Illuminating the Black Box:

Determining American Response Frameworks to Chinese Cyberattacks

Senior Thesis

Submitted in Partial Fulfillment of the Bachelor of Arts in Public Policy Studies

Nikhil Josyula Manglik

The University of Chicago

Spring 2021

To my parents and family, who always supported me in exploring my interests, and continually encouraged me to excel at them.

To my professional mentors and my thesis preceptor, who awakened my interest in this field and guided me through the thesis writing process itself.

And finally, to all my friends, who served as sounding boards, proofreaders, advice manuals, and shoulders to cry on during this process.

Thank you.

Table of Contents

The rise of cyberspace as a domain for state-state interaction has led to the rise of a digital version of the age-old “security dilemma”. Under conditions of low information, states may stumble into escalatory behavior which leads to a conflict which grows out of control. This paper seeks to determine how the United States responds to Chinese cyberattacks by compiling a list of all responses from 2010-2021 and analyzing that dataset for themes. It finds that there are several compelling themes which sketch out a coherent foreign policy under which domestic concerns primarily drive US public responses. Finally, the paper then looks to the future, applying these lessons to President Biden to try and understand how US-China relations may change in the years to come.

Introduction

The advent of cyberspace has created a new problem for great-power relationships in the modern day. While the norms of military escalation are well known, the norms of cyberspace are not. This makes it all too easy for inadvertent escalation to occur – while the costs of engaging in military actions are well known, the valuation of targets of cyberattacks are not. This means that while states are able to effectively plan for the consequences of a military attack, they are unable to do so for cyberattacks. This has some real harms. First, the rise of cyberwarfare has created a space where other countries can challenge US primacy through asymmetric warfare. Second, it has created the possibility of an inadvertent cycle of escalation in cyberspace. In conventional warfare, the costs of doing business are clear. Because the valuation of different targets is clear, countries can calibrate their attack to the message they want to send, and can roughly prepare for the kind of response they will receive. The idea of what counts as a proportional response is clear to all sides, preventing unnecessary escalation. In cyberspace, by contrast, the valuation of different targets is unclear. It is plausible, for instance, to consider a world in which China engages in a cyberattack on a target they mistakenly presume the United States places little value in. This mistake forces the United States to respond at the level they consider proportionate to the damage done, which may provoke China. From here, it is easy to see how this process of reciprocal response can lead to an escalation, as both sides miscalibrate their responses due to a misunderstanding of the valuations of the other side. This process of miscalibration is exacerbated by the fact that neither side has publicly available information regarding the capabilities or indeed even the valuations of the other, due to a combination of cultural and strategic choices. Given this dynamic, my paper seeks to achieve the following. First, it seeks to develop an understanding of the idea of a cyber-conflict of escalation, which in turn it seeks to prove is plausible and dangerous in the US-China context. Second, it then seeks to tamp down the temperature on this cycle by creating a publicly-available taxonomy of likely US responses to Chinese aggression in order to provide that information and aid in future decision-making.

Background

Dating back to the “Century of Humiliation”, China has considered the United States and its Western allies to be exploitative monarchs, abusing their position as world hegemons to force their way upon the rest of the world. This perception has shifted with modern times as China grows into its own role as a great power, but the underlying Chinese perception of the United States as vastly stronger persists. In light of this, China has turned to the Internet as a space of potentially asymmetric warfare and espionage. In line with Deng Xiaoping’s strategy of *xinxi duikang*, or “information warfare”[1], China has steadily cultivated its cyberattack capabilities as a means of inflicting damage on the militarily far superior United States. In doing so, it has continued the legacy of Project 863, which improved Chinese technology through a deliberate, endorsed process of industrial espionage and reverse-engineering waged against US competitors[2].

Any analysis of Sino-American foreign policy must begin with an understanding of China’s overall foreign policy project. For the Chinese Communist Party, the central issue of Chinese foreign policy remains the aftermath of the “Century of Humiliation”, when technologically superior Western powers fought China and stripped it of its possessions in a series of unequal, humiliating treaties. In response, the Chinese government has staked its foreign policy legitimacy on rolling back the effects of the Century of Humiliation and restoring China to her presumed rightful place as world superpower[3]. In order to do so, Premier Deng Xiaoping formulated three major stages for Chinese foreign policy, crystallized in his maxim “hide your strength, bide your time”[4]. These three stages still drive Chinese foreign policy today. In the

[1] Inkster, “The Chinese Intelligence Agencies: Evolution and Empowerment in Cyberspace,” 42.
[2] Ibid. 34-35.
[3] Meyer-Fong, “How China’s History Shapes, and Warps, Its Policies Today.”
[4] Kamphausen, Hearing on “The Chinese View of Strategic Competition with the United States.”

first stage, Deng believed that China was too weak to stand up to Western superpowers effectively. In that time, China should hide, seeking to avoid confrontation and avoiding conflicts where it would almost certainly lose[5]. In the second step, China should attempt to join international institutions, gaining access to world powers and positioning itself as an integral part of the global order. This takes the form of joining international trade organizations, making alliances, and engaging in the international community, but without displaying any sign of wanting to dominate the international system[6]. In Deng's thinking, the goal of this stage would be to lull Western powers into a state of complacency and reliance on China, all while building up Chinese power for the third stage. This stage took the form of China seeking to join the World Trade Organization and throwing itself open for manufacturing[7]. At the same time, China steadily built its international institutional power by placing Chinese officials in high ranking international positions, by engaging poorer countries, and by steadily assuming leadership roles on international initiatives. Finally, the third stage of Deng's theory entails the reveal of Chinese power, using its built up advantage and the element of surprise to assert its dominance on the global stage and reclaim its place atop the global hierarchy. This stage was activated by Premier Xi Jinping, who proclaimed the 'transcendence' of the hide and bide philosophy in favor of asserting Chinese strength[8]. With its newfound power, Xi argues, China should begin to act as superpowers did.

Sponsored by Deng Xiaoping, Project 863 represented one aspect of this three stage approach to foreign policy. A critical component of the hide and bide philosophy was growing one's own capabilities to be deployed when the time was right. In order to do so, Deng endorsed the use of industrial and intellectual espionage, siphoning off the intellectual property of American firms in order to reverse engineer their accomplishments in China[9]. Over time, Project 863 was expanded, with China embarking on a more

[5] Friedberg, "Globalisation and Chinese Grand Strategy."
[6] Kamphausen, Hearing.
[7] Friedberg, "Globalisation".
[8] Kamphausen, Hearing.
[9] Inkster, "The Chinese Intelligence Agencies: Evolution and Empowerment in Cyberspace."

general program of espionage against the United States which was accelerated with the advent of the Internet and technology[10]. Indeed, since then, the program has evolved and mutated to fit the needs of the 21st century, morphing into a more general form of using the Internet and cybersecurity probes more specifically to advance Chinese foreign policy by weakening competitors in Chinese space.

China first uses hacking as a way to expand it capabilities by stealing United States military knowledge. It does so by hacking into US defense contractors. These contractors typically have access to sensitive information needed to fulfill contracts with various branches of the military; however, they may not have the robust cybersecurity protections the military has. These documents have several key points of interest for China. First, it reveals the architecture of the latest American military generation, shedding light on key US vulnerabilities and capabilities. This allows China to more effectively plan for a potential upcoming war with the United States, as it can accurately estimate the United States' true capabilities. Second, China still lags behind the United States in military power and innovation. By stealing information from contractors, China can gain access to cutting edge military technology, and can use it to expand their own capabilities as well.

