation and increasing requests for small generator interconnection (smaller than 20 MW) (FERC, 2013).[52] As distributed and intermittent renewable energy sources are coupled to the grid (e.g., wind farms or photovoltaic panels), local intermittent generation can drastically change the amount of load (Anonymous interview, 2018) (smaller than 20 MW).[53] While intermittent generation cannot be formally regulated given its volatility, the NERC is currently debating a more formal observability strategy. Utility operators highlighted the introduction of new vulnerabilities to the grid via new distributed energy resources (DERs) that are not subject to FERC regulations in a Senate hearing before the Energy

[52]Federal Energy Regulatory Commission (FERC). 2013. 18 CFR Part 35. RM13-2-000; Order No. 792 Small Generator Interconnection Agreements and Procedures. https://www.ferc.gov/sites/default/files/2020-04/E-1_74.pdf

[53] The IEEE defines distributed resources as: “sources of electric power that are not directly connected to a bulk power transmission system. Distributed resources include both generators and energy storage technologies. (Institute of Electrical and Electronics Engineers (IEEE) Standard 1547 for Interconnecting Distributed Resources with Electric Power Systems, p. 3” (2013) (and ancillary services such as storage, etc.)

In 2016 the FERC noted how non-synchronous generators (whose speed can vary with wind speed) are increasingly replacing synchronous generators, which is resulting in a decrease in the amount of dynamic reactive power available to the transmission system (2016) and the need to ensure sufficient black-start capabilities can maintain a resilient grid (FERC, 2016).

and Natural Resources Committee titled “Electric Grid Threats” on March 28, 2017. The lack of stringent cybersecurity requirements for smaller, third-party connections to the grid is considered a vulnerability. That said, according to one utility executive, the compromise of a single SCADA system at the distribution level might impact at a block or neighborhood scale. However, the transmission-level Energy Management Systems (EMS) defining how power is moved across the US are the most critical systems in an electric utility overtaking nuclear security in terms of severity.

7.3.3.4 Policy solutions from National Labs: the DarkNet and the CRISP program

Using the authority of the DoE as a national safety guarantor, US National Labs aim to provide technological policy solutions to secure the grid from cybersecurity threats. The most relevant policy solutions stemming from national labs involve the ongoing information-sharing program called the Cybersecurity Risk Information Sharing Program (CRISP). The second is a proposal to create a separate communications network for critical grid infrastructure. Overall, experts from National Labs were found discernibly more concerned with cyber-physical threats than Congressional representatives, followed by agency bureaucrats, expert witnesses from security services firms, and CI owners and operators. That said, energy stakeholders from national labs and utilities have acknowledged that while nation-states remain the most capable threat actors, the severity of the threat is often overstated due to US attribution and retaliation capabilities (GAO-19-332, 2019).

The associate Laboratory Director for Idaho National Laboratory (INL) highlighted how energy asset owners are burdened with cyber exploits on IT and OT computer-based

control systems. The Director of Electrical and Electronics Systems Research at DoE's Oak Ridge National Laboratory (ORNL) and a manager at INL similarly emphasized the increasing threat and burden of IT/OT convergence on operators, especially after events of Ukraine in 2015 and 2016. In September 2017, DOE's Office of Electricity Delivery and Energy Reliability stated that ORNL is taking on cybersecurity technology solutions at the hardware and software levels via the Grid Modernization Laboratory Consortium (GMLC) to enhance grid distribution resilience by detecting APTs and zero-days. In a similar bid, in a hearing titled Cyber Technology Energy Infrastructure on October 26, 2017, the manager of Electricity Market Sector for Pacific Northwest National Laboratory (PNNL) discussed extending cyber situational awareness to focus on grid control systems internal to utilities, i.e., OT technologies. The PNNL Manager further stated that "the nation must develop an integrated, real-time view of cyber risk across the IT and OT elements of the power system to significantly improve our cyber resilience (Imhoff, 2017)."

CRISP is a voluntary program to facilitate the exchange of detailed cybersecurity information between utilities, the Electricity Sector Information Sharing and Analysis Center (ES-ISAC), the DoE, and the Pacific Northwest National Laboratory (PNNL). CRISP works by monitoring 80% of US power transactions with host utilities and separates known 'blacklist' signatures from its 'whitelist,' scanning the grey area for anomalous threat signatures using advanced machine learning algorithms (Anonymous interviewee, 2018).

In a hearing before the Committee on Energy and Natural Resources on October 26, 2017, ORNL's DarkNet project was presented as an isolated communications network for

energy CIP that moves grid controls and communications away from the public internet using "dark fiber" i.e., existing but unused optical fiber, to shield the grid from hostile cyber penetrations. The Director for Electrical and Electronics Systems Research at DoE highlighted the DarkNet project as a valid potential solution to the threat of convergence. The DarkNet has yet to be funded by Congress while ORNL scientists determine the over-capacity of fiber is to determine the project's viability.[54]

IT/OT convergence has enabled uncoordinated competition among national labs to provide pre-emptive solutions to cyber-physical threats. The notable omission of economic considerations included with the DarkNet proposal highlights the extent to which convergence is leveraged as a pressing security concern by National Labs aiming to solicit funding from Congress.[55] However, the uncoordinated nature of information sharing programs appears to stem from sub and cross-sector agency competition on policy solutions. As evidence of un-coordinated behavior at a sub-sector level, National Labs are currently competing for resources with each other to get their proofs-of-concepts funded as opposed to implementing a cross-sector or even sector-based directive led by the DoE (Anonymous interviewee 2018; Mermoud, 2018). As an information-sharing program specific to the energy sector, CRISP competes at a cross-sector level with DHS-based information-sharing programs yet is subject to the same overarching institutional pitfalls as discussed in the section on the DHS.

[54] Utilities in vertically integrated markets such as the Southern Company have more successfully experimented with unifying energy and communications within their networks due to their facility with top-down implementation.

[55] In notable contrast to Huawei's threat which was sufficient for Congress to fund a rip-and-replace program as discussed in chapter 7.

Further, the use of dark fiber as a policy solution for IT/OT convergence alludes to an ongoing public policy debate on industrial networking architecture that deserves closer attention given its intersection with the China threat.

7.3.3.5 The intersection of convergence and the threat of Chinese ICT

The 2006 Roadmap defined architecture in the energy sector as "the design of [control system] networks: how the components are arranged, how they communicate with each other, and how they are controlled (Eisenhauer et al., 2006)". The convergence and integration of IT and OT require recognizing the building blocks of that networking architecture encompasses, i.e., IT networking protocols and OT standards defining various topologies that help utilities decide how to layer and separate their devices both logically and physically.[56] Figure 11 below provides a typical energy communications architecture.

[56] Topologies are relevant at the sub-organizational-level and therefore outside the scope of this work. The only relevant distinction made in this work is between routable networking protocols such as LAN/Ethernet as distinct from serial communications such as RS-232 and RS-485 as relevant for CIP standards.

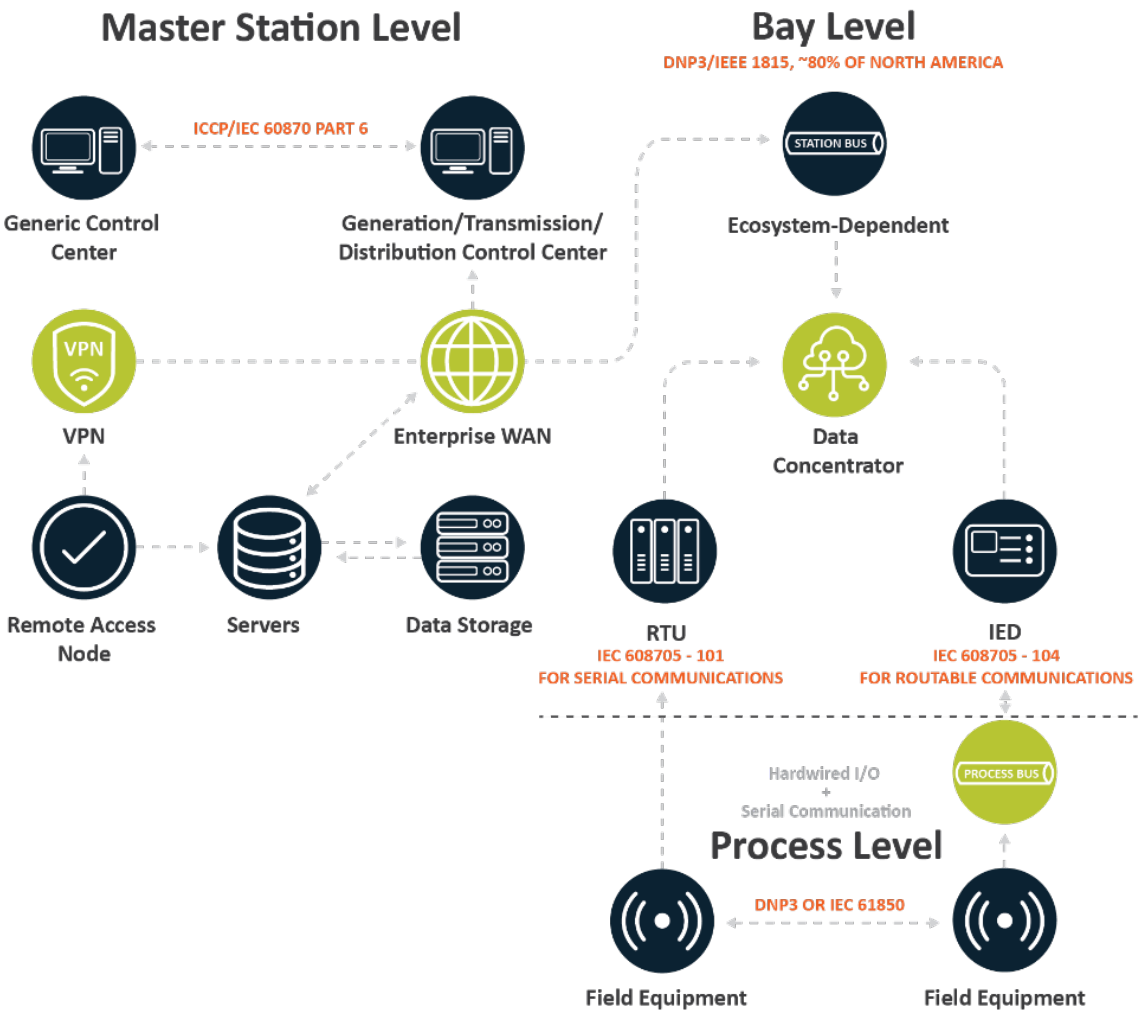


Figure 12: Typical energy communications architecture

Power utilities have increasingly used various forms of SCADA automation enabled by different IT communications architectures, standards, protocols, and communications topologies to generate, transmit and distribute electrical energy reliably and competitively (Aghdam and Hagh, 2019; Farhat and Mueller, 2020; Shahzad et al., 2016). Historically, industrial sectors have purposefully avoided using the public-facing internet and relied on proprietary standards running serial communications topologies. For security reasons, industrial sectors tend to be averse to change and adopt an "if it isn't broken, don't fix it" approach (Farhat and Mueller, 2020). The rate of standards diffusion is purposefully

slow, and 20-year validation periods for new technology are expected. For example, the IEC 61850 standard was poised to facilitate the proliferation of renewables, yet the prohibitive cost of retrofitting old equipment and a continuously expanding scope of industry demands have been delaying its adoption since the 1980s.

However, as industrial sectors increasingly demand low-latency and ultra-high dependable networking for their applications, some network engineers have argued that the IP cannot meet the current API requirements for OT (Mueller et al., 2020). Various proposals exist to either actively steer the dominant architecture or create conversion architectures that, while preserving air-gapped interoperability, would have more substantial governance implications as a fork from the dominant architecture (Clark, 2018). The IETF and Internet Society have argued for continued use of a spanning network with overlays for special services such as CDNs, lightweight cryptography for IoT, or other special on-demand services running at the application layer. Some network engineers have argued the need for a conversion architecture (Clark, 2018).[57] While many such proposals were put forward historically, they have all failed to reach critical mass for adoption due to the tremendous economic inertia of the dominant architecture.[58]

While many arguments for future internet architecture involve trade-offs based on different engineering philosophies, such as the end-to-end principle, the more normative

[58] Even authoritarian regimes struggle with the network effects of IP in its current version. In November 2017, The General Office of the CPC Central Committee and the General Office of the State Council issued a circular to scale the deployment of IPv6 for all Chinese internet users by 2025 and a quarter of them by the end of 2018. According to Google's statistics, China had an IPv6 adoption rate of 2.29% by April 2021 according to Google statistics. While that figure may underestimate the actual figure, it reinforces the theory that market forces determines standards adoption and not a government's efforts to make it so (Flinta, 2019; Google, 2021.; Xinhua, 2017).

dimension of the debate was hijacked by the anti-China rhetoric (Blumenthal and Clark, 2001; Mueller, 2020). In the first case, an argument was put forward that 5G standards espouse the values of their developer's nationalities instead of the market or a company. In the second case, an early proof-of-concept was presented as paving the way to fragment the internet and adopt an alternative form of Chinese-led multilateral internet governance (Hoffmann et al., 2020).

Richard Li of Huawei has aimed to actively converge IT and OT to favor the sale of Huawei equipment. Li proposed a draft industrial networking standard called "New IP" (Chen et al., 2020; IARIA, 2021). Huawei started work on New IP in 2015 and tried to standardize their protocol unsuccessfully in 2017 at the IETF, then proceeded with their effort through the Networks 2030 Focus Group at the ITU. "New IP" represents "a list of perceived issues about the current Internet architecture and a list of desired features" (Durand, 2020; Mueller, 2020). As an early draft, "New IP" is unlikely to impact the US energy sector in the foreseeable future. However, its politicization and the China animus it solicited are relevant to the analysis since it lends itself to the USG narrative that any technical standards or equipment involving a Chinese firm is a trojan horse that embeds ulterior motives by the CCP (Hoffmann et al., 2020).

At a 5G conference hosted by the American Enterprise Institute on May 29, 2019, an expert on wireless technology provided a Freudian slip revelatory of the dominant narrative in Washington: "usually you start with a set of objectives about what the capabilities will be for a technology and then the standards receive contributions from company which are proposals on how something might work. The proposals that get the greatest attention are the ones where a company says our proposal is based on something

that is demonstrated already works (…) *If a company- if a country* is starting to lead in a certain area, they can end up influencing the standards so that the standards favor their technologies (…) My understanding is that there is a lot of Chinese representation that is really disproportionate for a fair representation of a global participation effort (Rysavy, 2019)." tying private companies involved in 5G standards to the values and influence of nation-states

Similarly, in that same conference, the deputy assistant secretary for cyber and international communications and information policy at the State Department, Robert Strayer, perpetuated the pattern explored in chapter 7 whereby any high technology area is considered part of the strategic battleground with China and therefore subject to country-of-origin restrictions using a national security rationale. For Strayer, the appropriate risk-based approach for addressing the Internet of things, AI, the smart grid, or in this case, 5G deployment is to adopt country-of-origin restrictions on hardware and software vendors "subject to foreign government control (Strayer, 2019)."[59] Strayer continued arguing that the vanishing core-edge distinction as 5G networks become software-defined implies risking a Chinese kill switch via malicious updates should a monoculture of equipment from Huawei be allowed to continue.

[59] China's National Intelligence Law, enacted on June 27 places vague security obligations that attempt to shift legal obligations towards affirmative action for cooperation and support of Beijing's intelligence efforts (Tanner, 2017). The Chinese Cybersecurity Law of 2016 (effective June 2017) and the Counterespionage Law (Articles 9-16) provide similar vague language with flexibility of interpretation. The ambiguous definitions of what constitutes state security expressed in these laws may have been functionally set to either retroactively mold emergent cases into legal compliance or allow for general flexibility in interpretation. These laws are interpreted by USG officials to mean the CCP can compel Chinese ICT firms to exfiltrate US data or facilitate intrusions through supply chain vulnerabilities.

While arguments that Chinese-led standardization processes are an organized attempt by the CCP to take over the internet remain fringe in the expert community, they are leveraged by the USG to mobilize concerted action across different government agencies, often in the form of supply chain security programs. The propensity of these programs across the USG, including the FCC, DHS, and other public-private partnerships like the CSRIC, further validates how the China threat idea is a more potent driver of regime convergence than the standalone threat of IT/OT.

7.3.3.6 The Department of Homeland Security

The DHS is the only agency directly relevant to both policy problems addressed in this work. It was partially discussed in chapter 7 as one of the unique institutions with section 806 authorities to block individual vendors from federal networks.[60]

H.R. 3359 (115th): the Cybersecurity and Infrastructure Security Agency Act of 2018 was first introduced in 2016 by a Republican majority led by Rep. Michael McCaul (R-TX) and was later enacted in November 2018 after many hearing debates and negotiations. Following a decade of operations, DHS officials, staff, and Congressional representatives identified a need to streamline and consolidate the National Protection and Programs Directorate (NPPD) (GAO-21-236). Overall, the CISA act was a significant statutory adjustment, and organizational restructuring at the DHS intended to improve coordinative efficiency by adopting a service delivery approach for security. The

[60] The NDAA 2018 section 881 lifted the 5-year expiration of 806 authorities, making the 806/881 authorities permanent (unless revoked). DoD uses this authority to use supply chain risk as an evaluation factor in ICT procurements. The NDAA 2019 section 889 allowed the DHS to expand this evaluation factor to the civilian cybersecurity regime prohibit the purchase and use of equipment connected to, owned by, or controlled by the Chinese government.

bill was also the most extensive USG effort to legitimize the cybersecurity regime. In terms of organizational adjustments, the newly minted CISA elevates the mission of the former NPPD mission within the DHS to give it a CI focus and rebrands it as the Cybersecurity and Infrastructure Security Agency (CISA). CISA continues the mission of securing federal networks, coordinating the national effort to ensure CI in coordination with private partners, responding to requests from CI operators and offering support as needed, and carrying out emergency communications responsibilities (GAO-21-236).