China also uses hacking as a tool for state repression and domestic political ends. In addition to hacking for information, China is comfortable hacking Western companies in order to gain access to the details of dissidents or members of persecuted groups, or to punish Western companies for not toeing the Chinese party line. Indeed, it is these motivations that gave rise to Operation Aurora, the most prominent opening salvo of the US-China cyber relationship[11]. In that Operation, Google announced in 2010 that Chinese hackers linked to the PLA had broken into Google in 2009 seeking information related to dissident Ai Weiwei's Gmail account[12]. This caused a major international incident, as other companies revealed they had been broken into as well and made it clear that this was a large scale, wide ranging,

[10] Hannas, Mulvenon, and Puglisi, *Chinese Industrial Espionage*.
[11] "Connect the Dots on State-Sponsored Cyber Incidents - Operation Aurora."
[12] "The Chinese Dissident's 'Unknown Visitors.'"

targeted attack against the West[13] by Chinese state-affiliated hackers on behalf of the PRC[14]. In response, the US government denounced the attack and submitted a formal complaint to the Chinese government about the pattern of hacking and intellectual property theft it had observed[15].

After a continued series of irritants in the US-China relationship, including continued cyberattacks on American firms, Obama and Xi met in Southern California for a summit in 2015. As part of that summit, the two sides released a Memorandum of Understanding which addressed in part the US-China cyber relationship[16]. This Memorandum was the first time both sides had addressed the matter in a public, bilateral fashion, and as such remains a signpost moment for any analysis of US-China relationships. In it, the United States and China both recognized the costs of cyber-theft of intellectual property and pledged to work to prevent it. There were three main prongs to the agreement. First, the two sides agreed to honor requests to investigate cyber crimes originating in their own country, and to hold those responsible accountable[17]. This included informing the other country about investigation outcomes, but is limited by both sides' perceived domestic and international legal obligations[18]. While this clause should seem to break down the insoluble problem of state sponsored attacks, the inclusion of the domestic law clause means that the Chinese government can avoid prosecuting its hackers on the basis that no violations of domestic law occurred. Second, both sides agreed that they would work to stoBy p cyber theft in particular, and that neither government would knowingly support or engage in the theft of intellectual property[19]. This has been flagrantly violated by China, as the United States has filed numerous suits alleging that the Chinese government, acting through the People's Liberation Army, has continued with this practice apace. These lawsuits will be discussed in the rest of the thesis. Finally, the

[13] Nakashima, "Google China Cyberattack Part of Vast Espionage Campaign, Experts Say."
[14] Shane and Lehren, "Leaked Cables Offer Raw Look at U.S. Diplomacy (Published 2010)."
[15] Landler, "Clinton Urges Global Response to Internet Attacks (Published 2010)."
[16] "FACT SHEET."
[17] Ibid.
[18] Ibid.
[19] Ibid.

Memorandum called for the development of international standards regarding cyberspace, acknowledging the leading role both sides play in the development of such international norms[20]. In order to do so, both sides agreed to work with the United Nations, setting up a “Group of Governmental Experts” (GGE) which would report every two years on its findings. However, this GGE ultimately also failed, due to the differing values China and the United States wanted to have drive the Internet’s norms. While the United States placed a premium on freedom of expression and the free exchange of information, China viewed the Internet as an extension of sovereignty, and called for the right to restrict information flow in accordance with national laws[21].

While Obama era diplomacy was conducted under the premise that China should be brought into cooperation with the United States, the Trump Administration took a decidedly different tack. Unlike Obama, Trump came into office explicitly promising a hostile attitude towards China, who he viewed as a menace to American businesses. This took the form of a much more aggressive National Cyber Security Strategy which advocated for the concept of “defending forward”[22]. Under the doctrine of defending forward, the United States should not simply seek to prevent attacks by erecting defenses around sensitive targets. Rather, it should also seek to cut off capabilities at the source, including by engaging in preventative cyberattacks[23]. As an example of defending forward, United States Cyber Command was able to take Russian misinformation farms offline in the days leading up to the 2018 midterm elections[24]. The new focus on an aggressive cyber policy was complemented by more aggressive exposure and denunciation of Chinese malfeasance, which was further escalated after the COVID-19 pandemic originated in, and was covered up by, China.

[20] Ibid.

[21] “UN GGE on Cybersecurity.”

[22] “2018 DoD Cyber Strategy Summary.”

[23] “A Chinese Perspective on the Pentagon’s Cyber Strategy.”

[24] Borghard and Lonergan, “Cyber Operations as Imperfect Tools of Escalation,” 139.

The primary mechanism by which China has engaged in cyberattacks on the United States is through so-called Advanced Persistent Threats, or APTs. Different APTs are typically signaled by a number (eg, APT1, APT2, etc), or by some distinctive practice or naming scheme (eg, the “Elderwood” group was so named because of the commonality of that variable name in their exploits). These APTs, as defined by the Department of Justice, are groups of hackers distinguished by their use of techniques too sophisticated to have been independently developed[25]. In addition, they typically feature a military-esque command and control system designed to be able to focus on a target and ensure penetration[26]. These characteristics suggest that an APT, unlike ordinary collectives of hackers, are the beneficiaries of state sponsorship, and are acting at least partially according to the directives of an external state force. Notably, however, these APTs are not purely elements of the state, unlike an Army or an Air Force. Rather, they exist as a pseudo private entity, in a sort of “grey zone” between completely private and completely public forces. This provides the sponsoring nation state with a degree of plausible deniability, and provides the hackers with the freedom to pursue extracurricular projects designed to help raise money. For instance, several indicted Chinese APTs were caught hacking into military contractors for espionage as well as into credit card databases for identity theft, mixing pleasure with work. Moreover, these APTs are usually housed in China, far beyond the reach of the United States or its allies, allowing them to work with impunity.

The Sino-American relationship is the defining great-power relationship of the early 21st Century. As seen here, China is willing and able to push the limits of virtual great power interactions to claim its perceived ‘rightful’ place in the global hierarchy; conversely, the United States, as the reigning hegemon, can be expected to bitterly contest its potential usurpation. This conflict, when carrying such existential stakes, has the potential to boil over into unexpected, catastrophic consequences if not carefully managed through predictable state responses to provocation. By creating a systematic analysis of US foreign

[25] *US v Zhu and Zhang* at 2, Footnote 1.
[26] Ibid.

policy responses, we can hopefully make US responses more predictable, decreasing the chances of a catastrophic miscalculation of risk and a subsequent cycle of escalation.

Literature Review

The current logic of US cyberspace interaction is premised on the idea of “persistent engagement”[27]. By mutually probing each other’s boundaries through limited scale attacks and noting the response, China and the United States can mutually discover each other’s boundaries of acceptable conduct, creating a space of “acceptable action” and allowing for the risk of increased escalation to decrease. However, this delicate balance can be upset by a miscalculation of the other side’s boundaries both during and after the intelligence gathering process, creating a self-defeating spiral of escalation[28]. Thus, it is imperative that this bargaining process conclude quickly, so that both sides know the guardrails of acceptable conduct and do not stray outside them as soon as possible to avoid the risk of unnecessary conflict or escalation.