Part of the reorganization was mandated by statute, while others were left up to the executive at the DHS. Like the NPPD before it, CISA continued to oversee rebranded legacy subdivisions while consolidating others, according to figure 13.[61] CISA also consolidated the old NCCIC (now the cyber security division) to be on the same 'watch floor' as the NCC and NICC.

[61] Figure 13 is not exhaustive.

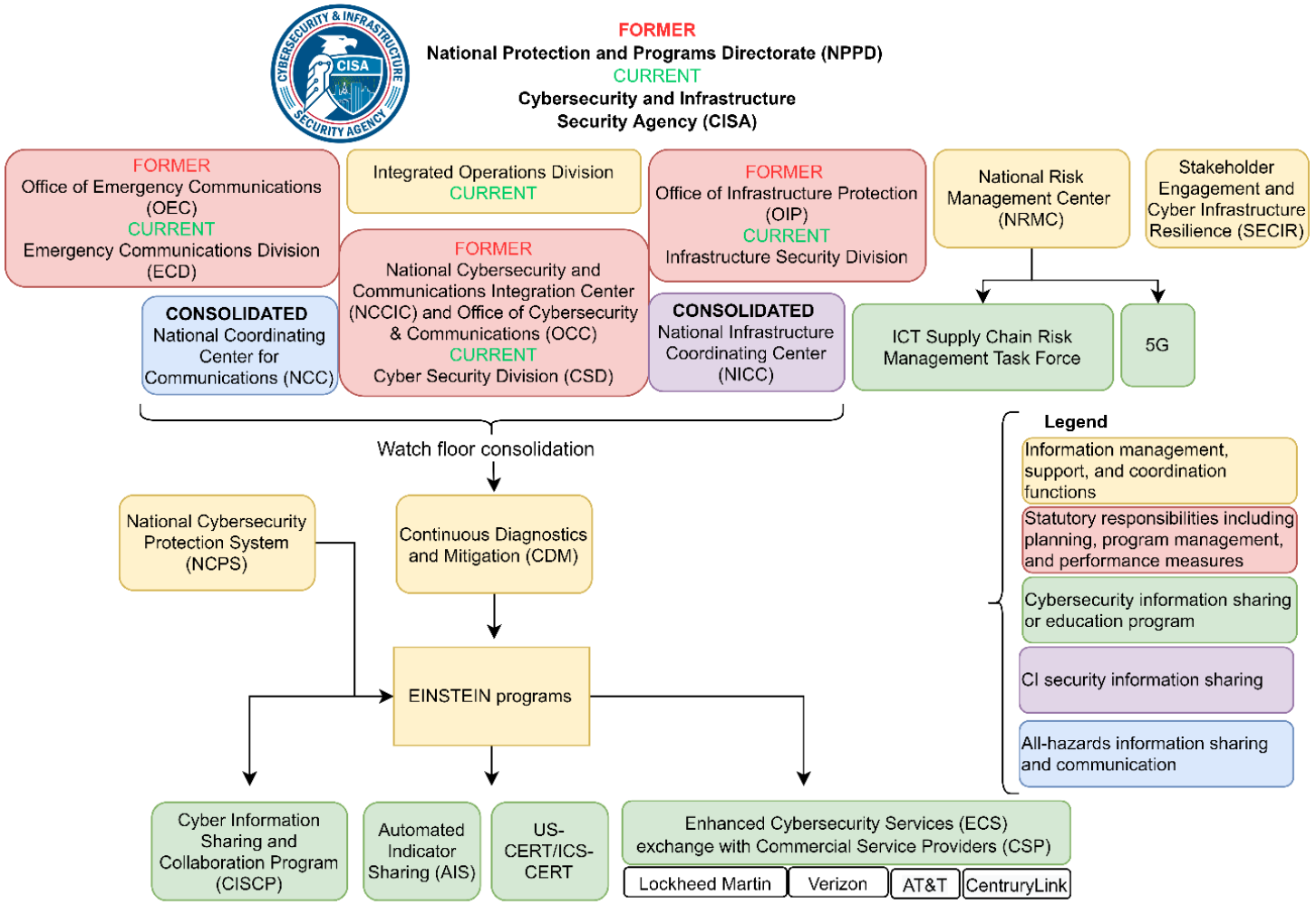


Figure 13: Restructured divisions at CISA

7.3.3.6.1 Motivation for the CISA restructuring

The motivation for the reform stems from four overarching problems, the first two of which are directly relevant to this analysis. First, ongoing cyber intrusions on federal networks reflected an upstream information management problem and mismanagement at the DHS and the federal government more broadly.[1] Second, with the resurgence of great power competition, Congress and the executive perceived the evolving nature of cyber threats such as supply chain risks as requiring a whole-of-government response, with the DHS leading the defensive operational component. Third, the CI community often referred to a "branding" problem DHS faced with the NPPD (McCaul, 2017). According to former CISA director Krebs, the former NPPD's name was "incomprehensible and unpronounceable," making the group's activities less recognizable among stakeholders (Krebs, 2017). Finally, the DHS suffered from a workforce supply shortage due to a pay gap with the private sector and the complicated procedural nature of federal hiring, especially when security clearances are required.[2] The Under Secretary for the NPPD, Suzanne Spalding, highlighted in a 2015 hearing entitled "DHS Efforts to Secure .gov" how the agglomeration of different agencies into sub-departments within the NPDD meshed various cultures and contributed to low morale within DHS over the years.[3] The CISA reformulation, it was hoped, would serve to attract the necessary talent to its cyber workforce and allow it to better compete with the

[1] As described in chapter 5.

[2] CISA is currently poised to implement Executive Order 13870 which directed the federal government to bolster its cybersecurity workforce.

[3] The NPPD was a conglomeration of different programs within DHS leftover from TSA, or FEMA, or other established legacy agencies after the original Homeland Security act agglomerated various agencies (Franco, 2018).

private sector and federal agencies like the NSA and the CIA (McCaul, 2017). The following section provides an overview of the PPP institutional structure to clarify the DHS's role as its information integrator.

7.3.3.6.2 DHS's role reflects disintegrated and incoherent policymaking in the federal government

Each of the 16 CI sectors is assigned a sector-specific federal agency (SSA) responsible for carrying out various coordinative functions and sub-sector oversight over their jurisdictions. For example, the DHS is the sector-specific agency for IT and Communications, while the DoE became the SSA for the Energy sector after the FAST act in 2015. The rest of the PPP is structured around a complex structure of coordinating councils whose membership ranges from federal agencies, private operators of infrastructure, and a broader class of nonprofit organizations, trade associations, and lobbies.

The Sector Coordinating Councils (SCCs) are the private sector councils led by owners, operators, and other entities within a sector as they coordinate over a wide range of security activities and provide a formal point of contact with the government (NIPP, 2006). SCCs have a governmental counterpart, i.e., the Government Coordinating Councils (GCCs), set up to enable "interagency and cross-jurisdictional coordination" (CISA, 2020). The GCCs are chaired by representatives from each Sector-Specific Agency (SSA) responsible for overseeing cross-sectoral coordination with all levels of government, but also for planning and implementing the CIP mission alongside the cross-sector councils. Similarly, the cross-sector councils are a collection of chairs and vice-chairs of the SCCs, which, as established with PDD-63, are maintained and self-regulated

by the private sector to achieve inter-sectoral coordination over interdependencies (CISA, 2021).[4]

The CIP structure has strong institutional path dependence based on the original statutes that continue an awkward demarcation of the IT and communications sectors. Given the increasing convergence of IP for all communications, including traditional media, functional distinctions have limited implications on information security.[5] However, many SCC member organizations continue to overlap as sector-specific members of the IT-SCC and the Comms-SCC. At the time of writing, the IT-GCC and Comms-GCC (the public sector councils) overlapped in 18 out of 27 agencies between the IT and Communications sectors, a strong indicator of policy incoherence by s of effort as defined in this work.[6] However, the IT-SCC and Comms-SCC overlapped in seven out of a combined 149 members.

Further, as self-organized collections, SCCs are also beset by collective action problems, including variation in membership that contributes to a loss of organizational knowledge (CSIS, 2013). These problems are particularly salient to the IT-SCC & GCC-IT.[7]
Each SCC contains an ISAC composed of segregated industry practitioners that collect information relevant to each sector. CISA describes ISAC functions as serving

[4] For example, the Tri-Sector Executive Working group, (part of CIPAC) is a PPP focusing on the interdependencies between energy, telecommunications, and the financial services sector.

[5] The more relevant sector-based distinctions today instead involve common carrier regulation and market structure concerns such as vertical integration. (Whitt, 2003; Mueller et al. 2007).

[6] For a complete list and detailed table refer to the appendix.

[7] It should be noted that information sharing is best in the homogenous financial services sector, followed by energy, and finally, the ICT sector. The diverse ecosystem of suppliers and convoluted supply-chains in the ICT sector undermines trust and creates massive collective problems.

"operational and dissemination functions for many sectors, subsectors, and other groups, and [facilitating] sharing of information between government and the private sector" (CISA, 2021). The creation of ISACs accounts for the hybrid structure of the information management ecosystem as opposed to a pure hub-and-spoke, DHS-led initiative (Bakis and Wang, 2017). In essence, ISACs analyze, synthesize, and inform their sectors back. At the local level, fusion centers were also set up with the Homeland Security act to gather information and "fuse" local law enforcement and common intelligence interests at the local level (DHS, 2021). Around 80 fusion centers were distributed in essential locations, with at least one per US state. However, this structure has been subject to "large, systemic breakdowns," owing to the absence of a standardized organizational model, lack of a binding policy idea, and missing external agency partnerships (Salvatore, 2018).

At the center of it all, the CISA, a large bureaucracy assigned to integrate the entire ISE. It acts as the official purveyor of defensive cyber operations (DCO) for USG networks, a clearinghouse of classified-unclassified information, and the central hub of the ISE by analyzing, synthesizing, and distributing data. CISA is the only organization that can transition DoD information that is "on a need to know basis" to a "need to share basis" to the private sector (Hurd, 2017).

Per chapter 5, section 3, information sharing is the success criteria by which risk-informed decision-making is framed. Agency officials have often repeated the mantra that "timely, trusted information sharing among stakeholders is essential to the security of the nation's critical infrastructure (Under Secretary Krebs, 2019)". However, the GAO has consistently reported endemic problems from 2003 onward how information sharing,

particularly from the private sector to the government, remained sparse. The lack of interagency coordination during periods where the all-hazards and terrorism threat-frames were operative is particularly relevant, especially when contrasting with cybersecurity policy motivated by China's threat as addressed in chapter 7.

With the signing of an Executive Order to *Promoting Private Sector Cybersecurity Information Sharing* on February 13, 2015, the White House sought to encourage informal coordination norms and create cross-sectoral cooperation capacity by creating Information Sharing and Analysis Organizations (ISAOs). ISAOs were designed to be flexible, ranging from informal groups of professional associations to entities that look like a more formally chartered ISAC. When combined with the liability protections afforded by the CISA act of 2015, the federal government tilted the ISE away from a top-down, centralized hub-and-spoke model towards a hybrid, decentralized ecosystem.[8] In other words, information sharing capacity was now theoretically expanded across sectors, organizational types, and levels (public, private, state, or local).

The federal government is contending with cross and sub-sector politics impacting its information management. At a cross-sector level, the issue of how ISACs should be merged or layered is an ongoing debate. ISACs and SCC are two independent structures that are not part of the same institutional hierarchy. For example, instead of having a single executive board and common governance structure, the strategic planning at the

[8] The Solarium Commission report in 2020 argued for a return to centralization of authority and information management. The report also argued for increasing CISA's budget despite also arguing for "speed and agility" in the ISE. The report recommends the integration of federal cyber centers within CISA as well as to empower them to serve administrative subpoenas by passing the Cybersecurity Vulnerability Identification Act.

SCC level is separate from the operational implementation at the ISAC level. In other words, power over the process does not rest with people who have an intimate sense of the context in which the strategies have to work (Mintzberg, 1994).[9] ISACs' fluid institutional design has implied limited incentives to share information and vague participation. This problem was addressed in a March 9, 2017 Subcommittee hearing entitled The Current State of DHS Private Sector Engagement for Cyber security discussed how to incentivize the private sector to share given the free-rider problem, i.e., the private sector receives information but does not share back.

In the wake of the OMB hack, it became increasingly clear that the DHS was not in a solid position to adequately plan and execute a national response to the growing threat of foreign attackers infiltrating critical resources (Brumfield, 2019). [10] On February 25, 2016, the Subcommittee on Cyber security, Infrastructure Protection, and Security Technologies held a hearing entitled Emerging Cyber Threats to the United States. Representative Ratcliffe (R-TX) highlighted how cyber threats from nation-states such as China, Russia, North Korea, and Iran were found to be exponentially increasing and to have "evolved in new ways that pose even greater risks to the U.S. Homeland and our critical infrastructure (Ratcliffe, 2016)."

As mentioned in section 3.3.2, Rep. Lieberman et al.'s were unable to reconcile political differences to pass CSA 2012 despite being a small interest group with fewer costs of collective action. The CISA expansion was now more palatable in Congress as great

[9] Mintzberg argues that effective strategy-making under difficult circumstances requires planners take personal charge of the implementation, in this case integration of the different subunit plans. Otherwise planners risk stifling the initiative of supervisors and operators due to lack of ownership of the process.
[10] The OMB hack involved the theft of the sensitive personal data on 22 million current and former federal employees by suspected Chinese hackers.

power competition and threat politics unified Congressional preferences. The CISA restructuring was a major effort to integrate the cybersecurity regime that set the DHS on a path of continuous budget and scope expansions (DeLauro, 2019; Katz, 2020). Unsurprisingly, however, chronic mismanagement issues have continued to stymie integration efforts.

Continuity of technology management as federal and state CIOs are appointees and not permanent across agencies has also been a long-standing issue (Hurd, 2017).[11]

For example, Representative Cedric Richmond (D-LA) noted that the cooperation between DHS's CISA and DoD had yet to articulate roles and responsibilities in the coordinative effort at the policy and operational levels, especially as they interface with the CI operators. Too often, the GAO reports that despite agreement on a policy design level, operational shortcomings are rampant, citing the lack of a WH cybersecurity czar (integrator) as sowing confusion about responsibilities. To sum, the path-dependent institutional structure of CI combined with cross and sub-sector politics has impeded CIP policy design's overall coherence and integration. Disintegrated policymaking is reflected by the ongoing problems with implementing sound information management and sharing practices in the USG. Per the PRF, and as evidenced by Congressional hearings and GAO reports, these challenges reflect endogenous political forces hampering any effort at overall regime integration. As addressed in the next section, organizational

[11] The White House Office of Management and Budget (OMB) houses the Federal CISO. Rep. Will Hurd (R-TX) and Kelly have sought to elevate the role of the Federal CIO to become a presidentially appointed position reporting to the OMB. Rep. Hurd was able to pass IT procurement bill through the 2018 NDAA to address legacy systems in the federal government and better prepare federal CIOs by allowing them to seek out support, training, and funding from the DHS on a voluntary basis.

mismanagement at the DHS is further compounding the problem of integrated policymaking in the cybersecurity regime.

7.3.3.6.3 Information management problems endemic to DHS

CISA says that since March 2016, it has shared more than six million unique cyber threat indicators with partners (as NPPD at the time). Currently, the agency has more than 250 organizations connected to its AIS server and more than 4,000 third-party AIS connections (Brumfield, 2019). However, missing contextual information included with AIS information sharing was flagged in many Congressional hearings as an ongoing technical problem that renders these numbers devoid of substance.

In a House Committee hearing on Government Waste and Inefficiency on April 13, 2016, Rep. Will Hurd asked the Comptroller General about the state of DHS's human resources and IT investments. The Comptroller General responded with: "this to me was a classic case of mismanagement of this effort over a number of years. There are 422 different systems over there[the DHS], there was lack of attention by management, they've supposedly now focused more on it and coming up with validating the business case and the model but I think Congressional oversight would be very appropriate and prudent at this point (Dodaro, 2016)."

DHS does not share with CI operators directly but through indirect mechanisms such as the voluntary Enhanced Cybersecurity Services (ECS) program. With the ECS, indicators of compromise (IoC) are shared with qualified commercial service providers (CSPs) (currently Lockheed Martin, Verizon, AT&T, and CenturyLink). Automated cyber threat information sharing is deemed necessary given the growing complexity of the threat landscape. For the automated exchange to occur successfully, incident data are first

automatically collected, parsed, filtered, and subsequently thoroughly analyzed by human experts to generate actionable intelligence. Most sharing standards are based on the exchange of Indicators of Compromise (IoCs). There are many initiatives to standardize formats for IoC descriptions for more efficient automated processing of these indicators. For example, DHS's Automated Indicator Sharing (AIS) program leverages existing technical standards (STIX language and TAXII protocol) to provide the automated sharing of unclassified machine-to-machine information between PPP partners.[12] At the same time, while the NTIA is making progress with their Software Bill of Materials which could in the future act as an information-sharing standard, duplication of standardization efforts is rampant throughout the USG, providing yet another sign of disintegrated policymaking.[13]

For instance, the newly appointed head of the CESER described in a hearing titled DoE Modernization: The Office of Cybersecurity, Energy Security, and Emergency Response on September 27, 2018, how utility executives contend with information-sharing bottlenecks, including automated information sharing devoid of context and contextual information sharing suffers from over-classification for information sharing and related delays in acquiring clearances.[14]

[12] The Cybersecurity Information Sharing Act of 2015 (CISA 2015) granted liability and privacy protections to organizations that share cyber threat indicators and defensive measures through AIS. It required the DHS to confirm ongoing operation of AIS in March 2016 and released guidance, in conjunction with the DoJ to help private sector entities share cyber threat indicators with the Federal Government.

[13] See (Jasper, 2017; Skopik et al., 2016) for more details on IoC standards efforts.

[14] That same hearing confirmed that the risk of nation-state actors infiltrating parts of the grid far outweighs that of other threats internal to the US as will be relevant in the next sub-section.

Despite not being impacted by the Covid-19 pandemic, the DHS had implemented three of the nine recommendations and 37 of 94 planned tasks for the third phase of their organizational implementation goals set after the CISA act ((GAO-21-236). CISA has yet to develop clarity regarding their organizational changes, lending to stakeholder confusion, which "may impair the agency's ability to identify and respond to incidents, such as the cyberattack discovered in December 2020 [SolarWinds] that caused widespread damage (Ibid)." The Comptroller General noted that 750 of the 3,300 recommendations GAO has made on federal cybersecurity since 2010 remain open (GAO-21-288 and GAO-21-236). He continued by stating that the SolarWinds hack would likely have been discovered earlier had these recommendations been addressed.

As of mid-February 2021, CISA has not yet defined processes for monitoring the effects of the CISA restructuring, including fragmentation, overlap, and duplication of efforts, such as watch floor consolidations and increased centralization. CISA officials told the GAO they intended to do so in the future but had not identified specific plans or time frames for these actions. To sum, it appears that the DHS and CISA are subject to problems endemic to any large bureaucracy with unclear performance metrics and absent a mobilizing idea. The following section addresses how China's threat contributed to CISA's shift towards ICT Supply Chain Risk Management initiatives.

7.3.3.6.4 Evolving cyber threats and Chinese ICT start motivating a whole-of-government integration effort on the ICT supply chain

After the CISA was enacted, then-director Krebs allowed the agency "two years to mature the organization and have it be the CISA we know it can be," DHS's cybersecurity strategy, the DHS Cybersecurity Strategy, unveiled in May 2018, presented a strategic framework to execute the government's cybersecurity responsibilities during

the following five years. CISA then launched several initiatives, including tackling supply chain threats to upcoming 5G networks, improving election security, bolstering government network security, protecting industrial control systems, including physical security (Ibid).

Software supply chain security programs existed early on in DHS. For example, the Software Assurance (SwA) Forum and Working Groups were initiated in 2003 as a Cross-Sector Cyber Security Working Group led by DHS that includes NIST and DoD for software assurance in the IT supply chain. Over time, the community evolved and broadened the scope to include additional focus on the supply chain. The renewed focus on supply chain security coincided with the Trump administration's campaign against Chinese ICT.

Within DHS, the Cyber Supply Chain Risk Management Program is a newly formed entity within the new National Risk Management Center. DHS's national risk management center is concerned with assisting the federal government, and private sector CI operators manage supply chain risk. There is overlap with the internally facing department mission with other agencies such as the FCC addressed in chapter 7. The China threat, in practice, allowed the DHS to combine all the previous recommendations from NISTIRs, NISTSPs, NIST/SGIP, and knowledge for supply chain recommendations, and adds new requirements citing section 889 from NDAA 2019. [15] However, the lack of prioritization based on a clearly defined cybersecurity threat meant

[15] Section 889 of the 2019 NDAA seeks to mitigate the risk of companies that are connected to, owned by, or controlled by the Chinese government by prohibiting the purchase and use of such equipment. CISA now provides a vendor template for ICT procurement borrowing from NIST and adding questions specifically targeted towards Chinese ICT "4.9. Do you ensure that you are not sourcing assets on a banned list to customers (e.g., ITAR, NDAA Section 889)?"

an overwhelming agenda that included election security, supply chain security (which has always been solved in the private sector), including reinventing CI language such as the new "National Critical Functions."

In a Homeland Security subcommittee on cybersecurity and infrastructure protection in November 2018, interagency cyber cooperation was being discussed in the context of a whole-of-government approach to securing American cyberspace from "contaminated supply."A discussion ensued on how to make the IT ecosystem more secure by decreasing dependency on China.[16] This hearing cited election security as a motivating factor for a whole-of-government response on cybersecurity, including the WannaCry malware and increased interdependence of critical infrastructure systems. In that same hearing, representative Ratcliffe (R-TX) alluded to Chinese IP theft, stating, "cybersecurity is national security."

7.3.3.7 The North American Electric Reliability Corporation (NERC)

The NERC is the Enforcement reliability organization (ERO) for the FERC. In other words, NERC performs security audits and can serve fines for utilities for each instance of non-compliance with CIP Reliability Standards up $1 million a day. NERC works with eight regional entities to improve the reliability of the bulk power system. As an energy regulator, NERC's jurisdiction extended to regional entities from various power industry market segments, i.e., investor-owned utilities (IOUs), rural electric cooperatives

[16] Until 2019, DoD and the IC have been amplifying the threat of China and Russia equally in both directions.

(Coops), federal power agencies, state, municipal, and provincial utilities; independent power producers; power marketers.[17]

On September 17, 2020, the FERC issued a Notice of Inquiry (NOI) prompted by EO 13873 on "Securing the Information and Communications Technology and Services Supply Chain" seeking sector comments on the use of equipment from Huawei and ZTE as a risk to the bulk electric system. The Commission wanted to understand whether its current CIP Reliability Standards were adequate for mitigating that risk.[18] The FERC also cited as motivation for the NOI the "significant developments in the form of Executive Orders, legislation, as well as federal agency actions that raise concerns over the potential risks posed by the use of equipment and services provided by certain entities identified as risks to national security." Later in November, the NERC and the six Regional Entities acknowledged that supply chain compromises to telecommunications equipment could be leveraged to disrupt operations of the BPS. The ERO refrained from commenting on CIP regulations for the supply chain had only gone into effect in October. The ERO declared "minimal exposure of the BPS through branded products from the name Chinese telecommunications and video surveillance manufacturers and a somewhat more common use of Chinese manufactured or supplied unmanned aerial systems (UASs)". They also appeared concerned with unbranded telecommunications devices used on the grid. Notably, the ERO Enterprises noted that "the presence of certain equipment does

[17] These entities account for virtually all the electricity supplied in the United States, Canada, and a portion of Baja California Norte, Mexico.

[18] The Commission had approved Reliability Standards CIP-013-1 (Cyber Security – Supply chain Risk Management), CIP-005-6 in October 2018. The FERC also cited as motivation for the NOI the "significant developments in the form of Executive Orders, legislation, as well as federal agency actions that raise concerns over the potential risks posed by the use of equipment and services provided by certain entities identified as risks to national security."

not necessarily indicate malicious activity" pushing back on the country-of-origin idea as a proxy for security. China's ability was estimated as being able to cause "disruptive efforts on critical infrastructure such as the destruction of natural gas pipeline for days to weeks." Russia on the other hand was reported to be able to execute more temporary and localized disruptive effects on critical infrastructure, a matter of hours. Russia is the main perpetrator when it comes to cyber-physical threats based on track record, and China still features based on great power competition (IP theft and the other usual themes). Despite a strong track record of self-reliance and self-regulation in the energy sector, the pre-existing inertia of the Homeland Security regime combined with agency competition and the internal dynamics of the ICT sector made for an incoherent CI policy response in the USG.

7.3.4 Chapter conclusion

"Risk management" in the ICT Supply Chain is a policy solution that diffused in the USG as part of a whole-of-government response discussed in chapter 7. It gained legitimacy by intersecting the ideational and political levels as theorized by the PRF. At the idea level, it is specifically geared to address the intersection of the problem presented by China's rise as a monolithic threat and the compounding risk of IT/OT convergence. These included China's ability to mount coordinated cyberattacks on geographically distributed low-impact distribution systems, creating cascading disruptions or compromising 5G core or base equipment via advanced hardware and firmware-level tampering for similar purposes.[19]

[19] While these threats can be differentiated in their expression this version captures most.

However, it is essential to note that IT/OT convergence is never used to bolster the case for decoupling from China. As the idea that nation-states can mount cyber-physical attacks gained legitimacy, government agencies such as the DoE, the national labs, the DHS, and the FERC were vying for leadership on CIP oversight, to fill the institutional vacuum created by IT/OT convergence. Ukraine and Information Operations focused attention on Russia, leading to mutual brinksmanship in the ICS space; however, given the minimal economic interdependence between the US and Russia, the nation-state focus went back to China and Chinese ICT champions around 2018. The threat of China was used to bolster the threat-priority agenda and influence regime policymaking.[20] The "contaminated supply" narrative is based on a country-of-origin national security rationale. It is geared towards Chinese ICT specifically because China provides the only viable cross-sector and bipartisan policy idea for political mobilization.[21] The ODNI and DoD, to a lesser extent, later used the Chinese threat idea to rally regime policy action in the energy sector. Notably, those translated to efforts to secure the supply chain of the bulk power systems but not the more contentious distribution portion of the grid owing to sector-specific technical and political considerations. On a technical level, the proliferation of distributed and renewable energy resources accelerated decentralization, which worsened the visibility of grid operational data and complicated the case for

[20] The ODNI stated that: "Our most capable adversaries can access this supply chain at multiple points, establishing advanced, persistent, and multifaceted subversion. Our adversaries are also able to use this complexity to obfuscate their efforts to penetrate sensitive research and development programs, steal intellectual property (IP) and personally identifiable information (PII), insert malware into critical components, and mask foreign ownership, control, and/or influence (FOCI) of key providers of components and services. Individually and in total, these supply chain attacks erode our nation's competitive advantages in commerce, technology, and security (Salazar, 2017)."

[21] With the notable exception of Kaspersky, the Russian internet economy was never significantly coupled with the US.

regulatory oversight. CI operators in the energy sectors have a history of skirting CIP Reliability Standards to avoid fines and have vital interests in defining their own mandatory regulations. They only initiated a review of Chinese-owned bulk power system equipment in response to the FERC agenda, which mirrored Executive branch priorities.

Congress assigned DoE as the SSA for energy as opposed to the DHS, which focused on sector-specific cybersecurity integration by creating the office of the CESER. This sector-specific integration effort brought out the fragmentation inherent in the overall CIP structure. In the IT sector, the response was to centralize the functions of defensive cybersecurity management for federal networks (the consolidation of the NPPD and others into the CISA) and create an interagency ICT Supply Chain Risk Management Task Force that combines with the FCC C-SCRM mandate in using hardware and software country-of-origin restrictions. Overall, the implementation of cybersecurity policies was beset by political bargaining, regulatory overlap between agencies, and mission creep. For example, DHS was focused on too many policy problems: election security and information operations, nation-state cyber threat actors, threats on ICS, and physical security. The way the DHS was created was central in explaining internal and sector-specific politics, including departmental competition with unclear authorities and endemic problems with the federal government's information management. Therefore, the integration of the cybersecurity regime remained provisional throughout 2015-2020. The IT/OT convergence threat factors did not lead to significant convergence and integration of the cybersecurity regime compared to China's threat.

CHAPTER 8 THESIS CONCLUSION

As this research has demonstrated, the idea that Chinese ICT was a trojan horse for CCP strategy was more effective than IT/OT convergence to mobilize interests and advance coherent cybersecurity policy. At the same time, the intersection of both ideas was minimal. After the cyber-attacks on the Ukrainian grid, nation-state cyber threats diffused throughout the energy sector expert community and Executive branch priorities shifted to indirectly address IT/OT convergence but only in the energy sector.

Chapter 6 described how China's threat successfully induced policy coherence through the FIRMMA and ECRA institutional expansions. Trade and IT policy were successfully integrated to achieve cybersecurity goals as regime interests recognized that critical trade interdependencies could be "weaponized" to gain a domestic advantage. Specifically, Congress initiated an institutional reform resulting in a cohesive set of trade restrictions on Chinese ICT at the USTR's recommendation. Congress used FIRMMA to block inbound foreign direct investments in the telecommunications services and platform markets while simultaneously using ECRA to severely limit Chinese ICT firms' access to crucial semiconductor components through export controls.

The regulatory implementation of both incoming foreign investment controls and export controls, which used to be fraught with jurisdictional disagreements and poor coordination between agencies, was now primed for success. Multiple agencies and regulatory authorities were motivated by the threat of Chinese ICT and *successfully coordinated* over the CFIUS process, including DoC, the DoJ, and the FCC. While problems remained in the implementation, given the regulatory overlap between CFIUS

and Team Telecom, they were not a result of agency competition but likely due to a shared organizational instinct towards self-preservation.[1] The question of why CFIUS and Team Telecom were not unified — whether due to institutional inertia or the lack of a cybersecurity czar with jurisdiction on trade policy — remains open for future research. CFIUS and Team Telecom are likely to continue to leverage the cybersecurity regime's broad national security rationale to counter the Chinese Trojan horse, encroaching on ever-broader sectors of the digital economy in the process.

The USG's ability to deploy export controls depends on the coordination of implementing agencies and its ability to leverage allies in establishing an international enforcement regime. However, the Trump administration campaign against Chinese ICT was characterized by a unilateral application of hardware-based export controls and therefore carried a disintegrative effect on the regime, especially in the temporary incoherence of its implementation procedure. Therefore, the Trump administration created a further impetus for a political bargain between groups 1 & 2, using concessions on commodities trade as a bargaining chip for a more coherent whole-of-government plan to counter China. This political bargaining shows how exogenous political considerations can be a nontrivial causal determinant of regime integration. In sum, chapter 6 showed how a whole-of-government non-cooperative response to the rise of China was a stable political equilibrium because it intersected the agendas of many government agencies. The consensus policy solution leveraged a broadly defined national security interest to

[1] A more neutral theoretical explanation for incoherent policy design i.e., one that is disassociated from regime theory, appertains to policy implementation. When government agencies interpret top-down mandates, problems related organizational culture and inertia can affect impede implementation. For example, the division of organizational labor involving the assignment of policies to tasks can be interpreted to suit agencies 'ongoing processes and power structures resulting in agency competition. However, the lack of organizational competition between CFIUS and Team Telecom is noteworthy and warrants further examination as it suggests an alignment of regime interests.

decouple Chinese ICT from US markets, while actively undermining Chinese vendors abroad through supply chain risk-management initiatives aiming to limit communications equipment or services to "trusted suppliers."

Chapter 7 analyzed how IT/OT convergence was not a sufficiently robust or coalescing idea to drive the integration of ICT and energy sector cybersecurity policies. IT/OT convergence was only regarded as a valid threat among energy sector operators and did not gain sufficient traction in Congress. As theorized by the PRF, a vague threat notion in Congress combined with endogenous sector politics i.e., a negative interaction of ideas and sector-specific political interests related to the DHS impeded regime integration. While the cross-jurisdictional and interagency coordinative capacity for information sharing between the public and private sectors has long been established, the institutional inertia at the founding of Homeland Security has been a constant source of disjointed policymaking and implementation. Despite repeated Executive branch efforts at readjustments, chronic mismanagement issues have also impeded the integration of nationwide national preparedness targets. Instead, endogenous political forces sought to shift the locus of information control towards the DHS. In that period, more traditional all-hazards and cybersecurity threat framing motivated Congressional attempts to increase the regime's coherence and coordination over information sharing. Eventually, infrastructure operators' complaints about the incoherence by which resilience was operationalized and the need for "one cop on the block" led Congress to assign the DoE as the SSA for the energy sector. While regime actors mostly regarded this policy change as positive, the integration gap due to the lack of a regime czar continued to be felt.

The cyber-attacks on the Ukrainian grid were a focusing event that resulted in high within-sector coordination between operators, the E-ISAC, and other three-letter agencies in the intelligence and military community, which started seeking an adjustment to the offensive US cyber posture. However, despite a rise in the number of Russian ICS-based incidents on US operators around the time, the Executive branch shifted its priorities to strategic technologies motivated by a resurgence of great power competition. That said, critical infrastructure operators are concerned with cyber-physical attacks in the general sense, i.e., Russia and China are both equally worrisome threat actors. The idea that the Chinese dominance in the IT sector is an attack vector on the US power grid has low legitimacy in the energy sector, which followed the intelligence community's threat warnings that adversarial nation-states – not Chinese ICT in particular – could disrupt the electric grid with cyber-physical attacks. The federal government could not dictate that the energy sector's bulk power-system equipment procurement follow its Chinese ICT agenda. This finding highlights the importance of conceptualizing idea legitimacy as the interaction of ideas and interest for future PRF analyses.

After the CISA reform, which centralized and expanded defensive authorities at the DHS, the label of supply chain risk management provided a technical basis to apply country-of-origin restrictions through CISA-led interagency programs. As experts disagreed over how to address cyber threats, the USG attempted to apply its brand of public risk mitigation to handle private risk traditionally addressed in the market. However, despite many interagency efforts at coordinating those supply chain security efforts, such as the "Clean Networks initiative," a coherent USG response to ICT supply chain risks remained lacking.

The China threat idea was longer-lasting than all-hazards threats and more comparable to the durability of the War on Terror and IT/OT convergence. The pattern and sequence of China threat ideas were also noteworthy, especially since themes accumulated rather than disappeared and reappeared. However, a well-formulated policy idea embedding a problem-solution pathway that interest groups consistently lobby for is a necessary but insufficient condition for regime change. The negative interaction of ideas and institutions in the case of the Homeland Security regime — before it recognized China's threat — explains the unaccounted-for temporal dimension of regime theory, i.e., "anemic regimes" (Jochim and May, 2010). While the DoD and IC were a consistent source of reinforcement, their ideas did not significantly intrude on the civilian cybersecurity regime until a political equilibrium was later reached. Therefore, the positive interaction of ideas, interests, and institutions are necessary conditions for regime integration. Similarly, competition among national labs highlighted the importance of a motivating idea as a starting point to rally political support in the energy sector. The following section describes how the legitimacy of the regime response varied with the positions of policy entrepreneurs.