The genesis of escalation literature is Herman Kahn’s *On Escalation,* which recast escalation between great powers in light of nuclear competition[29]. Kahn theorized that escalation could be conceived of as a ladder, with countries “climbing” the ladder as they depart from prior zones of agreed upon conflict. These departures can be along two dimensions[30]. First, one can escalate by involving those previously thought to be off limits, for instance by targeting civilian installations or engaging in mass atrocities[31]. Second, one can escalate by taking actions beyond the pale of agreed incursion, as when the Soviet Union put missiles in Cuba, far closer than the United States was willing to countenance[32].

[27] Fischerkeller and Harknett, “Persistent Engagement, Agreed Competition, and Cyberspace Interaction Dynamics and Escalation.”
[28] Ibid.
[29] Kahn, *On Escalation*.
[30] Ibid.
[31] Ibid.
[32] Ibid.

The risk of escalation in cyberspace has been well considered in the literature on both theoretical and Sino-US grounds. In the literature, several academics have found that the Kahn model of escalation is broadly applicable to cyberspace, with some tweaks to account for the ultimately non-kinetic nature of combat in cyberspace and the fact that cyberspace is an inherently "gray zone" of conflict[33]. Writing in *Lawfare*, Ben Buchanan and Robert Williams found that the risk of escalation is likely, and that its development mirrors the "security dilemma" familiar to international relations in the physical world[34]. The security dilemma typically plays out as follows. Suppose Country A has a tense relationship with Country B, such that both fear an imminent attack by the other. In response to this fear, Country A builds up its military in order to defend against any possible attack by Country B. However, Country B is not privy to Country A's motivations and so believes that the reason for a military buildup must be in order to attack Country B. In response, Country B builds up its own military, provoking further alarm and buildup from Country A. Eventually, this cycle of fear may result in one side attempting a pre-emptive strike, at which point war would erupt.

Buchanan's insight is that this cycle can play out not just in the real world, but in cyberspace as well, with potentially even more devastating results[35]. In the real world, the risk of the security dilemma is limited to an arms buildup which can be touched off by a pre-emptive attack. While this is obviously non-ideal, the norms of physical conflict mean that the likely outcome is simply a buildup of military forces. In cyberspace, by contrast, both the United States and China ascribe to the philosophy of "defending forward"[36], a phrase which implies the use of pre-emptive cyber attacks to shut a potential threat down at the source. This has a much greater chance of escalating into violence than a buildup of troops, since an actual injury has been done. Consider a world in which the United States believes that China is likely to try and hack into election offices to try and affect the outcome of an election. Further suppose that

[33] Healey, "The Implications of Persistent (and Permanent) Engagement in Cyberspace."
[34] Buchanan and Williams, "A Deepening U.S.-China Cybersecurity Dilemma."
[35] Ibid.
[36] Lyu, "A Chinese Perspective on the Pentagon's Cyber Strategy."

the United States has isolated the group which they believe would carry out the attack, but that China in reality has no such plans. If the United States then engages in an attack against the group in question, believing it to be in defense, China will see the attack as a deeply problematic violation of its sovereignty, and will feel compelled to respond in kind. This could touch off a series of escalatory attacks in cyberspace, with potentially very real damages to both countries.

In this vein, a key risk factor for escalation would be a failure of a party to appreciate how risky the moves they make are[37]. These risks ultimately arise from the cognitive biases of policymakers, who fail to appreciate the differing motives and information of their counterparts in other countries. Some scholars believe that the United States under President Trump was already verging on this, with the constant contact model of "defending forward" providing for a far greater risk of unintentional engagement than the Administration was willing to acknowledge publicly or privately. This is the case made by Jason Healey in 2019, who argued that while the United States' broad policy made sense, a re-calculation of cyber policy to increasingly emphasize stability of cyberspace alongside the Trump doctrine of constant engagement[38]. Indeed, some scholars point to the Sino-US relationship as the most likely flashpoint for any sort of cyber conflict[39]. As such, some scholars have attempted to wargame the resultant conflict, and warn that the lack of information commonality between the two sides makes the Sino-US relationship the tinderbox of cyberspace[40]. This miscommunication is ultimately costly in the cyber realm, and is what this paper attempts to try and mitigate.

Some authors also argue that cyberspace is escalatory due to cyberwarfare's status as the new form of "total war" in the 21st century. In this telling, propagated by Cavaiola et al, cyberwarfare at high levels inevitably involves the attack of dual use systems critical to both military and civilian functioning[41]. At a

[37] Hansel, "Cyber-Attacks and Psychological IR Perspectives."
[38] Healey, "The Implications of Persistent (and Permanent) Engagement in Cyberspace."
[39] "Preparing the Cyber Battlefield."
[40] Ibid.
[41] Cavaiola, Gompert, and Libicki, "Cyber House Rules."

catastrophic level, this could include power outages or healthcare facilities; more mundanely, however, any cyberattack represents the exploitation of a vulnerability that leaves both military and civilian data drastically underprotected. In addition, the recent move towards considering private data a national security threat due to its potential for identity theft means that the exfiltration of citizen data can be considered both a useful geopolitical objective and a critical assault on civilians at the same time[42]. As a result, any cyberattack must be treated as an unknown. Specifically, it is unknown whether the attack was meant to target the military or civilians. Even under defending forward, the most permissive framework for attacks, an attack on civilians is wholly beyond the pale, and grounds for drastic action. Thus, the uncertainty about who the attack was targeted transmutes into a belief that the attack must have or could have targeted civilians, and as such demands a strong response. Further, in a tense environment, the words of the enemy might be considered unreliable, throwing fuel on the fire rather than diffusing it due to the plausible deniability inherent to any cyberattack.

Finally, in some cases a cyberattack can lead to escalation because of a lack of clarity. In the physical world, the costs of taking a certain military action are reasonably well known – an attack on a port might engender an attack on an airstrip, for instance -- and the costs of a proportional response are fairly clear. This is only true because both sides know how the other side values certain targets, however, because those targets have roughly the same value to both sides. This mitigates the risks associated with mirror imaging, as using one's own frame of reference instead of the opponent's leads to fundamentally similar results. The same is not true, however, of cyberattacks. Since cyberattacks are by their nature about the theft of information or the denial of access, that information is valued differently by different parties. This leads to accidental cycles of escalation, as the victim lashes back with an intensity that was unexpected by the initial party. Angered by the seemingly unprovoked escalation, the initial attacker responds forcefully, precipitating another response, and quickly leading to an inflammatory cycle of

[42] Cyber, "Proportional Response to Cyberattacks."

escalation[43]. This sort of miscalculation is one of the likeliest causes of escalation, and is a topic on which both traditional and cyber international relations theorists have written at length due to its salience and importance to any realist theory.

All of these risks fundamentally share the same root. Each of the risks of a cycle of escalation come down to miscommunication or faulty assumptions. By developing a framework for how attacks are responded to, the United States can cut down on the risk of said miscommunication, making cyber-engagements less likely to escalate since both sides know roughly what to expect. While there may be challenges related to the potential reveal of operational capacity, this paper will seek to develop a framework broad enough to avoid compromising any operational intelligence while specific enough to neutralize the costs of poor information.