8.1 The role of policy entrepreneurs and its relation to the interaction of explanatory factors

The role of policy entrepreneurs was central in supporting the positions of China hawks in groups one, two, and three. Congressional representatives sought viewpoints from policy entrepreneurs that reinforced the overall preconception that China was a unified market and undifferentiated competitor. While policy entrepreneurs explored different competitive-cooperative economic solutions, ultimately, the competitive variants were

more uniform and in line with the dominant view of the three groups. Policy entrepreneurs presented a technical rationale whereby 5G raises stakes such that manufacturer trust becomes the preeminent concern. While some experts provided technical backing for that assertion in hearings, the matter of operator responsibility that other experts argue is crucial for security was sidelined.

Contrarian views proposing cooperative arrangements were rare and typically involved the position of academics. They argued that Chinese ICT firms are not undifferentiated competitors and share many aspects of the USG's unease with the CCP in its allowance of artificial monopolies.

The legitimacy of the China threat idea and competitive nature of the USG response described in chapter 6 was questioned by academics providing expert testimony and by group 3. The fundamental disagreement between policy experts was based on normative conjecture given the lack of evidence on whether the profit motive is sufficient to override Chinese ICT firms' willingness to cooperate with their Cybersecurity and National Intelligence laws. While moderate policy experts argued for a strategic pivot between cooperative and competitive trade stances with Chinese ICT firms, they failed to provide concrete and viable alternative solutions for representatives. Some of the shared positions between testifying experts included diversifying suppliers of core 5G telecom nodes in the IT sector. More extreme positions argued that software-defined networking was blurring distinctions between mobile telecommunications core and edge, effectively making the entire network more vulnerable and the issue of vendor origin more critical.

8.2 The validity of the Policy Regime Framework and future research

The Chinese political-economic system represents a foreign threat fundamentally incompatible with its US counterpart. The CCP will continue clashing with American values as it mimics the tying of economic, political, and potentially military threats while vying for world hegemony. There is little doubt that the perceived threat of China is enabling institutionalization and regime-like behavior in Washington D.C.

This research lends further validity to the Policy Regime Framework by analyzing cross-sector-spanning policy problems in the ICT space especially given recent calls for whole-of-government efforts to address emerging strategic technologies. This work highlighted the extent to which issues framed in the national security lens are more likely to gain traction in Washington compared to seemingly benign technical problems like IT/OT convergence. While the sensationalization and threat-politics involved with cybersecurity are not new, this research pointed to patterns showing identifiable policy mechanisms leading to explainable outcomes. As such, the study's findings transcend the individual details of the case and allow for generalization when exploring how the perceived threat of emerging strategic technologies will be negotiated in the USG.

The policy mechanisms in question are first mediated at the ideational level. As evident from this research, the choice of policy solution requires an alignment of endogenous and exogenous political interests to mediate the apprehension and risk-aversion stemming from technological threats. For example, IT/OT convergence was not framed as a national security threat and therefore could not be leveraged for policy change as much as

the threat of China.[2] While many high technology areas such as machine learning and quantum computing are poised to remain high on the USG's agenda, given that they all reduce to electron transfer via the Internet Protocol, cyberspace should remain the most fertile environment for threat politics. The second policy mechanism involves the effects of internal sector politics and bipartisan tensions on implementation. The PRF underscored the need to isolate both effects separately. Due to its *ad hoc* and isolationist ideology, and despite a nominally aggressive stance on China, the Trump administration amounted to disintegrated cybersecurity policy implementation. One would therefore expect further coherence and integration as a bipartisan alliance of China hawks further consolidates and aligns the cybersecurity regime's trajectory. Therefore, a cybersecurity regime motivated by China is likely durable. The institutional inertia set up by Congress with export controls and foreign investment restrictions makes any good-faith gesture from the Biden administration unlikely as it would require breaking the inertial forces behind the ongoing non-cooperative tit-for-tat game between both countries.

That said, considering the normative aspect of the cybersecurity regime's motivating threat idea, the defensive and offensive trade measures have raised questions about the regime's long-term viability, especially when paired with DoD's recent shift to a more offensive cyber posture.[3] While the regime's long-term effects on great power

---

[2] That said, in the event of a large-scale focusing event such as systemic outages in the energy sector, political attention may shift to IT/OT convergence and its underlying threat vectors.

[3] As a reminder, regimes can be durable but 'anemic'.
In 2018, the USG released a series of new cyber strategy documents that reflected a more offensive cyber posture intended to counter rival nation-states with advanced cyber-attack capabilities. These include DoD's "Defending Forward" strategy from the 2018 US Cyber Command Vision. The 2018 National Cyber Strategy similarly stated that the "The United States will develop swift and transparent consequences, which we will impose consistent with our obligations and commitments to deter future bad

competition and stability remain to be seen, the effects of this whole-of-government policy change carry strategic consequences that need to be investigated despite the ongoing implementation challenges highlighted in this work. For example, does a cybersecurity regime motivated by the threat of China contributes to more or less secure information management? Future research would be well served to explore the viability of "weaponized interdependence" and the viability of fusing strategic and economic aims for long-term stability. While the economic impacts of ICT trade can be measured, the impact of decoupling ICT sectors on security as a global public good raises the vital question of whether the trade-offs in economic welfare are worth the national security gains (Anderson, 2010; Ezell and Wu, 2017).

Future theory-building efforts could also consider internal and external threats to hegemony instead of the traditional balance of power, focusing solely on a state's need to counter foreign threats. A modified "omnibalancing" security theory that includes the PRF's accounting of internal political tensions within a defined regime where agents would have to simultaneously factor-in internal threats to their power and external IR threats may provide a complete theoretical picture (David, 1991). It became evident throughout this research that many of the political interests perpetuating the Trojan horse narrative operate under the constraint of short-term vested interests, a good-faith misunderstanding of technology, or an ideological distrust of globalism. At the root of the problem of how to compete with China in ICTs is a badly formulated national security rationale. The alignment of economic security with national security presents us with a

behavior." Whether the strategic objective was to deter engagement or to preemptively limit operational capabilities is subject of ongoing debate.

fundamentally incompatible approach for the ICT sector given that open trade is a requirement for growth and innovation. Since the cybersecurity regime is not about secure information management but power competition with China, the Biden administration would be better served by a more nuanced competitive-cooperative dynamic that leverages an alternative coalescing idea than that of an ICT Trojan horse. These considerations are especially relevant at the time of writing given the USG's failure to address the DoC's inconsistencies with its sanctions on Chinese ICTs at the time of writing.

APPENDICES

A. Appendices to chapter 6

A.1 Timeline of Huawei incidents

As two of the more globally prolific Chinese ICT firms, Huawei and ZTE presented representative cases of the relevant interplay of ideas, interests, and institutions contributing to the institutional expansions at all three junctures under consideration. The following table 8 summarizes a timeline of events relating to Huawei consolidated to display the main themes reported to have motivated specific incidents. While not all incidents are directly relevant to the analysis being outside the scope of the USG and timeline under consideration, they provide an important chronological context in understanding how ideas about Huawei spread and later motivated institutional changes at critical junctures. As shown by this summary of Huawei events, ideas, causal themes, and the evidence tend to match the predefined categories in figure # with some exceptions. Following this timeline helps contextualize the export control rules as an offensive measure against Huawei.

Table 8: Timeline of incidents involving Chinese ICTs with a specific focus on Huawei

Timeline	**Incident**	**Themes from the main idea**
2001	• Unnamed "Western officials" are said to have asked Beijing to investigate suspicions that Huawei violated U.N. sanctions by selling Iraq fiber-optic cable to improve links between antiaircraft missiles and the radar systems (Pomfret and Pan, 2001).	Untrustworthy, bad legal track record**,** they export Chinese authoritarianism to developing world or violate US and UN export control rules.

	• Indian security services accuse Huawei of aiding the Taliban in defiance of UN regulations (EE, 2001).	
2003-4	Against a backdrop of fierce competition to capture Chinese telecommunications market share in the 1990s, Huawei engages in reverse engineering of Cisco, Fujistu, and others to sell hardware in China (Bueri & huang, 2006). Cisco responds by producing documents to associate Huawei with the PLA as part of a marketing campaign. Cisco then sues Huawei on patent infringement after one of their employees was found to have copied 2% of 1.5 million lines of source code part of STRCMP generic string comparison routines (C language) (Kang, 2012). The issue is settled privately out of court in 2014 as Huawei modified the copied code (Cisco, 2012). Huawei's corporate governance structure attracts negative media attention as two former executives sue the firm in 2003 (Hawes, 2020).	Untrustworthy, bad legal track record, they violate IPR by stealing technology.
2005	The Air Force hires RAND Corporation to examine Chinese ICT firms. Rand declares that Huawei is part of a "digital triangle" alongside the Chinese military, state research groups, and other Chinese ICT firms. Rand argues the new process of "civilianization" introduces the profit-seeking motive to boost the military's IT readiness via public contracts (Rand, 2005).	Trojan horse for CCP grand strategy, Opaque corporate governance structures and behaviors, ulterior motives, facilitates the transfer of dual-use tech

2007	• In July 2007 Huawei founder and CEO Ren Zhengfei is interviewed by the FBI regarding a possible breach of US sanctions on Iran. The DoJ will later find Huawei to have violated a US export ban by supplying the North Korean wireless mobile system though another subsidiary Chinese company, SkyCom (LA Times, 2019). • Meanwhile, the NSA launches operation "ShotGiant" to exploit Huawei systems and source code as later leaked by Edward Snowden. Evidence of direct link between Huawei and the People's Liberation Army is lacking (New York Times, 2008, 2014).	Untrustworthy, Bad legal track record, they export Chinese authoritarianism to developing world or violate US and UN export control rules.
2008	CFIUS blocks Huawei from buying networking manufacturer 3Com on national security grounds. 3Com provided intrusion detection and prevention system for the US military. Senator John Kyl and representative Ileana Ros-Lehtinen led the Congressional charge. They warned that it would be a "grave error for US regulatory community to approve a deal that permits minority ownership in 3Com by one of	Trojan horse for CCP grand strategy, they have opaque corporate governance structures and behaviors, they have porous boundaries with cyber-PLA and intelligence units, acting as

	the least transparent companies operating in China, a firm with shadowy ties to Chinese army and intelligence services" (Reuters, 2007). This bipartisan political thrust cited the 2005 Rand report as evidence for ties between Huawei and the Chinese military.	(direct/indirect) intermediaries
2009	The UK Joint Intelligence Committee issues warning over the data and voice network conversion project, the BT 21CN network, from being partly supplied by Huawei. As 21CN used Huawei equipment in the past GCHQ warned that it had not paid "sufficient attention to the threat [from Huawei] in the past", warning that the network could have been open to attacks from China.	Chinese ICT firms need to be countered in the interest of national security, they have ulterior motives as either willing agents or unwitting participants of CCP grand strategy, they could 'backdoor' their equipment
2010	• In August, a group of eight Republican representatives addressed a letter to the Director of National Intelligence, the Secretaries of the Treasury and Commerce, and the Administrator of General Services, warning about Huawei's planned bid to supply equipment to Sprint Nextel Corp. • In September, four US representatives send a letter urging the FCC to consider restrictions that would make it harder	Chinese ICT firms need to be countered in the interest of national security, they have ulterior motives as either willing agents or unwitting participants of CCP grand strategy, they have porous boundaries with cyber-PLA and intelligence units, acting as

	for Huawei and ZTE to do business in the U.S (WSJ, 2010). • In November, Sprint Nextel Corp. excludes Huawei and ZTE from bidding on contract to upgrade mobile networks. DoD claimed it was "very concerned about China's emerging cyber capabilities and any potential vulnerability within or threat to DoD networks" (WSJ, 2010). In its annual report, the US-China commission had recently declared that China's rise in telecommunications raised risks for US national security. • CFIUS blocks Huawei's acquisition of 3Leaf Systems. • Huawei establishes Cyber Security Evaluation Center to perform vulnerability testing in partnership with British intelligence, GCHQ.	(direct/indirect) intermediaries as part of CCP MCF mechanisms
2011	• Huawei sends an open letter to the U.S government denying involvement with the Chinese government and invites an investigation. An investigation ensues. • FY 2012 National Defense Authorization Act ("NDAA") Committee Report details security concerns regarding Huawei and ZTE equipment. The report from the House	Trojan horse for CCP grand strategy, they need to be countered in the interest of national security, they have ulterior motives as either willing agents or unwitting participants of CCP grand strategy,

	Armed Services Committee noted: "[g]iven the potential ties between the Chinese Government and malicious actors within China, the committee is alarmed that two state-owned Chinese firms, Huawei and ZTE, [erroneous] have been included on the Department of Agriculture's list of safe and approved telecommunications equipment providers for the U.S. broadband expansion program. … [T]he committee is concerned about the potential threat this may pose to national security as well as to Department of Defense data." • After a Pentagon report on the Chinese military singled out Huawei as a company that maintains "close ties" to the PLA, the DoC barred Huawei in September from participating in FirstNet as part of a nation-wide public-safety wireless network for first responders stating they were a "security concern" COMPUTERWORLD UK, Oct. 14, 2011	they facilitate the transfer of dual-use technologies
2012	• The House Intelligence Committee headed by Mike Rogers publishes a seminal report on Huawei urging CFIUS to block any foreign direct investment from Huawei and ZTE in the US. The	Untrustworthy, Trojan Horse, needs to be countered for national security, they have a bad legal track record,

	report also requires the exclusion of Huwei and ZTE's equipment from federal systems and contractors. The private sector is "strongly encouraged" to refrain from transacting with both firms. • Meanwhile, British Prime Minister David Cameron confirmed a 1.3-billion-pound investment in Huawei. CEO Ren Zhengfei praises UK government and open market as "transparent, efficient and practical". The Economist decries US techno-nationalistic behavior based on the report's lack of evidence (Economist, 2012). • Reuters uncovers how Huawei supplied equipment to Iran's mobile operator through a proxy called Skycom that implicates Meng Wanzhou, the company's CFO • Spectrum Act prohibits 'barred' entities from participating in certain activities under FCC authority. Section 6004 of the 2012 Spectrum Act prohibits any entity or person "who has been, for reasons of national security, barred by any agency of the Federal Government from bidding on a contract, participating in an auction, or receiving a grant" from	they have opaque corporate governance structures and behaviors, they have ulterior motives as either willing agents or unwitting participants of CCP grand strategy, they have porous boundaries with cyber-PLA and intelligence units, acting as (direct/indirect) intermediaries as part of CCP MCF mechanisms, they are propped up as national champions and leveraged to corner global markets using techno-mercantile policies

	receiving FirstNet and state implementation funds or participating in a spectrum auction. According to the TIA, this provision was intended to prohibit Huawei or ZTE from formally participating in FirstNet.	
2013	• Michael Hayden describes Huawei as "unambiguous national security threat to the US and Australia". The U.S. approves purchase of Sprint Nextel by Softbank under conditions that exclude Huawei equipment (CRS, 2018). • In March, the Commerce, Justice, Science, and Related Agencies Appropriations Act bars certain agencies from purchasing IT systems from China-subsidized entities**.** Section 516 (b) bars the Departments of Commerce and Justice, NASA, and the National Science Foundation from purchasing IT systems "produced, manufactured or assembled" by entities "owned, directed, or subsidized by the People's Republic of China" unless the purchase is "in the national interest of the United States." Moreover, Section 516(a) requires that agencies must consult with the FBI or another appropriate federal entity to assess the risk of cyberespionage or sabotage before considering purchasing any such systems.	Chinese ICT firms are a Trojan horse hiding CCP grand strategy

2014	T-Mobile sues Huawei over misappropriation of trade secret "Tappy the Robot" designed to test mobile devices' touchscreens before they market. Huawei was found guilty of misappropriation in mid-2017 albeit without "malicious" intent proven. Huawei pays $4.8 million in damages down from $500 million originally demanded by T-Mobile (AH, 2018).	Chinese ICT firms are untrustworthy, they violate IPR by stealing technology
2017	• Draft strategy document by NSC member Brigadier General Rob Spalding leaks. The record reveals plans to counter China's dominance of 5G space achieved through Huawei's lead. It proposes the deployment of a nationalized network that "reflects our [US] principles". • China enacts its National Intelligence law which encourages "all organizations and citizens" to support in national intelligence work (Wired, 2018). • After the Kaspersky prohibition, Section 1656 of the NDAA FY 2018 bars the Department of Defense from "procur[ing] or obtain[ing], or extend[ing] or renew[ing] a contract" with Huawei or ZTE for "any equipment, system, or service" that forms a substantial component of any nuclear deterrence or homeland security mission.[34] Section 888 further empowers	Chinese ICT firms are a Trojan horse hiding CCP grand strategy

	the Defense Secretary to "terminate existing contracts or prohibit the award of contracts for the procurement of goods or services for the Department of Defense" from any "Chinese commercial entities" that "materially support the illicit activities on the part of North Korea."	
June 2017	• CFIUS blocks TCL Electronics Holdings Limited from acquiring Novatel Wireless, a $50 million deal	
September 2017	• CFIUS blocks Canyon Bridge Capital Partners from acquiring Lattice Semiconductor as it is partially funded by CCP, a 1.3 billion	Chinese ICT firms are a Trojan horse hiding CCP grand strategy
2018	• Huawei's deal with AT&T to distribute its flagship phone Mate 10 Pro is canceled a the last minute following letter signed by 18 members of US Senate and House intelligence committees to FCC chair (AH, 2018). Verizon follows suit shortly after. – January 8, 2018 • Rep. Michael Conaway and Liz Cheney introduce H.R.4747 Defending U.S. Government Communications Act co-sponsored by a republican majority and meant to block the US government from	Chinese ICT firms need to be decoupled from the US economy in the interest of national security

	using Huawei and ZTE hardware “or an entity reasonably believed to be owned or controlled by China”. February 7, 2018 • Huawei devices are banned from military bases entirely by order of the Pentagon. May 2nd 2018 • Arkansas Senator Tom Cotton and Florida Senator Marco Rubio amend the previous bill to include provision that aimed at preventing all federal agencies from "procuring or obtaining, renewing or extending a contract to obtain or procure, or entering into a contract with" any telecom company that uses any kind of technology from Huawei and ZTE, as well as any entity believed to be owned or otherwise controlled by China. • US starts leaning heavily on allies on 5G front: 1) Australian Signals Directorate head Mike Burgess claims that high-risk vendors could systematically threaten Australian critical infrastructure. Australia then bans Huawei 5G equipment altogether. 2) Sen. Mark Warner and Marco Rubio urge Canadian PM Trudeau to ban Huawei from 5G networks. 3) Washington starts a global campaign	

	urging allies like Germany, Italy, and Japan to drop trade with Huawei. • On 1 December 2018, Huawei CFO Meng Wanzhou indicted and arrested in Canada.	
2019	• Despite settlement in 2017, the DoJ files an industrial espionage indictment on January 16 through the US District Court at Seatle against Huawei for stealing code from T-Mobile known as "Tappy the Robot". • The DoJ serves Huawei indictments on January 24, 2019 accusing them of violating Iran sanctions "since at least 2016" (DoJ, 2019). • On January 28, the DoJ files criminal charges against Huawei's CFO who is arrested in Canada. A Huawei executive is arrested in Poland and is accused along with a Warsaw official of spying for Beijing (AH, 2018) • UK aims to correct for the "blunt instrument" of US export controls. 1) Mi6 head Alex Louder previously outspoken on Huawei says that a blanket ban was not an appropriate course for Britain adding that the subject matter was complex, and that maximum supplier diversity should be	Chinese ICT firms need to be decoupled from the US economy in the interest of national security

	UK CIP strategy. 20 Former GCHQ Robert Hannigan states that calls for blanket bans are "short on tech understanding of cybersecurity and 5G architecture". 3) UK NCSC says Huawei risk "manageable". 4) UK's Huawei oversight board finds plenty of bugs of engineering processes with problems but no more so than other vendors. 5) On April 24, the UK's NSC allows 5G procurement from Huawei for non-core tech such as antennas. • In April 19, the CIA claims Huawei receives funding from China's National Security Commission, the PLA and a branch of Chinese state intelligence network (CNET, 2019) • On May 1st, UK defense secretary Williamson is fired over allegedly leaking the plans allowing Huawei to provide non-core tech even though he was against allowing it. • On May 16, 2019, the Bureau of Industry and Security (BIS) amends the Export Administration Regulations (EAR) by adding Huawei Technologies Co., Ltd. (Huawei) to the Entity List, an embargo that cuts Huawei from US supply chain. All companies are forbidden from	

	exporting/transferring access to 152 Huawei affiliates. Global telecommunications and software have to choose between transacting with Huawei or being cut off from sourcing US tech/software. As a result, ARM is forced to comply with US regulations and retracts business contracts with Huawei. Google is forced to limit Android on Huawei and has 90 days to comply. • The UK bans Huawei from 5G network effective December 31. • The Bureau of Industry and Security's adds Huawei to its "entity-list" to on May 21st, stating there was "reasonable cause to believe that Huawei has been involved in activities contrary to the national security or foreign policy interests of the United States" (Federal Register, 2019). [5 year-long designation, material impact of estimated $30 billion] • Ren argues Huawei is being forcibly used as bargaining chip for US-China trade concerns (confirmed but only as far as Trumpian politics are concerned). • FCC passes its order banning use of its Universal Service Fund from being	

	spent on Huawei, deemed a threat to US national security. November 2019. After Huawei fights back, the ban is upheld in Dec 2020. • The Trump administration mulls placing Huawei on DoT's SDN list, the "nuclear option" that makes it virtually impossible for a company to transact in US dollars. Adding Huawei to the SDN list would have implied a host of logistical, diplomatic and economic difficulties for the USG given the impact on US allies that rely on Huawei for their 4G networks (Reuters, 2019).	
2020	• Minority voices at DoD claim Huawei hardware is not sensitive technology and that banning trade with them will harm the DIB's ability to remain competitive, which indirectly affects national security (WSJ, 2020; Purdy, 2020). • On August 17, 2020 DoC secretary Wilbur Ross continues reducing the margin by which the entity-list applies (the Foreign Direct Product Rule), (from at least 19% components made in the US to 10%) and claims "there has been a very highly technical loophole through which Huawei has been able, in effect,	Chinese ICT firms need to be decoupled from the US economy in the interest of national security

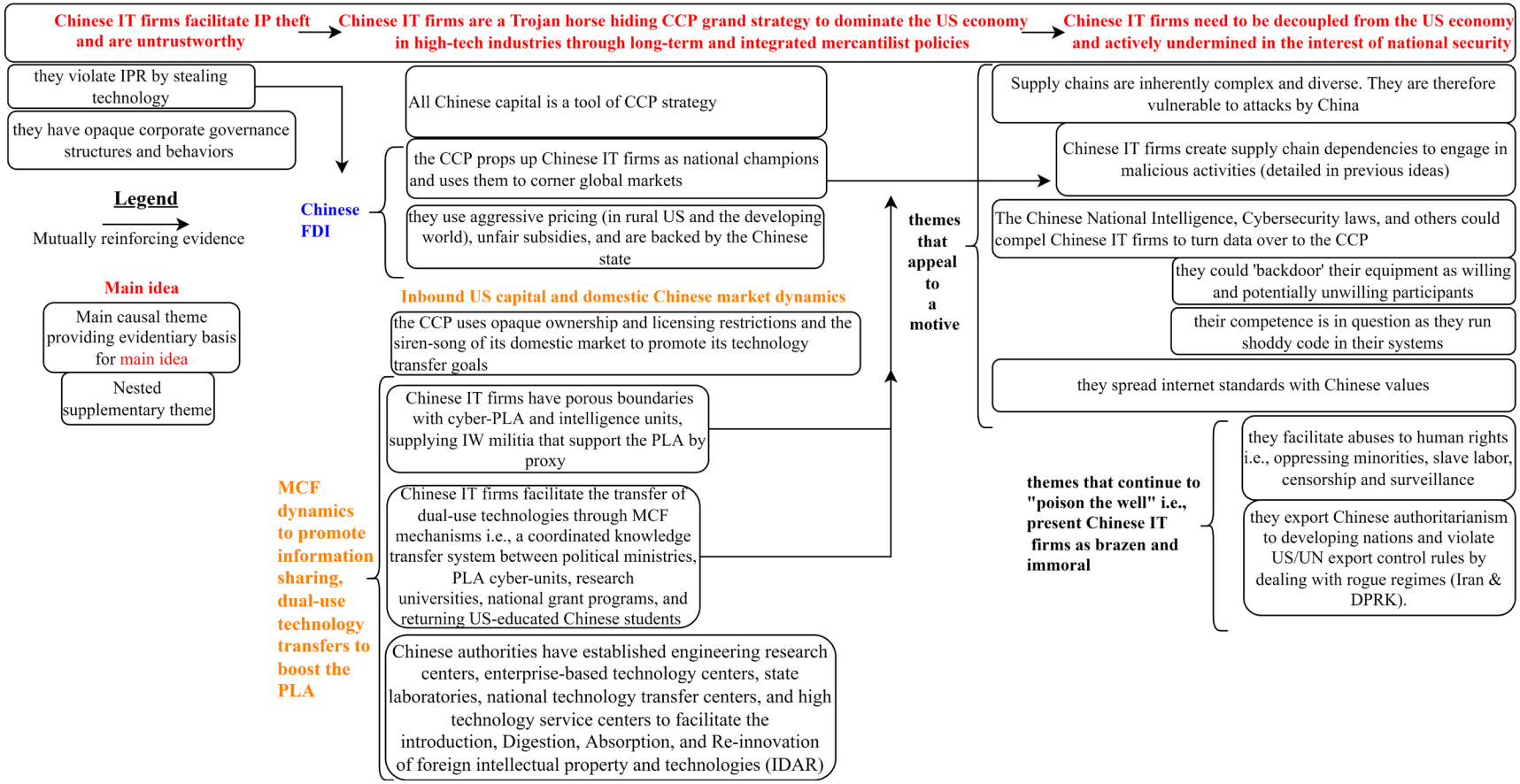
	to use US technology with foreign fab producers" (Reuters, 2020). • BIS further amended its direct product rule to further restrict Huawei and its affiliates' ability to receive certain semiconductor products. Bis expanded Export Administration Regulations (EAR) include offshore semiconductor production based on US tech. DoC's BIS further restricts Huawei's ability to use U.S. tech and software to design and manufacture its semiconductors abroad. The change (effective September 2020) is an amendment to a longstanding foreign-produced direct product rule as well as the "entity-list" to narrowly target Huawei's acquisition of semiconductors that are the product of U.S. software/hardware. It blocks any global company from using US-made hardware/software to design or produce chips for Huawei. • On May 15, 2020 the President of the semiconductor lobby John Neuffer declares the rule would "create uncertainty and disruption for the global semiconductor supply chain". However, the DoC and Trump administration more broadly continue citing threats to national security as motivating factor as	

	they continue to consider Huawei as beholden to the CCP. • Disappointed with DoT's Steve Mnuchin (often perceived as sympathetic to Beijing) China hawks proposed the NETWORKS act on March 12 2020. Rep. Gallego (D-Arizona) stated: "'American cutting edge technology has been systematically stolen by Chinese state actors for decades. As we develop 5G, it's clear that this frontier is no different," "Companies like Huawei who willfully compromise our information security and laws should be excluded from the global marketplace. I'm determined to work with my Congressional colleagues to protect U.S. networks and interests as we move into the 5G era,". Rep. Cheney (R-Wyoming) stated: "Just as a Russian or Iranian regime-controlled company that steals intellectual property or enables sanctions evasion would be placed on the Specially Designated Nationals (SDN) list, so should Huawei, a company controlled by the Chinese Communist Party that is facing charges for those exact activities. Security must be our first priority-especially when it comes to next-generation	

	telecommunications. Companies like Huawei should not be given free rein to infiltrate and monopolize 5G networks. They must be barred from the financial system so that the U.S., our allies, and others are not enabling their nefarious campaign," Senator Chuck Shumer (D-New York) stated: “China-based companies like Huawei cooperate heavily with the Chinese Communist Party and the Chinese government in political and economic espionage. Allowing China to dominate global 5G networks threatens America's national security. It is time for the Trump administration to take swift and forceful action to block Huawei from accessing the U.S. financial system”. (Cotton, 2019) • On April 9, 2020, the FCC, Department of Justice, and Department of Defense revoke and terminate China Telecom, Pacific Networks, ComNet, and China Unicom’s authorizations to provide Telecommunications services in the United States (DoJ, 2020). (as a result of team telecom?) • On August, 11 Trump bans TikTok and WeChat with Executive order until a	

	federal court repeals the decision on Sep. 28 • The director of the FBI has said that acts of espionage and theft by China's government pose the "greatest long-term threat" to the future of the US (BBC, 2020).	

A.2 Evolution of ideas of a Chinese threat in the cybersecurity regime, complete version



REFERENCES

Advanovsky, R.S. and McDougall, A., 2018. CI: Homeland Security and emergency preparedness. crc press

Aero Staff, (2016). FPGA development devices for radiation-hardened space applications introduced by Microsemi [online]. https://www.militaryaerospace.com. Available from: https://www.militaryaerospace.com/computers/article/16714808/fpga-development-devices-for-radiationhardened-space-applications-introduced-by-microsemi

Aggarwal, V.K. and Reddie, A.W., 2018. Comparative industrial policy and cybersecurity: a framework for analysis. Journal of Cyber Policy, 3(3), pp.291-305.

Aggarwal, V.K. and Reddie, A.W., 2020. New Economic Statecraft: Industrial Policy in an Era of Strategic Competition. Issues & Studies, p.2040006.

Allison, G., 2017. Destined for war: Can America and China escape Thucydides's trap?. Houghton Mifflin Harcourt.

Alt, J. E., & North, D. C. 1990. Political Economy of Institutions and decisions: Cambridge University Press

Anderson, R., Fuloria, S., 2010. Security economics and critical national infrastructure, in: Economics of Information Security and Privacy. Springer, pp. 55–66.

Andrews, Black (2020). Comments of the Telecommunications Industry Association. In the Matter of Protecting Against National Security Threats to the Communications Supply Chain Through FCC Programs. Federal Communications Commission. WC Docket No. 18-89.

Anton, S.D., Fraunholz, D., Lipps, C., Pohl, F., Zimmermann, M., Schotten, H.D., 2017. Two decades of SCADA exploitation: A brief history, in: 2017 IEEE Conference on Application, Information and Network Security (AINS). IEEE, pp. 98–104.

Apple CEO calls Bloomberg report '100% false' - CNN Video [online]. (no date). CNN.. Available from: https://www.cnn.com/videos/politics/2018/10/24/tim-cook-china-bloomberg-amanpour.cnn

Atkinson, R.D., 2012. Enough is enough: Confronting Chinese innovation mercantilism. Information Technology and Innovation Foundation.

Baker, L., 2017. Trump bars Chinese-backed firm from buying U.S. chipmaker Lattice. [online] Reuters.com. Available at: https://www.reuters.com/article/us-lattice-m-a-canyonbridge-trump/trump-bars-chinese-backed-firm-from-buying-u-s-chipmaker-lattice-idUSKCN1BO2ME

Bakis, B.J. and Wang, E.D., 2017. Building a national cyber information-sharing ecosystem. MITRE CORP Mcclean Virginia.

Baumgartner, F.R. and Jones, B.D., 2010. Agendas and instability in American politics. University of Chicago Press.

BBC News, (2020). FBI director: China is 'greatest threat' to US [online]. BBC News. Available at: https://www.bbc.com/news/world-us-canada-53329755

Beach, D. and Pedersen, R.B., 2019. Process tracing methods: Foundations and guidelines. University of Michigan Press.

Bellovin, S.M., Bradner, S.O., Diffie, W., Landau, S., 2011. Can It Really Work - Problems with Extending EINSTEIN 3 to Critical Infrastructure. Harv. Nat'l Sec. J. 3, 1–38.

Bendiek, A., Von Daniels, L. and Günther Hilpert, H., 2020. Strategic Rivalry Between United States And China. [online] Swp-berlin.org. Available at: https://www.swp-berlin.org/10.18449/2020RP04/

BIS, 2020. Huawei Entity List Frequently Asked Questions (FAQs) [WWW Document]. URL https://www.bis.doc.gov/index.php/documents/pdfs/2447-huawei-entity-listing-faqs/file

Blau, P.M., 1970. A formal theory of differentiation in organizations. American sociological review, pp.201-218.

Bloomberg Finance L.P. (2021). Wire: Bloomberg News (BN). "Huawei" from 01/1/95 to 08/30/2020. Retrieved from Bloomberg database.

Blumenthal, M.S., Clark, D.D., 2001. Rethinking the Design of the Internet: The End-to-End Arguments vs. the Brave New World: Defense Technical Information Center, Fort Belvoir, VA. https://doi.org/10.21236/ADA629281

Blustein, 2019. The Untold Story of How George W. Bush Lost China. Foreign Policy. October, 4, 2019. https://foreignpolicy.com/2019/10/04/the-untold-story-of-how-george-w-bush-lost-china/

Blyth, M.M., 1997. "Any More Bright Ideas?" The Ideational Turn of Comparative Political Economy. Comparative Politics 29, 229–250. https://doi.org/10.2307/422082

Bosnjak, D., 2018. FCC Asked To Investigate Huawei's US Smartphone Plans: Report. [online] Android Headlines. Available at: https://www.androidheadlines.com/2018/01/fcc-asked-to-investigate-huaweis-us-smartphone-plans-report.html

Bosnjak, D., 2018. Huawei & US Government Timeline: A Standoff Years in The Making. [online] Android Headlines. Available at:

https://www.androidheadlines.com/2018/04/huawei-us-government-timeline-a-standoff-years-in-the-making.html

Bown, C.P., 2020. How the United States marched the semiconductor industry into its trade war with China. East Asian Economic Review, 24(4), pp.349-388.

Bown, C.P., 2020. How Trump's Export Curbs on Semiconductors and Equipment Hurt the US Technology Sector. Peterson Institute for International Economics Trade and Investment Policy Watch, September, 28.

Brake, D., Bruer, A., 2020. The Great 5G Race: Is China Really Beating the United States? Information Technology and Innovation Foundation.

Brown, M. and Singh, P., 2018. China's technology transfer strategy. Silicon Valley, CA: Defense Innovation Unit Experimental (DIUx)Report.

Brumfield, C., 2019. What is the CISA? How the new federal agency protects critical infrastructure [Online]. CSO. Available at: https://www.csoonline.com/article/3405580/what-is-the-cisa-how-the-new-federal-agency-protects-critical-infrastructure-from-cyber-threats.html

Buchanan, B. 2017. The Cybersecurity Dilemma: Hacking, Trust, and Fear Between Nations. Oxford University Press.

Bureau of Industry and Security (BIS), 2020. Export Administration Regulations: Amendments to General Prohibition Three (Foreign-Produced Direct Product Rule) and the Entity List https://www.federalregister.gov/documents/2020/05/19/2020-10856/export-administration-regulations-amendments-to-general-prohibition-three-foreign-produced-direct

Buzan, B., Wæver, O., Wæver, O. and De Wilde, J., 1998. Security: A new framework for analysis. Lynne Rienner Publishers.

Canadian Security Intelligence Service, (CSIS). China's intelligence law and the country's future intelligence competitions - Canada.ca. Available at: https://www.canada.ca/en/security-intelligence-service/corporate/publications/china-and-the-age-of-strategic-rivalry/chinas-intelligence-law-and-the-countrys-future-intelligence-competitions.html

Candel, J.J. and Biesbroek, R., 2016. Toward a processual understanding of policy integration. Policy Sciences, 49(3), pp.211-231.