Some authors do, however, reject the idea that cyberspace is inherently escalatory compared to the kinetic world[44]. For instance, Borghard and Lonergan write that because of their intelligence-heavy requirements and short time windows, it is hard for a country to effectively respond quickly to an unprovoked cyberattack, neutralizing the cycle of escalation at its source[45]. This could buy time for agencies to determine the extent of the attack, and for cooler heads to prevail once the parameters of the attack are known[46].

While these papers have developed a sophisticated understanding of the theory behind cyber escalation, there are very few papers trying to apply theories to the real world to see how governmental actors actually carry out cyber responses[47]. This paper aims to fill this gap, by trying to see how the American government responds to cyberattacks by a specific rising power, China, which has repeatedly demonstrated its ability and willingness to engage in cyberattacks at peer capability with the United

[43] Lin, “Escalation Dynamics and Conflict Termination in Cyberspace,” 52.
[44] “The Escalation Inversion and Other Oddities of Situational Cyber Stability.”
[45] Borghard and Lonergan, “Cyber Operations as Imperfect Tools of Escalation.”
[46] Ibid.
[47] Gorwa and Smeets, “Cyber Conflict in Political Science.”

States. In doing so, this paper hopes to apply some of the lessons of the literature to test how they stand up against real world escalations.

A key secondary part of theory-building is the potential temporal relevance of when responses are carried out. In particular, the regular and frequent nature of United States elections, as well as the transfer of power, means that the role of electoral politics and transfers of power in the determination of American foreign policy must be carefully considered.

One piece of information clearly explicated in the literature that can help with this theory exercise is the concept of the “rally around the flag” effect. Most commonly seen in discussions of kinetic warfare, the rally around the flag effect suggests that leaders who go to war or preside over a major tragedy see their approval ratings increase dramatically as the populace seeks to unify around a leader and in favor of quick, decisive action against the crisis. Thus, the literature suggests a real electoral benefit to decisive action, which would suggest an electoral benefit to highly public, aggressive responses to Chinese action in the leadup to an election. When focusing on China specifically, there is further evidence to suggest “tough on China” policies and ads do in fact result in a meaningful boost in electoral support in key swing states, most notably in the Rust Belt[48]. This would provide candidates with greater impulse to pick and publicize fights with China around election time, a key potential predictor in the dataset.

The other piece of theory building which is important is the extent to which foreign policy at the sub-decision maker level remains consistent across different administrations. Analytically, this would seem to be a non-issue since the people creating the “option set” of possible responses tend to be career civil servants who cross administrations. Indeed, the field of international relations makes little sense unless there is some sense that countries act with continued interests and behaviors even across leadership changes. However, a look at the literature to confirm this analytical presupposition is in order.

[48] Fang, “ANTI-CHINA RHETORIC, PRESIDENTIAL ELECTIONS AND U.S. FOREIGN POLICY TOWARDS CHINA.”

Buttressing this analytical supposition is a finding that in the determination of US foreign policy, voter preferences fall fairly low on the pendulum; most important instead are business leaders and civil service experts, both of whom will have relatively stable foreign policy preferences across governments[49]. This, combined with the typical finding that American voters do not care much about foreign policy as a rule[50], suggests that while Presidents may be sensitive to the electoral benefits of projecting strength, particularly on China, they do not then carry that consideration of the voters into their actual official work. Even if the voters desire a radical change in direction, they may or may not follow depending on the interests of other classes.

Methods

In order to effectively analyze US responses to a cyberattack, it is imperative that we determine what exactly qualifies as a cyberattack. This paper will propose the following three-part definition of a cyberattack:

(1) A subversion of defined critical infrastructure (as designated by the US Federal Government) designed to disrupt normal processing or produce results favorable to Chinese ends.

(2) A data breach revealing sensitive information which could be used for the purposes of Chinese geopolitics. While this definition is ill defined, two examples make it clear. The hack of the Office of Personnel and Management's data resulted in the theft of thousands of federal employees' medical data, information which could be of use to Chinese statecraft. By contrast, the theft of credit card information from Target or other stores is not meaningful, since the proximate reason and the danger in these attacks is in identity theft.

(3) Hacks of companies which serve as pillars of the American economy, with the end goal of transferring intellectual property to state affiliated Chinese companies. This is distinct from those

[49] Jacobs and Page, "Who Influences U.S. Foreign Policy?"
[50] Sutter, *The United States and Asia*.

companies conducting economic espionage themselves or from China's legendary forced partnerships acting as a pipeline for stolen IP – this represents using agents of covert state power to forcibly steal the crown jewels of American companies to better Chinese competitors. These attacks could also be political in nature, designed to punish companies for not bending to Chinese demands.

The justification for this definition flows from two key sources. First, it arises from the different kinds of incidents cited in the CFR Cyber Operations tracker[51]. It also tracks closely with stated United States priorities about what Chinese actions in cyberspace are considered unacceptable, as in the 2015 Memorandum of Understanding[52].

A key problem with analyzing any cyberattack is the problem of attribution. This paper sidesteps that issue by asserting the following: In order to respond to the actor of a cyberattack, the United States government needs to have identified to a reasonably high certainty who the actor in question is. As this paper only analyzes responses, it enters the response process after the attribution mechanism has finished. Notably, this does not mean the United States knows with full certainty who specifically carried out the cyberattack, simply that we sidestep the problem of international attribution specifically. Whoever carried out the cyberattack, we are confident they did so at the direction of the Chinese government. This is not an unreasonable assumption to hold: frequently, state-sponsored groups have a variety of "calling cards", including increased sophistication generally and country-specific tells, which allow analysts to quickly identify the country responsible, even if the identification of the individual actors takes longer to ascertain. For instance, analysts were able to quickly identify Russia as the primary source of the SolarWinds hack to a high degree of certainty within three days of the hack becoming public knowledge, even as they still worked to identify the primary group responsible.

[51] "Tracking State-Sponsored Cyberattacks Around the World."
[52] "FACT SHEET."

In order to create a taxonomy of US responses, however, we must use a set of case studies as our primary tool. While access to US governmental documents would be ideal, many of them are still classified, as this problem is extremely new. Instead, we will use case studies and broadly available public data. Using these case studies, we will attempt to tease out the particulars of how each attack was characterized in terms of scope, severity, and probable geopolitical goal, and in turn analyze the US response. By doing so, we hope to be able to determine what factors drive US decision making, and what issues force them to take greater action.

The cases used will span the Obama and Trump Administrations, and will involve a variety of severity levels for both incident and response. Cases were selected on the basis of time of incident, effective attribution to China as a state-involved attack, and publication of a response. Within those cases which remained, seventeen were chosen based on the availability of public information. In addition, two non-attack case studies were included due to the way in which they illuminate the United States' thinking on critical technological infrastructure and Chinese attacks.

As part of the analysis of these cases, the paper will seek to use sources explicating the United States' official position as far as possible. In some cases this will come through official statements, sometimes through reports of actions or unveiled indictments, and sometimes simply from public statements themselves. When analyzing these documents, the paper will choose to focus on determining the nature of the Chinese aggression, teasing out the specific characteristics, while attempting to characterize the nature of the United States response. By replicating this analysis over several cases, we hope to find correlates and patterns suggesting a coherent United States policy. Some possibilities include the nature of the attacked party (federal government, state government, local government, private company), the extent of damage done, the extent to which the response was publicized, the extent to which the response was acted upon, and the severity of the response itself.