Capri, A., 2020. Semiconductors at the Heart of the US-China Tech War. Hinrich Foundation, https://www. hinrichfoundation. com/research/white-paper/trade-and-technology/semiconductors-at-the-heart-of-the-us-china-tech-war.

Carr, M., 2016. Public–private partnerships in national cyber-security strategies. International Affairs, 92(1), pp.43-62.

Cavelty, M.D, 2013. From cyber-bombs to political fallout: Threat representations with an impact in the cyber-security discourse. International Studies Review, 15(1), pp.105-122.

Cavelty, M.D., 2007. Cyber-security and threat politics: US efforts to secure the information age. Routledge.

Cejudo, G.M. and Michel, C.L., 2017. Addressing fragmented government action: Coordination, coherence, and integration. Policy Sciences, 50(4), pp.745-767.

Center for Strategic and International Studies (CSIS). Public-Private Partnerships for Critical Infrastructure Protection. August 19, 2013

CFIUS Reform: Administration Perspectives on the Essential Elements [online]. (no date). United States Committee on Banking, Housing, and Urban Affairs. Available from: https://www.banking.senate.gov/hearings/cfius-reform-administration-perspectives-on-the-essential-elements

Chandler, M. (2012). Huawei and Cisco's Source Code: Correcting the Record - Cisco Blogs. Cisco Blogs. Available at: https://blogs.cisco.com/news/huawei-and-ciscos-source-code-correcting-the-record

Chaudhary, T., Jordan, J., Salomone, M. and Baxter, P., 2018. Patchwork of confusion: the cybersecurity coordination problem. Journal of Cybersecurity, 4(1), p.tyy005.

Chen, Z., Wang, C., Li, G., Lou, Z., Jiang, S., Galis, A., 2020. New IP framework and protocol for future applications, in: NOMS 2020-2020 IEEE/IFIP Network Operations and Management Symposium. IEEE, pp. 1–5.

Cheung, T.M., 2020. Understanding the New Great Power Competition [WWW Document]. URL https://igcc.ucsd.edu/news-events/news/understanding-the-new-great-power-competition.html

Chisholm, D., 1995. Problem solving and institutional design. Journal of Public Administration Research and Theory, 5(4), pp.451-492.

Christensen, T. and Lægreid, P., 2007. The whole-of-government approach to public sector reform. Public administration review, 67(6), pp.1059-1066.

Cimpanu, C., (2019). APT-doxing group exposes APT17 as Jinan bureau of China's Security Ministry | ZDNet [online]. ZDNet. Available from: https://www.zdnet.com/article/apt-doxing-group-expose-apt17-as-jinan-bureau-of-chinas-security-ministry/

CISA, 2021. Russia Cyber Threat Overview and Advisories | CISA [WWW Document]. URL https://us-cert.cisa.gov/russia

Clapper, J., 2011. Statement for the Record. Worldwide Threat Assessment of the US Intelligence Community. Armed Services Committee.

Clark, D.D., 2018. Designing an internet, Information policy series. The MIT Press, Cambridge, Massachusetts.

Clark, J.; Gilstrap, M.; Amin, S.; DeCorla-Souza, K. United States Electricity Industry Primer. Department of Energy 2015, 6.

Clarke Y. (2013). Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies of the Committee on Homeland Security. Cyber Threats from China, Russia, and Iran: Protecting American Critical Infrastructure.

Clinton, H., 2011. America's Pacific Century. Foreign Policy. URL https://foreignpolicy.com/2011/10/11/americas-pacific-century/

Cole, S., n.d. Cyberwarfare: Battlefield precursor for kinetic attacks? - Military Embedded Systems [Online]. Available at: http://dev007.militaryembedded.com/cyber/cybersecurity/cyberwarfare-battlefield-precursor-for-kinetic-attacks

Council on Foreign Relations. APT 17 [online]. (no date). Available from: https://www.cfr.org/cyber-operations/apt-17

Council on Foreign Relations. Timeline: U.S. Relations With China 1949–2021. [online] cfr.org. Available at: https://www.cfr.org/timeline/us-relations-china

Cowhey, P.F., 1990. The international telecommunications regime: the political roots of regimes for high technology. International Organization, pp.169-199.

Coyne, R., 2005. Wicked problems revisited. Design studies, 26(1), pp.5-17.

Crapo, M., 2019. Crapo Statement at Hearing on Export Controls. [online] Banking.senate.gov. Available at: https://www.banking.senate.gov/imo/media/doc/Crapo%20Statement%207-18-19.pdf

Critical Infrastructure Cross Sector Council Charter [online]. (no date). cisa.gov. Available from: https://www.cisa.gov/sites/default/files/publications/chartercscapp-508.pdf

Critical Infrastructure Protection: Key Private and Public Cyber Expectations Need to Be Consistently Addressed [online]. (no date). U.S. Government Accountability Office (U.S. GAO). Available from: https://www.gao.gov/products/gao-10-628

CSIS, 2021. Significant Cyber Incidents | Center for Strategic and International Studies [Online]. Available at: https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents

Cyberspace Solarium Commission., 2020. [online] Available at: https://www.solarium.gov/

Daugirdas, K. and Mortenson, J.D., 2017. Contemporary Practice of the United States Relating to International Law. AJIL, 111, pp.781-783.

David, S.R., 1991. Explaining Third World Alignment. World Pol. 43, 233–256. https://doi.org/10.2307/2010472

Davis, B., 2020. Pentagon Blocks Clampdown On Huawei Sales. [online] WSJ. Available at: https://www.wsj.com/articles/pentagon-blocks-clampdown-on-huawei-sales-11579870801

Davis, B., 2020. Pentagon Blocks Clampdown on Huawei Sales. Wall Street Journal.

Deibert, R.J., Rohozinski, R., Manchanda, A., Villeneuve, N. and Walton, G.M.F., 2009. Tracking ghostnet: Investigating a cyber espionage network.

DeLauro, R., 2019. Appropriations Committee Releases Fiscal Year 2020 Homeland Security Funding Bill [Online]. House Committee on Appropriations. Available at: https://appropriations.house.gov/news/press-releases/appropriations-committee-releases-fiscal-year-2020-homeland-security-funding

Department of Commerce. Bureau of Industry and Security. General Prohibition No. 3: Foreign-Produced Direct Product Rule § 736.2(b)(3). [online] https://www.bis.doc.gov/ Available at: https://www.bis.doc.gov/index.php/licensing/reexports-and-offshore-transactions/direct-public-guidelines

Department of Homeland Security (DHS) 2021. Fusion Centers. Online, available at: https://www.dhs.gov/fusion-centers#

Department of Homeland Security, NIPP 2013: Partnering for Critical Infrastructure Security and Resilience, (Washington D.C.: DHS, 2013): 2–56, available at: https://www.cisa.gov/publication/nipp-2013-partnering-critical-infrastructure-security-and-resilience

Department of Justice, June 2020. Office of Public Affairs. Team Telecom Recommends that the FCC Deny Pacific Light Cable Network System's Hong Kong Undersea Cable Connection to the United States. Available at: https://www.justice.gov/opa/pr/team-telecom-recommends-fcc-deny-pacific-light-cable-network-system-s-hong-kong-undersea

Department of State. U.S. Collective Defense Arrangements [online]. (no date). U.S. Department of State Archive. Available from: https://2009-2017.state.gov/s/l/treaty/collectivedefense/index.htm

DHS, 2014. Incident Reponse/Vulnerability Coordination in 2014.

Diffie, W. and Landau, S., 2010. Privacy on the line: The politics of wiretapping and encryption (p. 496). The MIT Press.

DoE, 2009. Cyber_Security_Governance_051811.pdf [WWW Document]. Information Management Governance Council. [Online] Available at: https://www.energy.gov/sites/prod/files/cioprod/documents/Cyber_Security_Governance_051811.pdf

DoJ, 2017 U.S. Charges Three Chinese Hackers Who Work at Internet Security Firm for Hacking Three Corporations for Commercial Advantage

DOJ, 2020. Six Russian GRU Officers Charged in Connection with Worldwide Deployment of Destructive Malware and Other Disruptive Actions in Cyberspace [Online]. Available at: https://www.justice.gov/opa/pr/six-russian-gru-officers-charged-connection-worldwide-deployment-destructive-malware-and

DoJ, 2020. Team Telecom Recommends that the FCC Deny Pacific Light Cable Network System's Hong Kong Undersea Cable Connection to the United States [Online]. Available at : https://www.justice.gov/opa/pr/team-telecom-recommends-fcc-deny-pacific-light-cable-network-system-s-hong-kong-undersea

DoJ, 2021. The Committee For the Assessment of Foreign Participation in the United States Telecommunications Services Sector – Frequently Asked Questions.

DoS, 2008 CFIUS reform: The Foreign Investment & National Security Act of 2007 https://www.treasury.gov/resource-center/international/foreign-investment/Documents/Summary-FINSA.pdf

Dunn, M., 2009. Cyber-Security and Threat Politics: US efforts to secure the information age. Routledge.

Dunn, M., 2013. From cyber-bombs to political fallout: Threat representations with an impact in the cyber-security discourse. International Studies Review, 15(1), pp.105-122.

Eisenhauer, J., Donnelly, P., Ellis, M., O'Brien, M., 2006. Roadmap to Secure Control Systems in the Energy Sector 58.

ELECTRUM | Dragos (2020) [Online]. Available at: https://www.dragos.com/threat/electrum/ (accessed 9.24.21).

Enose, N., 2014. Implementing an integrated security management framework to ensure a secure smart grid, in: 2014 International Conference on Advances in Computing, Communications and Informatics (ICACCI). Presented at the 2014 International Conference on Advances in Computing, Communications and Informatics (ICACCI), IEEE, Delhi, India, pp. 778–784. https://doi.org/10.1109/ICACCI.2014.6968521

EPIC, 2010. EPIC - Perfect Citizen [WWW Document]. URL https://epic.org/privacy/cybersecurity/nsa-perfect-citizen/default.html (accessed 9.16.21).

Eriksson, J., 2001. Cyberplagues, IT, and security: Threat politics in the information age. Journal of Contingencies and Crisis Management, 9(4), pp.200-210.

Ezell, S.J., Wu, J.J., 2017. How Joining the Information Technology Agreement Spurs Growth in Developing Nations. INFORMATION TECHNOLOGY 60.

Farhat, K., Mueller, D.M., 2020. Energy Infrastructure and Industrial Data: Between Global Data Policies and an Evolving iIoT Environment 45.

FCC, 2020. FCC Affirms Designation of Huawei as National Security Threat [WWW Document]. Federal Communications Commission. URL https://www.fcc.gov/document/fcc-affirms-designation-huawei-national-security-threat (accessed 10.19.21).

Federal Bureau of Investigation (2016) Best Practices in Supply Chain Risk Management for the U.S. Government. Online, available at: https://www.fbi.gov/file-repository/scrmbestpractices-1.pdf/view

Federal Communications Commission (FCC). 2019. Memorandum Opinion and Order. In the Matter of China Mobile International (USA) Inc. Application for Global Facilities-Based and Global

Federal Communications Commission (FCC). 2021. In the Matter of China Unicom (Americas) Operations Limited. Order Instituting Proceeding On Revocation. March 19, 2021. Online. Available at: https://docs.fcc.gov/public/attachments/FCC-21-37A1.pdf

Federal Communications Commission. WC Docket No. 18-99, Protecting National Security Through FCC Programs. “Protecting Against National Security Threats to the Communications Supply Chain Through FCC Programs” Online. Available at: https://www.fcc.gov/document/protecting-national-security-through-fcc-programs-0

Federal Energy Regulatory Commission (FERC). 2019. Security Investments for Energy Infrastructure Technical Conference Comments of the Electric Power Supply Association. Washington, D.C., May 28, 2019.

Fergusson, I. and Kerr, P., 2020. The U.S. Export Control System and the Export Control Reform Initiative. [online] Federation of American Scientists (Fas.org). Available at: https://fas.org/sgp/crs/natsec/R41916.pdf

Fischer, 2014. Federal Laws Relating to Cybersecurity: Overview of Major Issues, Current Laws, and Proposed Legislation. Congressional Research Service https://fas.org/sgp/crs/natsec/R42114.pdf

Fischerkeller, M.P., Harknett, R.J., 2018. Persistent Engagement and Tacit Bargaining: A Path Toward Constructing Norms in Cyberspace.

Fischerkeller, M.P., Harknett, R.J., 2019a. A Response on Persistent Engagement and Agreed Competition.

Fischerkeller, M.P., Harknett, R.J., 2019b. What Is Agreed Competition in Cyberspace?

Fitch, A. & O'Keeffe, K. 2020, Qualcomm Lobbies U.S. to Sell Chips for Huawei 5G Phones; Smartphone chip maker warns of potentially losing billions of dollars in sales because of export limits, New York, N.Y.

Fitzgerald et al.2016 https://ecfsapi.fcc.gov/file/10818156479720/White%20Paper.pdf

Flinta, C., 2019. Digging Into IPv6 Traffic to Google: Is 28% Deployment Really the Limit? [Online]. Available at: http://circleid.com/posts/20190529_digging_into_ipv6_traffic_to_google_is_28_percent_deployment_limit

Franco, J., 2018. NPPD Leader Ready for Recognition as 'National Cybersecurity Agency' [WWW Document]. URL https://www.meritalk.com/articles/krebs-on-cisa-passage/ (accessed 10.13.21).

Fritz, A., 2019. China's Evolving Conception of Civil-Military Collaboration. CSIS, August, 2, p.2019.

Fukuyama, F., 1989. The end of history? The national interest, (16), pp.3-18.

Gagliardone, I., 2020. The Impact of Chinese Tech Provision on Civil Liberties in Africa.

GAO, 2011. Electricity Grid Modernization: Progress Being Made on Cybersecurity Guidelines, but Key Challenges Remain to be Addressed [WWW Document]. URL https://www.gao.gov/assets/gao-11-117.pdf (accessed 10.11.21).

GAO-19-332, 2019. Critical Infrastructure Protection: Actions Needed to Address Significant Cybersecurity Risks Facing the Electric Grid.

Gartzke, E., Lindsay, J.R., 2015. Weaving Tangled Webs: Offense, Defense, and Deception in Cyberspace. Security Studies 24, 316–348. https://doi.org/10.1080/09636412.2015.1038188

George, A.L. and Bennett, A., 2005. Case studies and theory development in the social sciences. mit Press.

Glaser, C.L., 1997. The security dilemma revisited. World politics, 50(1), pp.171-201.

Goldstein, J. and Keohane, R.O. eds., 1993. Ideas and foreign policy: beliefs, institutions, and political change. Cornell University Press.

Goldstein, J., 1993. Ideas, interests, and American trade policy. Cornell University Press.

Google, n.d. IPv6 – Google [WWW Document]. URL https://www.google.com/intl/en/ipv6/statistics.html#tab=per-country-ipv6-adoption (accessed 9.24.21).

Gopstein, A., n.d. NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 4.0. NIST Special Publication 239.

Gorman, S., 2009. Electricity Grid in U.S. Penetrated By Spies. Wall Street Journal, Eastern edition A.1.

Gorwa, Robert, and Max Smeets. "Cyber Conflict in Political Science: A Review of Methods and Literature." (2019).

Graff, G. M. (2020, January 16). Inside the feds' battle against Huawei. Wired. https://www.wired.com/story/us-feds-battle-against-huawei/

Green, B. (2021) Open Source Threat Intelligence Feeds

Grindal, K., 2019. Trade regimes as a tool for cyber policy. Digital Policy, Regulation and Governance.

Haas, D. and Leoni M. 2019. The Useful Life of Microprocessor-Based Relays: A Data-Driven Approach. 72nd Annual Conference for Protective Relay Engineers College Station, Texas March 25–28, 2019. Online:[http://prorelay.tamu.edu/wp-content/uploads/sites/3/2019/03/TheUsefulLife_6904_20190313.pdf]

Halbert, D., 2016. Intellectual property theft and national security: Agendas and assumptions. The Information Society, 32(4), pp.256-268.

Hall, P.A., 1993. Policy paradigms, social learning, and the state: the case of economic policymaking in Britain. Comparative politics, pp.275-296.

Hannan, M.T. and Freeman, J., 1977. The population ecology of organizations. American journal of sociology, 82(5), pp.929-964.

Harknett, R.J., Smeets, M., 2020. Cyber campaigns and strategic outcomes. Journal of Strategic Studies 0, 1–34. https://doi.org/10.1080/01402390.2020.1732354

Harold, S.W., Libicki, M.C. and Cevallos, A.S., 2016. Getting to yes with China in cyberspace. Rand Corporation.

Harold, S.W., Nakagawa, Y., Fukuda, J., Davis, J.A., Kono, K., Cheng, D. and Suzuki, K., 2017. The US Japan Alliance and Deterring Gray Zone Coercion in the Maritime, Cyber, and Space Domains.

Haselton, T., (2018). FBI director on whether Apple and Amazon servers had Chinese spy chips: 'Be careful what you read' [online]. CNBC. Available from: https://www.cnbc.com/2018/10/10/fbi-director-wray-on-super-micro-servers-be-careful-what-you-read.html

Hawes, C., 2020. Why is Huawei's ownership so strange? A case study of the Chinese corporate and socio-political ecosystem. Journal of Corporate Law Studies, pp.1-38.

Healey, J. ed., 2013. A fierce domain: Conflict in cyberspace, 1986 to 2012. Cyber Conflict Studies Association.

Heginbotham, E., 2015. The U.S.-China Military Scorecard: Forces, Geography, and the Evolving Balance of Power, 1996-2017. RAND, Santa Monica, CA.