Cases were selected through the CFR Cyber Operations Tracker, an independent database of cyberattacks published by the Council on Foreign Relations[53]. This database was chosen for its comprehensiveness, the ease with which it provided sources for more in-depth analysis, and the status of the database and CFR broadly as a leading source in the field. In order to provide a modicum of consistency, we chose to begin the analysis in 2010 with the Operation Aurora attack, commonly cited as the moment the United States government began taking cyberattacks seriously.

Starting in 2010, the dataset for this analysis was constructed by only looking at cases perpetrated by China against the United States (per CFR's own coding). Once all of these attacks were isolated from the database, each attack was checked for duplicates and against other news sources to ensure that further analysis could be undertaken. At this stage, each attack was also checked to ensure that its precipitating cyberattack fell under this paper's composite definition of a cyberattack, and those that did not were removed. This process led to a final tally of 17 cyberattacks across 11 years. These cyberattacks were then coded along a variety of axes, which will be discussed in further depth below.

First, every attack was coded with its month and year. In order to assign a date, we followed the CSIS convention and used the date of the United States' response to a cyberattack. This choice has a few major benefits for this project. Using the date of the United States' response provides a definite date for each attack, which would not be gained if we tried to determine the beginning of a cyberattack. In addition, there is frequently a time lag between when a cyberattack is discovered and the United States' response. As we are analyzing the United States' response to cyberattacks, focusing on the date of that response provides more useful information about the context of the response than the date of discovery, given that the two are frequently not the same. We chose to only use month and year to allow us to draw out some conclusions about the commonalities of each attack; including the specific date would have added little to the analysis at the cost of greatly increased complexity.

[53] "Tracking State-Sponsored Cyberattacks Around the World."

Second, we assigned each column an indicator describing the government response it caused. This indicator was not particularly coded, instead being a more straightforward kind of description which did not require or use any further categorizations. Nevertheless, the dataset did end up with an implicit coding scheme. If multiple actions were taken at the same time, they are individually noted (for instance, the 2018 Fujian Jinhua hack resulted both in an indictment and a ban on Fujian Jinhua accessing the US Market). If multiple actions were taken at times distinct from each other, as in the case of the OPM hack, the two events are coded separately. Thus, OPM Hack and OPM Hack-Ind. are considered two separate responses with two separate rows, despite sharing the same precipitating incident. This choice goes back to the focus on analyzing responses; when two responses are carried out separated by time, treating them as separate incidents allows us to analyze the factors that may have changed in the interim to warrant the addition of new action.

The next column sought to determine who was attacked, coding the type of groups affected as private, contractor, or government. This tripartite distinction arose naturally out of the groups affected, and was chosen to try and create a spectrum from fully non-governmental to fully governmental effects. In the case of widespread attacks which hit a variety of targets with a variety of kinds of coding, we chose to code the type of entity affected based on what most news coverage revolved around and a subjective feeling about what entities attacked were most "important" to the aim of the hack. In cases where it seemed like two different entities were equally important to the analysis, we decided to simply code both kinds of groups affected in service of completeness.

The next column tried to divine the purpose of the attack, again in broad categories. This was the first time that rather than a distinction naturally arising, the author chose how to define the categories which were part of the coding schema. As such, a description of that schema will be provided here.

The coding schema used has three major prongs, corresponding to the three major ways in which the Chinese Communist Party has used cyberattacks against American entities before. “Political” cyberattacks are those which the Communist Party undertook in the service of some domestic political end – this could be hacking into emails to find dissident communications, for instance, or hacking into news organizations’ servers to find their sources for critical reporting on China. These attacks bear no specific ill-will towards the United States; they just require breaking into American entities due to the ubiquity with which American services are used around the world. These are, on some level, the least damaging kind of attack to US interests.

“Trade Secrets” hacks refer to those which are undertaken in order to steal the intellectual property and trade secrets of American firms in China. This kind of hack has a long history in China, with variants of this intellectual property theft a common complaint of American businesses since the 1980s. These thefts of intellectual property are carried out by Chinese government affiliated groups as part of a broad government policy, with the benefits being funneled to Chinese companies to allow them to bypass the time cost of innovating new features or improvements to a product, in turn allowing them to provide a better product and compete in the global marketplace using American knowledge. In addition, when used against military contractors or companies working on sensitive projects, the theft of trade secrets can also provide critical information about the weaknesses of key points in the American system or in American weaponry. Thus, the theft of Trade Secrets can also have important national security implications, even if those are not the primary purpose of these hacks.

The final major code involved here is “Intel”. On its face, this appears to be the most serious violation, referring to those cases in which the primary purpose of the cyberattack in question is to gain access to sensitive US military or diplomatic intelligence. Typically, this is done by targeting contractors or the United States government in order to gain access to schema of upcoming next-generation weaponry, or to plans regarding US diplomatic endeavors. This access to secret product information, however, is qualitatively different from the national security implications of Trade Secret theft. The national security implications of Trade Secrets stem from the fact that economic security is national security under current American foreign policy doctrines, and from the risk that Chinese companies might overtake American companies in global marketplace supremacy. While private companies do supply components of Chinese military and national security apparatuses, and several state-owned enterprises do benefit from trade secrets, these national security implications ultimately stem from the risk of economic dominance. Intelligence thefts, by contrast, have as their primary concern the risk to national security from a hostile actor like China knowing about sensitive information. By stealing intelligence around next-generation weaponry, for instance, China will know the weaknesses of American weaponry and can develop ways to exploit those weaknesses. By stealing information on the United States' diplomatic priorities, China can tailor their approach to ensure that America is forced into negotiating from a position of strategic disadvantage wherever possible.

The next column attempts to determine how widespread the attack was, defining "widespread" to mean the number of different entities affected by the hack. If an attack seemed to focus only on one or two entities or a single industry, it was deemed targeted; if it implicated systemic issues (as in the OPM hack) or seemed to involve a broad array of companies across multiple industries, it was deemed widespread. At the same time, we try and code the industry in which the attack occurred in a separate column, if that attack seems to be confined to one industry. In cases where the target was a government entity or spanned multiple industries, we did not try and ascertain a particular industry, instead coding it as "N/A".

Next, we code two columns based on when the attack occurred to test the hypothesis that the United States political situation meaningfully affects US responses. The first column is fairly straightforward, merely noting the President at the time noted. The second column is a binary variable coding for whether or not the response happened in "election season", which we define to be within 12 months of the election, or up to the end of the year of the election. Thus, the election season for 2020 was Nov 2019 – Dec 2020. We begin the coding at 12 months prior due to the long US primary season, and the fact that media attention begins turning to the next election cycle twelve months before the election. Thus, any action taken then by political actors could have a political motivation beyond the simple policy benefits. We also keep the month after the election, because any policy action announced then would have been prepared during election season; thus, the decision to take and prepare that action would have been done in light of political pressures stemming from electoral concerns.

The next column codes the attacks based on the likelihood of future targets being engaged. This column's coding was ultimately up to researcher judgement. We chose not to do this based on the technological capabilities evinced in the attack for two reasons. First, technological exploits tend to operate on a use it or lose it basis – once a hack was uncovered and a patch released, that exploit would no longer be available. Second, even given the patching of exploits the PRC almost certainly has the cyber capabilities to overwhelm almost any entity who they seek to infiltrate. As a result, the question "Would China be able to hack into other entities on the evidence presented in this attack?" ceases to be a meaningful one. Instead, we chose to try and determine if other attacks were likely based on the motive of an attack. Based on coverage and official statements about each hack, we attempted to determine the overarching purpose of the attack. This purpose could be finding information about a specific innovation, probing for general information, or anything in between. Based on this, we tried to ascertain if the PRC would be incentivized to try and hack other entities in order to gain access to the information sought, or if the information at hand was located only in those entities which were hacked.

The final column simply seeks to determine if the threat actor responsible for the cyberattack had been positively identified. This goes beyond merely fingering China as the culprit – this seeks to determine if a specific hacker group or even individual can be ascertained to have been principally behind the hack. This is a binary variable – if yes, a specific actor has been identified; if no, they have not.

Limitations

The methodology and nature of this inquiry subject it to several limitations. We will discuss them in two sections: Concerns about data collection and concerns about the inquiry itself.

First, due to public access regulations this study elected to forgo the use of national security documents in favor of publicly available speeches and document releases. This means that while this paper can isolate speculative causes of different outcomes, we lack the ability to make definitive determinations about the deliberations which informed such policy decisions. However, this blindness is not total – in some cases, American officials have made their rationale or at least general stances public, allowing for a degree of informed speculation about the causes of their actions. In fact, the difficulty will not be in teasing out the rationale behind specific actions, but weaving those rationales into an overarching set of doctrines with few official guideposts to work from.

Second, the operative events in this timeline have only developed in the last ten years. While this means that there is direct relevance today, it means that events taking place in response are unlikely to be declassified, or may even still be ongoing. As a result, it may be difficult to find official, confirmatory information on items simply because they have not yet finished operation. This is another reason why official documents were foregone – it was simply unlikely that the Federal Government would have been willing to declassify the necessary documents given that they were at most ten years old and likely implicated operatives still working in the field, or methods still used today.

In addition to the concerns about data collection, there are specific concerns related to the nature of the inquiry itself. These will be discussed below.

First, there is a question of temporality which this paper has to address. In its current incarnation, the China-US relationship has only developed recently. Indeed, China was not popularly seen as a potential great-power threat to the United States until the Obama Administration. This is doubly true when considering American grievances around cyberattacks specifically, rather than the sorts of trade disputes that characterized Sino-US relations in prior Administrations. This means that while there are several incidents to draw from, they have all occurred in the last ten years, a limited time frame to analyze. This limited time frame also limits the information the government is willing to divulge about its counter operations, since many of them may still be active or involve people currently at risk.

Second, different Administrations will naturally have different approaches and positions regarding such a key geopolitical standard as the response to a cyberattack. In its analysis, this paper will straddle three Presidents. First, it will analyze the response to incidents under the Obama Administration as well as under the Trump Administration. Given their differing approaches to foreign policy, this poses a distinct problem of analysis. It is entirely plausible that Obama and Trump may have had different foreign policy response to the same problem. If that is true, then developing a historical analysis merging the two into one framework may be incoherent. The counterpoint is as follows. While the President has the final say on foreign policy, he does not have the only say. United States foreign policy is still largely driven by career officials in the State Department and intelligence agencies. These officials do not turn over with Administrations, but are dedicated civil servants with terms and expertise which cross many administrations. This backbone of institutional knowledge likely remained largely the same between Obama and Trump, and likely shaped the options presented to them. The only difference between the two Administrations, then, is which option the President elected to take, rather than the options themselves. This means that even if the final outcome may have been radically different, and while the two Administrations may have had distinctly different orientations to China at the top level, the options for response presented to both Presidents was likely similar. Without access to internal documents, however, it will be difficult to ascertain what the other presented options were. This would make it difficult to know that there truly is an overarching, trans-Presidential framework, and what the characteristics of that framework would look like for certain.

Third, this paper is released at the dawn of the Biden Administration, which may have an entirely different approach to China than his predecessors. This is doubly true given the way in which China has been politicized in recent American discourse, as well as the belligerent behavior of President Trump compared to the more diplomacy-oriented approach of President Joe Biden. This is worrying because this paper is meant in part to be prognosticative. If a key driver of instability in cyberspace is not knowing how countries will react, then illuminating the United States' decision structure may help tamp down that uncertainty and prevent situations from escalating. However, it is difficult to tell if Biden will use the same framework as his foreign policy predecessors, blunting the predictive power of this paper a little. Early indications suggest that he will indeed follow the rough foreign policy framework of the Obama Administration, with his Foreign Policy hires generally having extensive senior experience in that Administration. However, this is a concern that must be taken into account.

Analysis

In order to show how this coding plays out at the micro-level, we provide a preliminary analysis here. This preliminary analysis consists of two cases which serve as representative examples of the cases in the dataset. The first case serves as a representative example of trade secret cases ending in indictments, by far the most common variant in the dataset. The second case, in which the Trump Administration closed the Chinese Consulate in Houston over claims of research and IP theft related to the COVID 19 pandemic, represents a more wide-ranging attack with uncertain attribution and a quickly-developing timeline. In this case, we chose the Houston consulate closure due to the extremity of the US response and the interesting questions it raised in analysis. We provide the analysis of these two examples below. We present here a preliminary analysis to provide a sense for how the analysis will play out in the final product. This analysis will consist of analyses for two cases.

In 2018, the United States Department of Justice unveiled an indictment in the Southern District of New York. The case was titled *United States v. Zhu Hua and Zhang Shilong*[54]. The indictment charged Zhu and Zhang with hacking into American corporations, stealing both personal and espionage related data[55]. The two were charged as the principal members of APT10, which engaged in hacking behavior across the globe. In doing so, they especially targeted American defense firms, seeking to gain access to a number of technologies. They did this in a number of ways. First, APT10 hacked into defense contractors with weak cybersecurity protections, and tried to lift technology blueprints directly. In doing so, the Justice Department charges, APT10 attempted to break into over 45 organizations, both public and private, across 12 states in order to steal hundreds of gigabytes of sensitive technological data[56]. The explicit goal of this phase, according to the Justice Department, was to gain access to cutting-edge technologies developed in the United States for free, and provide them to China to facilitate its own technological advancements[57].

The second stage, the United States charged, involved Zhu and Zhang hacking into a so-called Managed Service Provider (MSP) and installing malware. Managed Service Providers effectively serve as a contracted out information technology team, responsible for handling software installation and occasionally cybersecurity defenses for a company[58]. Thus, by infiltrating MSPs and installing malware, the Justice Department claimed, APT10 was able to effectively infiltrate every single one of the MSP's clients at the same time[59]. The goal of this stage was to install keyloggers and illicitly obtain user credentials in these key organizations[60]. Having gained access to the system, the Justice Department

[54] *US v Zhu and Zhang*.

[55] "Two Chinese Hackers Associated With the Ministry of State Security Charged with Global Computer Intrusion Campaigns Targeting Intellectual Property and Confidential Business Information."

[56] *US v Zhu and Zhang*.