Heginbotham, E.et al., 2015. China's Military Modernization Increasingly Challenges U.S. Defense Capabilities In Asia. [online] Rand.org. Available at: https://www.rand.org/pubs/research_reports/RR392.html

Heritage, I., 2019. Protecting Industry 4.0: challenges and solutions as IT, OT and IP converge. Network Security 2019, 6–9. https://doi.org/10.1016/S1353-4858(19)30120-5

Hill, J.F., 2012. A Balkanized Internet?: The Uncertain Future of Global Internet Standards. Georgetown Journal of International Affairs, pp.49-58.

Hoffmann, S., Lazanski, D., Taylor, E., 2020. Standardising the splinternet: how China's technical standards could fragment the internet. Journal of Cyber Policy 5, 239–264. https://doi.org/10.1080/23738871.2020.1805482

Hogan, J. and Doyle, D., 2007. The importance of ideas: An a priori critical juncture framework. Canadian Journal of Political Science/Revue canadienne de science politique, pp.883-910.

Hogan, J., 2006. Remoulding the critical junctures approach. Canadian Journal of Political Science/Revue canadienne de science politique, pp.657-679.

Homel, U.S.S.C. on, Security, Washington, G.A. 340 D.S.O.B., DC, Committee, 20510224-2627 Get Directions Contact The, 2012. Minority Media | Homeland Security & Governmental Affairs Committee | Homeland Security & Governmental Affairs Committee [Online]. Available at: http://www.hsgac.senate.gov/

Homeland Security Presidential Directive 7 | CISA [online]. (2003). Homepage | CISA. Available from: https://www.cisa.gov/homeland-security-presidential-directive-7

https://www.justice.gov/nsd/committee-assessment-foreign-participation-united-states-telecommunications-services-sector

https://www.justice.gov/opa/pr/us-charges-three-chinese-hackers-who-work-internet-security-firm-hacking-three-corporations

https://www.senki.org/operators-security-toolkit/open-source-threat-intelligence-feeds/

Hutchinson, K.B., 2012. U.S. Senate Senate legislative Session [WWW Document]. URL https://www.c-span.org/video/?307260-1/senate-session

IARIA, 2021. Renwei (Richard) Li, Ph.D.

International Monetary Fund (IMF). World Economic Outlook Database. Available from: https://www.imf.org/external/pubs/ft/weo/2014/02/weodata/index.aspx]

Investigative Report on the U.S. National Security Issues Posed by Chinese Telecommunications Companies Huawei and ZTE. 2012. House Permanent Select Committee on Intelligence (HPSCI). Washington, D.C.

Jackson, J., 2018. The Committee on Foreign Investment in the United States (CFIUS). [online] Federation of American Scientists (fas.org). Available at: https://fas.org/sgp/crs/natsec/RL33388.pdf

Jasper, S.E., 2017. US cyber threat intelligence sharing frameworks. International Journal of Intelligence and CounterIntelligence, 30(1), pp.53-65.

Jensen, B., Valeriano, B., Maness, R., 2019. Fancy bears and digital trolls: Cyber strategy with a Russian twist.

Jiang, S., 2018. ZTE employees in China cheer Trump tweet. [online] U.S. Available at: https://www.reuters.com/article/us-usa-china-zte-trump/zte-employees-in-china-cheer-trump-tweet-idUSKCN1IF0RP

Jnagal , et al. (2010). Quality of service in virtual computing environments (7,711,789). U.S. Patent and Trademark Office.

Jochim, A.E. and May, P.J., 2010. Beyond subsystems: Policy regimes and governance. Policy Studies Journal, 38(2), pp.303-327.

John Pomfret and Philip P. Pan 2001, Chinese Firm Is Focus of U.S. Iraqi Suspicions: The Washington Post, Washington, D.C.

Johnson, Ian. 2012. “China's lost decade.” New York Review of Books, 27 September. Available at: http://www.nybooks.com/articles/archives/2012/sep/27/chinas-lost-decade/.Google Scholar

Jones, B.D. and Baumgartner, F.R., 2005. The politics of attention: How government prioritizes problems. University of Chicago Press.

Josten, B., 2012. Chambre of Commerce letter to the members of the United States Senate [Online]. Available at: https://www.steptoe.com/images/content/2/6/v1/2689/4441.pdf]

Kahan, J.H., 2014. Preparedness Revisited: W(h)ither PPD-8? Homeland Security Affairs X.

Kahan, Jerome H. “Resilience Redux: Buzzword or Basis for HS.”Homeland Security Affairs 11, Article 2 (February 2015). https://www.hsaj.org/articles/1308

Kahneman, D., Tversky, A., 1981. The Simulation Heuristic.

Kan, M., 2011. Huawei asks why U.S. barred it from emergency network project. [online] Computerworld. Available at: https://www.computerworld.com/article/2498771/huawei-asks-why-u-s--barred-it-from-emergency-network-project.html

Katz, J., 2020. Senate proposes $58M boost to CISA's budget to clear out risk assessment backlog - [Online]. FCW. Available at: https://fcw.com/articles/2020/11/24/nccic-backlog-approps-senate.aspx

Kavanagh, D. and Richards, D., 2001. Departmentalism and joined-up government. Parliamentary Affairs, 54(1), pp.1-18.

Kean, T. and Hamilton, L., 2004. The 9/11 commission report: Final report of the national commission on terrorist attacks upon the United States (Vol. 3). Government Printing Office.

Kemp, H., (2017). Left of Launch: Countering Theater Ballistic Missiles [online]. Atlantic Council - Shaping the global future together. Available from: https://www.atlanticcouncil.org/wp-content/uploads/2017/07/Left_of_Launch_web_0731.pdf

Keohane, R.O., 1982. The Demand for International Regimes.

Khan, S.M., Mann, A. and Peterson, D., 2021. The Semiconductor Supply Chain: Assessing National Competitiveness. Washington, DC: Center for Security and Emerging Technology.

Kingdon, J., 1995. Agendas, alternatives, and public policies., 2nd. NY: Haper Collins College Publisher. ed.

Kingdon, J.W., 1989. Congressmen's voting decisions. University of Michigan Press.

Kirk, J., 2011. "Night Dragon" Attacks From China Strike Energy Companies [WWW Document]. PCWorld. URL https://www.pcworld.com/article/219251/article.html (accessed 9.11.21).

Klimburg, A. ed., 2012. National cyber security framework manual. NATO Cooperative Cyber Defense Center of Excellence.

Koschinsky, J. and Swanstrom, T., 2001. Confronting Policy Fragmentation: A Political Approach to the Role of Housing Nonprofits. Review of Policy Research, 18(4), pp.111-127.

Krasner, S.D., 1999. Sovereignty: organized hypocrisy Princeton University Press. Princeton, NJ.

Krebs, C., 2017. Examining DHS's Cybersecurity Mission.

Krekel, B., Adams, P. and Bakos, G., 2014. Occupying the information high ground: Chinese capabilities for computer network operations and cyber espionage. International Journal of Computer Research, 21(4), p.333.

Krugman, R.P., Obstfeld, M. and Melitz, J.M., 2018. International trade: Theory and policy. Pearson Education Limited.

Kuehn, A. and McConnell, B., 2020. Weathering TechNationalism. [online] https://www.eastwest.ngo/. Available at: https://www.eastwest.ngo/technationalism

Kuerbis, B., 2018. The flaws and risk in the Kaspersky case - Internet Governance Project. Internet Governance Project. Available at: https://www.internetgovernance.org/2018/02/19/flaws-risk-kaspersky-case/

Kynge, J. 1998, Disappointment despite growth of 35%: CHINA by James Kynge in Beijing: A surge of forceful local competition in the equipment market has contributed to falling profit margins for foreign companies and, in some areas, begun to eat into overseas investors' market share: [Surveys edition], London (UK).

Lee, M., (2012). Letter from The Honorable Fred Upton et al. to President Barack Obama [online]. Energy and Commerce Committee. Available from: https://republicans-energycommerce.house.gov/sites/republicans.energycommerce.house.gov/files/letters/20121011Cybersecurity.pdf

Leswing, K., (2018). The security community increasingly thinks a bombshell Bloomberg report on Chinese chip hacking could be bogus (AAPL) [online]. Available from: https://www.yahoo.com/lifestyle/security-community-increasingly-thinks-bombshell-133000590.html?guccounter=1

Lewis, T.G., 2014. CI protection in HS: defending a networked nation. John Wiley & Sons, 2nd edition. Ch.1 Origins of CI Protection

Lewis, T.G., 2019. CI protection in HS: defending a networked nation. John Wiley & Sons, 3rd edition. Ch.3 Theories of Catastrophe

Libicki, M.C., 2009. Cyberdeterrence and cyberwar. RAND Corporation.

Lieberman, J., 2012. Congressional Record Proceedings and Debates of the 112th Congress, Second Session [WWW Document]. URL https://www.congress.gov/112/crec/2012/07/26/CREC-2012-07-26-pt1-PgS5419-6.pdf (accessed 10.11.21).

Lindsay, J.R., 2020. Cyber conflict vs. Cyber Command: hidden dangers in the American military solution to a large-scale intelligence problem. Intelligence and National Security, pp.1-19.

Lindsay, J.R., Cheung, T.M. and Reveron, D.S. eds., 2015. China and cybersecurity: Espionage, strategy, and politics in the digital domain. Oxford University Press, USA.

Lippert, B., Perthes, V., Stiftung Wissenschaft Und Politik, 2020. Strategic rivalry between United States and China: causes, tragectories, and implications for Europe. SWP Research Paper. https://doi.org/10.18449/2020RP04

Lipton, G., 2018. The Elusive 'Better Deal' With China. [online] The Atlantic. Available at: https://www.theatlantic.com/international/archive/2018/08/china-trump-trade-united-states/567526

M. P. Fischerkeller and R. J. Harknett, "Persistent Engagement, Agreed Competition, and Cyberspace Interaction Dynamics and Escalation," The Cyber Defense Review, 2019.

Markusen, A.R., 2003. The case against privatizing national security. Governance, 16(4), pp.471-501.

Martin, L.L., Simmons, B.A., 1998. Theories and Empirical Studies of International Institutions. Int Org 52, 729–757. https://doi.org/10.1162/002081898550734

Mascitelli, B. and Chung, M., 2019. Hue and cry over Huawei: Cold war tensions, security threats or anti-competitive behaviour?. Research in Globalization, 1, p.100002.

Mattis, J., 2018. Summary of the 2018 National Defense Strategy of the United States of America. Department of Defense Washington United States. Online. Available at: https://dod.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf

May, P.J. and Jochim, A.E., 2013. Policy regime perspectives: Policies, politics, and governing. Policy Studies Journal, 41(3), pp.426-452.

May, P.J. and Koski, C., 2013. Addressing public risks: Extreme events and CI s. Review of Policy Research, 30(2), pp.139-159.

May, P.J., Jochim, A.E. and Sapotichne, J., 2011. Constructing HS: An anemic policy regime. Policy Studies Journal, 39(2), pp.285-307.

May, P.J., Koski, C. and Stramp, N., 2016. Issue expertise in policymaking. Journal of Public Policy, 36(2), pp.195-218.

McCaul, M., 2017. Rep. McCaul (R-TX). House of Representatives, Committee on Oversight and Government Reform H.R. 3359, the ''Cybersecurity and Infrastructure Security Agency Act of 2017.

McGraw, G. and Fick, N., 2011. Separating the Threat from the Hype: What Washington Needs to Know About Cyber Security. American's Cyber Future: Security and Prosperity in the Information Age Volumes I and II, Washington DC: Center for a New American Security.

McGregor, J., 2012. No ancient wisdom, no followers: The challenges of Chinese authoritarian capitalism. Easton Studio Press, LLC.

Mermoud, A., Keupp, M.M. and David, D.P., 2018, September. Governance Models Preferences for Security Information Sharing: An Institutional Economics Perspective for CI Protection. In International Conference on Critical Information Infrastructures Security (pp. 179-190). Springer, Cham.

Metcalfe, L., 1994. International policy co-ordination and public management reform. International review of administrative sciences, 60(2), pp.271-290.

Meyers, J., 2013. How the Convergence of IT and OT Enables Smart Grid Development 7.

Miller, G., Nakashima, E., Entous, A., 2017. Obama's secret struggle to punish Russia for Putin's election assault. Washington Post 6, 2017.

Miller, J. W. and Mauldin, W., (2016). U.S. Imposes 266% Duty on Some Chinese Steel Imports [online]. WSJ. Available from: https://www.wsj.com/articles/u-s-imposes-266-duty-on-some-chinese-steel-imports-1456878180

Ming, T., (2020). Understanding the New Great Power Competition [online]. Institute on Global Conflict and Cooperation. Available from: https://igcc.ucsd.edu/news-events/news/understanding-the-new-great-power-competition.html

Mintzberg, H., 1994. The rise and fall of strategic planning: reconceiving roles for planning, plans, planners. Free Press ; Maxwell Macmillan Canada, New York : Toronto.

Mitchell, B., (2019). Google's departure from Project Maven was a 'little bit of a canary in a coal mine' - FedScoop [online]. FedScoop. Available from: https://www.fedscoop.com/google-project-maven-canary-coal-mine/

Morgan, S.L., Winship, C., n.d. Counterfactuals and Causal Inference 526.

Moses, A., 2011. Fighting China's Golden Shield: Cisco sued over jailing and torture of dissidents. The Sydney Morning Herald, 16.

Moses, A., (2011). Fighting China's Golden Shield: Cisco sued over jailing and torture of dissidents [online]. The Sydney Morning Herald. Available from: https://www.smh.com.au/technology/fighting-chinas-golden-shield-cisco-sued-over-jailing-and-torture-of--dissidents-20110816-1ivkv.html

Moteff, J., 2015. Critical infrastructures: Background, policy, and implementation: RL30153.

Mueller & Farhat (2020). Energy Infrastructure and Industrial Data: Between Global Data Policies and an Evolving iIoT Environment. Strategic Energy Institute (SEI), Georgia Institute of Technology.

Mueller, M. and Tan, Z., 1997. China in the information age: Telecommunications and the dilemmas of reform (No. 169). Greenwood Publishing Group.

Mueller, M., 2020. ICANN OCTO Report on New IP. Internet Governance Project. URL https://www.internetgovernance.org/2020/10/29/icann-octo-report-on-new-ip/ (accessed 10.15.21).

Mueller, M., Cogburn, D.L., Mathiason, J. and Hofmann, J., 2007, November. Net neutrality as global principle for Internet governance. In GigaNet: Global Internet Governance Academic Network, Annual Symposium.

Mueller, M., Li, R., Sullivan, A., 2020. Do we need a new generation of data communication protocols?

Mueller, M.L. and Badiei, F., 2020. 3 Inventing Internet Governance: The Historical Trajectory of the Phenomenon and the Field. Researching Internet Governance: Methods, Frameworks, Futures, p.147.

Mueller, M.L., 2019. Against Sovereignty in Cyberspace. International Studies Review.

Mueller, M.L., Badiei, F., 2019. Requiem for a Dream: On Advancing Human Rights via Internet Architecture. Policy & Internet 11, 61–83. https://doi.org/10.1002/poi3.190

Mulligan, S. and Linebaugh, C., 2021. Huawei and U.S. Law. [online] Congressional Research Service. Available at: https://crsreports.congress.gov/product/pdf/R/R46693

Murray, G., Johnstone, M.N., Valli, C., 2017. The convergence of IT and OT in critical infrastructure. Australian Information Security Management Conference. https://doi.org/10.4225/75/5A84F7B595B4E

Musil, S., (2019). CIA reportedly says Huawei funded by Chinese state security [online]. CNET.. Available from: https://www.cnet.com/tech/services-and-software/cia-reportedly-says-huawei-funded-by-chinese-state-security/

National Institute for Standards and Technology (NIST), 2014. NISTIR 7628 Revision 1, Guidelines for Smart Grid Cybersecurity Volume 1, - Smart Grid Cybersecurity Strategy, Architecture, and High-Level Requirements Available at: https://dx.doi.org/10.6028/NIST.IR.7628r1

National Institute for Standards and Technology (NIST), 2014. NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 3.0. [online] Available at: https://www.nist.gov/news-events/news/2014/10/nist-releases-final-version-smart-grid-framework-update-30

Navari, C., 1989. The great illusion revisited: the international theory of Norman Angell. Review of International Studies, 15(4), pp.341-358.

NCCIC, 2016. GRIZZLY STEPPE – Russian Malicious Cyber Activity. Joint Analysis Report. [Online]. Available at: https://us-cert.cisa.gov/sites/default/files/publications/JAR_16-20296A_GRIZZLY%20STEPPE-2016-1229.pdf

North, D., 1990. Institutions, institutional change and economic performance Cambridge University Press. New York.

North, D.C., 1986. The new institutional economics. Journal of Institutional and Theoretical Economics, pp.142:230-37.

Nowlin, M.C., 2011. Theories of the policy process: State of the research and emerging trends. Policy Studies Journal, 39, pp.41-60.

Nye Jr, J.S., 2004. Soft power: The means to success in world politics. Public affairs.

Obama, B., 2015. Remarks by the President at the National Cybersecurity Communications Integration Center.

Odlyzko, A., 2019. Cybersecurity is not very important. Ubiquity, 2019(June), pp.1-23.

Office of the Chairman of the Joint Chiefs of Staff, DOD Dictionary of Military and Associated Terms, (Washington DC: The Joint Staff, July 12 2017), page 29. Available at: https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp1_ch1.pdf

Ogus, A.I., 2004. Regulation: Legal form and economic theory. Bloomsbury Publishing.

Olson, M., 1965. The logic of collective action, cambridge, mass. Harvard Univ. Pr.

Ostrom, E., 2005. Understanding institutional diversity, Princeton paperbacks. Princeton University Press, Princeton.

Otto, G., (2018). Coats: ODNI has seen 'no evidence' of supply chain hack detailed in Bloomberg story - CyberScoop [online]. CyberScoop. Available from: https://www.cyberscoop.com/dan-coats-bloomberg-supply-chain-the-big-hack/

Padilla, C., et al. 2018. National Security & International Trade. [online] Wita.org. Available at: https://www.wita.org/event-videos/national-security-international-trade/ .