[57] "Two Chinese Hackers Associated With the Ministry of State Security Charged with Global Computer Intrusion Campaigns Targeting Intellectual Property and Confidential Business Information."

[58] *US v Zhu and Zhang*.

[59] Ibid.

[60] Ibid.

argues, APT10 was able to move laterally within the MSP's networks, which were frequently connected with the target's networks for maintenance purposes[61]. By moving through the network, APT10 was able to continuously infect new machines, looking for information of interest[62]. Once such information was identified, APT10 also undertook sophisticated tactics to package and exfiltrate the data to pre-registered domains, modifying their tactics as needed in the face of increasing American alarm[63]. Ultimately, the Justice Department claimed, APT10 was able to infiltrate everything from global financial companies to technology companies to the United States Navy using this tactic, stealing everything from sensitive personal information to highly classified technical documents depending on what was found[64].

The Justice Department further characterized APT10 as a Chinese entity. They noted that APT10 seemed to be based in Tianjin, China, and that the hackers seemed to work during Chinese working hours[65]. Through unrevealed work, the Justice Department also isolated that the hackers were working as part of a corporate environment, and that they were working at the behest of the Tianjing State Security Bureau, an official organ of the People's Republic of China. This was bolstered by the Justice Department's estimation that the tools in question were highly sophisticated, and by the nature of the organizations that were attacked in APT10's campaigns[66]. Notably, however, Zhu and Zhang were both still located in China, and the Justice Department conceded that both were likely to remain there. Instead, the indictment ought to be viewed as a so-called "speaking indictment": These are indictments that go beyond the scope necessary for an indictment, and indeed may not expect any legal outcome. Instead, the indictment is filed as a protective measure, meant to inform China about the United States' awareness of the attack and their assignation of blame. In addition, it provides a means for the

[61] Ibid.
[62] Ibid.
[63] Ibid.
[64] "Two Chinese Hackers Associated With the Ministry of State Security Charged with Global Computer Intrusion Campaigns Targeting Intellectual Property and Confidential Business Information."
[65] *US v Zhu and Zhang*.
[66] *US v Zhu and Zhang*.

government to talk openly about the attack, providing companies with a notification and allowing them to take the necessary precautions to protect themselves from future attacks conducted this way.

In the Zhu and Zhang analysis, there are a few factors which are important to consider in the analysis. First, the Zhu and Zhang analysis shows how difficult it can be to differentiate between privately acting and publicly acting groups. In this case, APT10 was engaged both in hacks for identity theft and in sensitive espionage, even as it is clear they were partially directed by Beijing. This partial responsibility makes it difficult to put sole responsibility on Beijing and take actions which harm the PRC, since there is ample plausible deniability to claim that APT10 was acting on their own initiative in cases rather than on instruction. Note, however, that this is distinct from problems with attribution. It is clear that APT10 conducted the attacks, and that they did so at the urging of the Chinese government. It is less clear, however, whether a given attack was conducted for business on behalf of the Chinese government, or personally, or whether the two were commingled. Thus, for any given attack it is important to acknowledge the difficulty of disentangling private engagements from state-backed ones, even if the United States knows to a high degree of certainty that China ordered at least some of the attacks. Policymakers must consider not just whether there is a high degree of certainty about the identity of the attacker or whether an attack was sponsored by China, but a high degree of certainty about the intent as well. This lack of certainty may have been a reason why the United States government elected to bring a personal indictment against Zhu and Zhang, rather than by taking aim at the broader Chinese government.

Second, the Zhu and Zhang indictment makes it plain how difficult it can be to go after decision-makers in enterprises such as APT10. In actuality, both Zhu and Zhang were fairly low-level employees – one was a penetration tester and one developed and tested malware[67]. Neither were, as far as the United States government revealed in its indictment, particularly important to the process of selecting or even

[67] Ibid.

overseeing targets. Their exposure meant that the United States could definitively tie them to interactions with United States adjacent actions, however, meeting the standing necessary to try them in American courts. This insulation enjoyed by the decision-makers of groups such as APT10 makes it a challenge to attack them directly, but indictments such as these can chip away at the pool of labor which works for them.

Third, the reason action may have been taken at all is because the attacks also impacted the United States government. As revealed by the Department of Justice, NASA and the United States Navy were both caught up in the dragnet of information theft[68]. This act of aggression against the United States government specifically, rather than merely private industry, likely motivated the United States to take a harder stance, especially once the national security implications of stealing the personal information of active servicemen are considered.

Fundamentally, however, the Zhu and Zhang indictment concerns the theft of information. While the information is sensitive and has real national security implications, the fact of the matter is very few of the pieces of stolen information could not be worked around. Technology can be redesigned; identity theft protections be engaged. The low impact nature of these violations in the context of the greater US-China trade relationship might mean that the United States did not consider this a big enough problem to take greater action on.

Finally, the Zhu and Zhang case showcases how long the timeline of these responses can be. According to the Department of Justice's filings, the Technology Theft campaign was started in 2006, while the MSP theft campaign began in 2014. The case was brought in 2018. This four year layover indicates that it is possible for responses to happen in a delayed reaction, as the necessary evidence is compiled and a decision is ultimately taken. While on the one hand this blunts the impact of the punishment, it signals

[68] "Two Chinese Hackers Associated With the Ministry of State Security Charged with Global Computer Intrusion Campaigns Targeting Intellectual Property and Confidential Business Information."

the thoroughness of the investigations and provides an explanation for why the United States may not declassify its documents or provide public notice of its response at the time of an attack. The public acknowledgement of an attack and public reveal of its punishment can happen years apart, as here.

The second example we seek to analyze is that of the Houston consulate closure in July 2020. This response poses interesting questions when placed in comparison with the response of the Zhu and Zhang indictment, which we will explore here.

The nucleus of the events leading up to the closure of the Houston consulate is the United States' claims of repeated biomedical research theft by the Chinese government coordinated through their Houston location. Per the Department of Justice in a briefing, the Houston consulate served as the nexus of a wide-reaching program of visa fraud and intellectual theft from research institutions in the United States, with the purposes of sending that information back to China[69]. This was coupled with accusations that the Houston consulate in specific had been promoting a program of biomedical research theft from the numerous institutions around Houston[70].

When considered in comparison to the indictment above, a few things become clear. First, the Houston response is much more severe than the Zhu and Zhang indictment, despite the far reaching potential implications of the APT10 hacks. One possible distinction to draw here is that unlike the indictment, the incidents leading to the Houston closure had a direct, immediate impact on national security. Happening in the middle of summer 2020, the Houston disclosures of information theft had heightened significance in the context of the COVID-19 pandemic and particularly in the context of the race to a vaccine, which the Trump Administration had made clear it viewed as a national security issue vis a vis China[71]. Whichever country came up with the vaccine first was likely to be able to distribute it fastest, with all the

[69] "Briefing With Senior U.S. Government Officials On the Closure of the Chinese Consulate in Houston, Texas."
[70] Ibid.
[71] "China's Houston Consulate Closure Linked to Covid-19 Research, Says US Official."

national security implications that entails. Thus, China stealing biomedical information from one of the largest research hubs in the United States in the middle of the race to a vaccine may have been considered an immediate ongoing national security threat that had to be rectified[72]. By contrast, many of the worst potential impacts of the APT10 hacks could be worked around, as the technology in question had not necessarily been put into production yet; as a result, the technology could be redesigned if necessary. At any rate, the United States was not in any armed conflict opposing China, preventing any immediate costs from China having that information other than the risk that they might come closer to attaining military parity.