Pai, A. (2018). Federal Communications Commission (FCC). Statement of FCC Chairman Ajit Pai On the Future of 5G Available at: https://www.fcc.gov/document/statement-fcc-chairman-ajit-pai-future-5g

Pan, C., 2021. British firm Arm says new chip tech could be licensed to Huawei, potentially easing the telecoms giant's supply chain woes. [online] South China Morning Post. Available at: https://www.scmp.com/tech/tech-trends/article/3127782/british-chip-design-firm-arm-takes-aim-intel-biggest-tech-overhaul

Parsons, C., 2007. How to map arguments in political science. Oxford university press.

Paul,. Ryan. 2010. Ars Technica. Researchers identify command servers behind Google attack

Pierson, P., 2000. Increasing returns, path dependence, and the study of politics. American political science review, pp.251-267.

Pollitt, C., 2003. Joined-up government: a survey. Political studies review, 1(1), pp.34-49.

Popper, K., 2005. The logic of scientific discovery. Routledge.

Porter, P., (2018). How the U.S. Foreign Policy Establishment Constrains American Grand Strategy [online]. Belfer Center for Science and International Affairs. Available from: https://www.belfercenter.org/publication/how-us-foreign-policy-establishment-constrains-american-grand-strategy

Presidential Policy Directive 8: National Preparedness [online]. (2011). Department of Homeland Security. Available from: https://www.dhs.gov/presidential-policy-directive-8-national-preparedness

President's Commission on Critical Infrastructure Protection, 1997. Critical Foundations: Protecting America's Infrastructures.

Radvanovsky, R.S. and McDougall, A., 2018. CI :Homeland Security and emergency preparedness. CRC Press.

Rausser, G. and Stevens, R., 2009. Public-private partnerships: goods and the structure of contracts. Annu. Rev. Resour. Econ., 1(1), pp.75-98

Reitman, W.R., 1964. Heuristic decision procedures, open constraints, and the structure of ill-defined problems. Human judgments and optimality, pp.282-315.

Resale International Telecommunications Authority Pursuant to Section 214 of the Communications Act of 1934. [online] fcc.gov Available at: https://docs.fcc.gov/public/attachments/DOC-357087A1.pdf

Reuters. 2011. Huawei backs away from 3Leaf acquisition. [online] Available at: https://www.reuters.com/article/us-huawei-3leaf/huawei-backs-away-from-3leaf-acquisition-idUSTRE71I38920110219

Review of Controls for Certain Emerging Technologies; A Proposed Rule by the Industry and Security Bureau, 83 FR 58201. November 19, 2018. https://www.federalregister.gov/documents/2018/11/19/2018-25221/review-of-controls-for-certain-emerging-technologies

Richard White, Randy George, Terrance Boult, and C. Edward Chow. “Apples to Apples: RAMCAP and Emerging Threats to Lifeline Infrastructure.”Homeland Security Affairs 12, Article 2 (September 2016). https://www.hsaj.org/articles/12012

Richardson, J.J., Bosma, J.T., Roosild, S. and Larriva, D., 1999. A review of the technology reinvestment project. Potomac Institute for Policy Studies.

Ridding, J. 1996, China's fledgling export base takes off: But Shenzen economic zone finds the future insecure, John Ridding writes: [London edition], London (UK).

Riedman, David. “Questioning the Criticality of CI : A Case Study Analysis.”Homeland Security Affairs 12, Essay 3 (May 2016). https://www.hsaj.org/articles/10578

Rittel, H.W. and Webber, M.M., 1973. 2.3 planning problems are wicked. Polity, 4(155), p.e169.

Roberts, P., 2014. Heartbleed: Technology Monoculture’s Second Act [Online]. The Security Ledger with Paul F. Roberts. Available at: https://securityledger.com/2014/04/heartbleed-technology-monocultures-second-act/

Roberts, P.S., 2005. Shifting priorities: Congressional incentives and theHomeland Security granting process. Review of Policy Research, 22(4), pp.437-449.

Robertson, J. & Riley, M. 2018, New Evidence of Hacked Supermicro Hardware Found in U.S. Telecom, New York. Available from: https://www.bloomberg.com/news/articles/2018-10-09/new-evidence-of-hacked-supermicro-hardware-found-in-u-s-telecom

Robertson, J. and Riley, M., 2018. New Evidence of Hacked Supermicro Hardware Found in U.S. Telecom. [online] Bloomberg.com. Available at:

Rogin, J., 2012. NSA Chief: Cybercrime Constitutes the “Greatest Transfer of Wealth in History. Foreign Policy, 9.

Ryan, P., (2010). Researchers identify command servers behind Google attack [online]. Ars Technica. Available from: https://arstechnica.com/information-technology/2010/01/researchers-identify-command-servers-behind-google-attack/
Paulson, H., 2015. Dealing with China. Hachette UK.

Rysavy, P., 2019. International economics and securing next-generation 5G wireless networks: A conversation with Amb. Robert Strayer. American Enterprise Institute - AEI. URL https://www.aei.org/events/international-economics-and-securing-next-generation-5g-wireless-networks-a-conversation-with-amb-robert-strayer/ (accessed 10.14.21).

Sabatier, P.A. and Weible, C.M. eds., 2014. Theories of the policy process. Westview Press.

Sabatier, P.A. and Weible, C.M., 2007. The advocacy coalition framework. Theories of the policy process, 2, pp.189-220.

Salazar, D., 2017. TRUST in the Supply Chain 25.

Salvatore, S.A., 2018. Fusion center challenges: why fusion centers have failed to meet intelligence sharing expectations 101.

Sanger, D.E., Perlroth, N., 2019. US escalates online attacks on Russia's power grid. The New York Times 15.

Schneier, B., 2009. Essays: Beyond Security Theater - Schneier on Security [Online]. Available at: https://www.schneier.com/essays/archives/2009/11/beyond_security_thea.html

Schneier, B., 2010. Essays: Threat of "Cyberwar" Has Been Hugely Hyped - Schneier on Security. [online] Schneier.com. Available at: https://www.schneier.com/essays/archives/2010/07/threat_of_cyberwar_h.html

Schwab, K., 2017. The fourth industrial revolution. Currency.

Scot Tanner, M., 2017. Beijing's New National Intelligence Law: From Defense to Offense. [online] Lawfare. Available at: https://www.lawfareblog.com/beijings-new-national-intelligence-law-defense-offense

Scott, W.R. and Davis, G.F., 2015. Ch.6 Technology and Structure. Organizations and organizing: Rational, natural and open systems perspectives., Routledge.

Semiconductor Industry Association (2020). 5G Wireless Infrastructure Semiconductor Analysis. Semiconductors.org. [online] Available form: https://www.semiconductors.org/wp-content/uploads/2020/07/SIA-5G-Report_2.pdf

Sens. Webb, Kyl: Sale of U.S. Computer Technology to Chinese Firm Poses 'Serious Risk' 2011, , Washington, D.C.

SGIP, 2010. Introduction to NISTIR 7628 Guidelines for Smart Grid Cyber Security.

Shahzad, A., Lee, M., Xiong, N., Jeong, G., Lee, Y.-K., Choi, J.-Y., Mahesar, A., Ahmad, I., 2016. A Secure, Intelligent, and Smart-Sensing Approach for Industrial System Automation and Transmission over Unsecured Wireless Networks. Sensors 16, 322. https://doi.org/10.3390/s16030322

Shane, S. and Lehren, A., 2010. Leaked Cables Offer Raw Look at U.S. Diplomacy. [online] Nytimes.com. Available at: https://www.nytimes.com/2010/11/29/world/29cables.html.

Shane, S. and Lehren, A. W., (2010). Leaked Cables Offer Raw Look at U.S. Diplomacy (Published 2010) [online]. The New York Times. Available from: https://www.nytimes.com/2010/11/29/world/29cables.html?_r=1&hp

Shepardson, D., Freifeld, K. and Alper, A., (2020). U.S. moves to cut Huawei off from global chip suppliers as China eyes retaliation [online]. Reuters.com. Available from: https://cn.reuters.com/article/us-usa-huawei-tech-exclusive-idINKBN22R1KC

Shilov, A., 2020. Chinese SMIC Tapes Out First N+1 ‘7 nm’ Chip, But Mass Production Uncertain. Tom's Hardware. Available at: https://www.tomshardware.com/news/chinese-smic-tapes-out-first-n-7-nm-chip-but-mass-production-uncertain

SIA, 2021. Reduce Burdens on the Export of Commercial Semiconductors [Online]. Semiconductor Industry Association. Available at: https://www.semiconductors.org/policies/export-control/

Simon, H.A., 1977. The structure of ill-structured problems. In Models of discovery (pp. 304-325). Springer, Dordrecht.

Sivan-Sevilla, I., 2019. Explaining Policy Change in Governing Digital Technology Risks.

Skopik, F., Settanni, G., Fiedler, R., 2016. A problem shared is a problem halved: A survey on the dimensions of collective cyber defense through security information sharing. Computers & Security 60, 154–176. https://doi.org/10.1016/j.cose.2016.04.003

Skorobogatov, S. and Woods, C., 2012, September. Breakthrough silicon scanning discovers backdoor in military chip. In International Workshop on Cryptographic Hardware and Embedded Systems (pp. 23-40). Springer, Berlin, Heidelberg.

Slayton, R., Clark-Ginsberg, A., 2018. Beyond regulatory capture: Coproducing expertise for critical infrastructure protection: Beyond regulatory capture. Regulation & Governance 12, 115–130. https://doi.org/10.1111/rego.12168

Sofield, R., 2021. Wiley Law Biographies. [online] Wiley.law. Available at: https://www.wiley.law/pp/bio-RickSofield.pdf

Strohmaier, E., Dongarra, J., 2019. The 54th edition, November 2019.

Subramanian, A., 2011. Chinese Mercantilism: The Long View. [online] PIIE. Available at: https://www.piie.com/commentary/op-eds/chinese-mercantilism-long-view

Swales, A., 1999. Open Modbus/TCP Specification.

Swanson, A., (2018). Trump Strikes Deal to Save China’s ZTE as North Korea Meeting Looms [online]. The New York Times. Available from: https://www.nytimes.com/2018/06/07/business/us-china-zte-deal.html

Taleb, N.N., 2007. The black swan: The impact of the highly improbable (Vol. 2). Random house.

The Economist, (2012). Put on hold [online]. The Economist. Available from: https://www.economist.com/business/2012/10/13/put-on-hold

The IP Commission Report [online]. (2013). Home - The National Bureau of Asian Research (NBR). Available from: https://www.nbr.org/wp-content/uploads/pdfs/publications/IP_Commission_Report.pdf

The White House, 1998. Presidential Decision Directive-63. Protecting America's CI s. https://fas.org/irp/offdocs/pdd/pdd-63.htm

The White House, Complete Cybersecurity Proposal, 2011, http://www.whitehouse.gov/sites/default/files/omb/ legislative/letters/law-enforcement-provisions-related-to-computer-security-full-bill.pdf. Cite: Eric Fisher CRS "Federal Laws Relating to Cybersecurity legislation"

Thomas, M.S. and McDonald, J.D., 2017. Power system SCADA and smart grids. CRC press.

Thomas, M.S., McDonald, J.D., 2017. Power system SCADA and smart grids. CRC press.

Top 500, The List., 2019. Blog. Available at: https://www.top500.org/lists/2019/11/

Tosun, J. and Lang, A., 2017. Policy integration: Mapping the different concepts. Policy Studies, 38(6), pp.553-570.

Turner, D., 2010. Prepared Testimony and Statement for the Record of Dean Turner Director, Global Intelligence Network, Symantec Security Response Symantec Corporation Hearing on Securing Critical Infrastructure in the Age of Stuxnet United States Senate Committee on Homeland Security And Governmental Affairs.

Tversky, A. and Kahneman, D., 1981. The framing of decisions and the psychology of choice. science, 211(4481), pp.453-458.

U.S. Government Accountability Office (GAO), High-Risk Series: An Update, GAO-07-310, January 2010.

U.S. Senate Committee on Homeland Security & Governmental Affairs, 2012. Lierberman, Collins, Rockefeller, Feinstein, Carper Offer Revised Legislation to Improve Security of Our most Critical Private-Sector Systems.

UNITED STATES. (1987). John S. McCain National Defense Authorization Act for fiscal year 2019: conference report. Washington, D.C., U.S. G.P.O. Available at: https://www.congress.gov/bill/116th-congress/senate-bill/1790/text

US-China Commission. 2018 Report To Congress of the U.S.-China Economic and Security Review Commission, p. 37. On Hundred Fifteenth Congress, Second Session. November 2018. Available at: https://www.uscc.gov/annual-report/2018-annual-report-congress

US-China Economic and Security Review Commission hearing titled “The Evolving US-China Trade and Investment Relationship” 2012. [online]. Available from: https://www.uscc.gov/hearings/hearing-evolving-us-china-trade-investment-relationship

Valeriano, B. and Maness, R.C., 2015. Cyber war versus cyber realities: Cyber conflict in the international system. Oxford University Press, USA.

Valeriano, B., Jensen, B.M., Maness, R.C., 2018. Cyber Strategy: The Evolving Character of Power and Coercion. Oxford University Press.

Van Hollen (2019). Senate Committee on Banking, Housing, and Urban Affairs Hearing on Export Control Reform Implementation: Outside Perspectives. First Session on Conducting Oversight On Implementation Of the Export Control Reform Act (ECRA). [online]. Available from: https://www.govinfo.gov/content/pkg/CHRG-116shrg39542/html/CHRG-116shrg39542.htm

Van Thiel, S., Verhoest, K., Bouckaert, G., Løegreid, P., 2012. Lessons and recommendations for the practice of agencification, in: Government Agencies. Springer, pp. 413–439.

Varas, A., Varadarajan, R., Goodrich, J. and Yinug, F., 2020. Government Incentives and US Competitiveness in Semiconductor Manufacturing. BCG Global, September, 9.

Verizon (2013). Breach Investigation Report [online]. [online] https://www.netsurion.com/. Available at: https://www.netsurion.com/eventtracker/media/eventtracker/files/collateral/verizon-data-breach-2013.pdf

Vijayan, J., 2010. Senators ramp up cyberwar rhetoric. [online] Computerworld. Available at: https://www.computerworld.com/article/2516720/senators-ramp-up-cyberwar-rhetoric.html

Von Bertalanffy, L., 2010. General Systems Theory. The Science of Synthesis: Exploring the Social Implications of General Systems Theory, 103.

Wang, F.L., 2017. The China order: Centralia, world empire, and the nature of Chinese power. Suny Press.

Wang, J.-W., 2012. Modeling cascading failures in complex networks based on radiate circle. Physica A: Statistical Mechanics and its Applications 391, 4004–4011.

Wang, J.-W., Rong, L.-L., 2009a. Edge-based-attack induced cascading failures on scale-free networks. Physica A: Statistical Mechanics and its Applications 388, 1731–1737.

Wang, J.-W., Rong, L.-L., 2009b. A model for cascading failures in scale-free networks with a breakdown probability. Physica A: Statistical Mechanics and its Applications 388, 1289–1298.

Wang, J.-W., Rong, L.-L., 2011. Robustness of the western United States power grid under edge attack strategies due to cascading failures. Safety science 49, 807–812.

Warner, M., 2018. A New Doctrine for Cyberwarfare & Information Operations. Center for New American Security. Available at: https://www.warner.senate.gov/public/index.cfm/2018/12/warner-calls-for-society)

White, R.H., Tai, A.J., Leach, D., Santmire, T.E. and Nash, M., 1995. The Economics of Commercial-Military Integration and Dual-Use Technology Investments. INSTITUTE FOR DEFENSE ANALYSES ALEXANDRIA VA.

Whitt, R.S., 2003. A Horizontal Leap Forward: Formulating a New Communications Public Policy Framwork Based on the Network Layers Model. Fed. Comm. LJ, 56, p.587.

Wildavsky, A., 1987. Choosing preferences by constructing institutions: A cultural theory of preference formation. American political science review, 81(1), pp.3-21.

Williamson, O.E., 1981. The economics of organization: The transaction cost approach. American journal of sociology, 87(3), pp.548-577.

Williamson, O.E., 1989. Transaction cost economics. Handbook of industrial organization, 1, pp.135-182.

Wise, R. and Baumgartner, P., 1999. Go downstream. Harvard business review, 77(5), pp.133-141.

Witt, A., (2020). Formalizing Team Telecom [online]. The National Law Review. Available from: https://www.natlawreview.com/article/formalizing-team-telecom

Wolf, K. J. (2017). Examining the Committee on Foreign Investment in the United States Hearing before the Committee on Banking, Housing, and Urban Affairs United States Senate.

Wolf., K. (2017) Foreign Investment and National Security A House Financial Services subcommittee. December 14, 2017. Available at: https://www.c-span.org/video/?438564-1/hearing-examines-national-security-implications-foreign-investment-us

Xinhua, 2017. The General Office of the CENTRAL Committee of the Communist Party of China (CPC) the General Office of the State Council issued the Action Plan for the Promotion of the Scale of the Sixth Edition of the Internet Protocol (IPv6) [WWW Document]. URL http://www.gov.cn/zhengce/2017-11/26/content_5242389.htm (accessed 9.24.21).

Yanaa Technologies LLC
https://ecfsapi.fcc.gov/file/1022666936593/Yaana_comments_18-89.pdf

Yin, R.K., 2017. Case study research and applications: Design and methods. Sage publications.

Zafar, R., 2021. SMIC Rumored To Have Achieved 95% 14 nm Chip Yield - But Industry Insiders Doubt The Claim. [online] Wccf (Where Consumers Come First) tech. Available at: https://wccftech.com/smic-rumored-to-have-achieved-95-14nm-chip-yield-but-industry-insiders-doubt-the-claim/