The Houston consulate closure may have been more severe than the Zhu indictment due to the more direct state involvement as well. In the Zhu indictment, China maintained a degree of plausible deniability regarding the activities of APT10 due to their status as effectively a contractor and the way in which personal tasks were mixed with state defined ones. In the Houston case, however, the fact that the operations in question were coordinated and run through the Chinese consulate provided strong, nearly incontrovertible evidence that China knew and directed the program of visa fraud and biomedical theft. As discussed above, the uncertainty of whether or not China was behind a given attack is a key part of any response consideration; in this case, the obvious proof that it was allowed for a more direct punishment aimed at the Chinese state itself.

Finally, while it is possible to theorize foreign policy justifications for why the response in one case may be harsher than in others, the answer may be as simple as domestic political concerns. As an election year, 2020 provided powerful political incentives for the President to appear tough on America's enemies for his own political gain. For President Trump, this was compounded by his prior rhetoric, which had consistently painted China as an enemy and which blamed China for the spread of the coronavirus to the

[72] Shinkman, "Houston Consulate Closure Deterred China, But Not Before It Meddled With Vaccine Efforts: U.S. Intel Sources."

United States' shores. Announcing the discovery of a major campaign of theft and shutting down the consulate for one of America's biggest competitors could have proved an enticing option for President Trump politically, compared to more understated solutions. In addition to the President's personal political concerns, 2020 featured a far more bipartisan consensus on the fact that China represented a competitor to the United States than even 2018; the harsher response could simply be a reflection of the straining of ties between China and the United States since then.

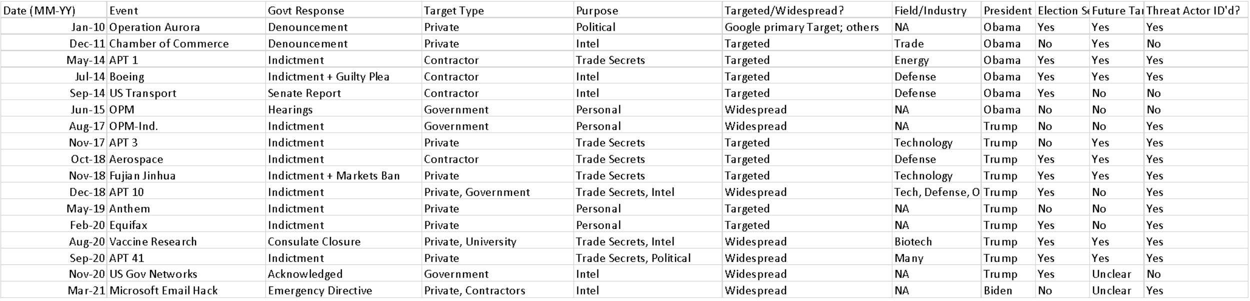
Interestingly, the closure of the Houston consulate prompted a response from China, who closed the American consulate in Chengdu in response. While this is an expected response to a consulate closure, there are a few factors that make it interesting. First, the Chengdu consulate is the base for America's pro-Tibet and pro-Xinjiang actions[73]. Closing the American consulate thereby achieves the domestic political aim of stifling critiques of the CCP's actions in both areas[74]. Second, the fact that China responded at all suggests that it understood the severity of the action and was taking retaliatory responses. Indeed, evidence suggests that the closure of the Houston consulate did end Chinese interference with US COVID efforts, although it is unclear if this was voluntary or due to a lack of capability[75]. This marks a difference from prior indictments, which were generally met with at most a press release. The retaliation certainly means that Beijing took note of this action; the question is whether it means that they are entering a new phase of responding to, and potentially directly challenging, American responses. If so, it could mean that the risks of a cycle of escalation will go up as China feels more comfortable directly challenging the United States.

[73] Fifield, Morello, and Nakashima, "China Tells U.S. to Shut Consulate in Chengdu, in Retaliation for Houston Closure."

[74] Ibid.

[75] Shinkman, "Houston Consulate Closure Deterred China, But Not Before It Meddled With Vaccine Efforts: U.S. Intel Sources."

The creation of this dataset resulted in a set of seventeen cases which prompted a US response over a period of about eleven years. The data of these responses is provided below (Figure 1).



Date (MM-YY)	Event	Govt Response	Target Type	Purpose	Targeted/Widespread?	Field/Industry	President	Election Se	Future Tar	Threat Actor ID'd?
Jan-10	Operation Aurora	Denouncement	Private	Political	Google primary Target; others	NA	Obama	Yes	Yes	Yes
Dec-11	Chamber of Commerce	Denouncement	Private	Intel	Targeted	Trade	Obama	No	Yes	No
May-14	APT 1	Indictment	Contractor	Trade Secrets	Targeted	Energy	Obama	Yes	Yes	Yes
Jul-14	Boeing	Indictment + Guilty Plea	Contractor	Intel	Targeted	Defense	Obama	Yes	Yes	Yes
Sep-14	US Transport	Senate Report	Contractor	Intel	Targeted	Defense	Obama	Yes	No	No
Jun-15	OPM	Hearings	Government	Personal	Widespread	NA	Obama	No	No	No
Aug-17	OPM-Ind.	Indictment	Government	Personal	Widespread	NA	Trump	No	No	Yes
Nov-17	APT 3	Indictment	Private	Trade Secrets	Targeted	Technology	Trump	No	Yes	Yes
Oct-18	Aerospace	Indictment	Contractor	Trade Secrets	Targeted	Defense	Trump	Yes	Yes	Yes
Nov-18	Fujian Jinhua	Indictment + Markets Ban	Private	Trade Secrets	Targeted	Technology	Trump	Yes	Yes	Yes
Dec-18	APT 10	Indictment	Private, Government	Trade Secrets, Intel	Widespread	Tech, Defense, O	Trump	Yes	No	Yes
May-19	Anthem	Indictment	Private	Personal	Targeted	NA	Trump	No	No	Yes
Feb-20	Equifax	Indictment	Private	Personal	Targeted	NA	Trump	Yes	No	Yes
Aug-20	Vaccine Research	Consulate Closure	Private, University	Trade Secrets, Intel	Widespread	Biotech	Trump	Yes	Yes	Yes
Sep-20	APT 41	Indictment	Private	Trade Secrets, Political	Widespread	Many	Trump	Yes	Yes	Yes
Nov-20	US Gov Networks	Acknowledged	Government	Intel	Widespread	NA	Trump	Yes	Unclear	No
Mar-21	Microsoft Email Hack	Emergency Directive	Private, Contractors	Intel	Widespread	NA	Biden	No	Unclear	Yes

Figure 1. Dataset of Cyberattacks and US Responses.

From this dataset, we will go column by column, showing that there are indeed discernable patterns of US engagement within the broader information in the dataset.

The first major class of findings relate to the timing of responses to cyberattacks. By analyzing the timing of cyberattacks, we find three major key findings. First, we find that America tends to hold off on responses when working under a diplomatic framework with China. Second, we find that American responses tend to tick up drastically around election season. Finally, we find that the frequency and intensity of response to cyberattacks has gone up over time, both between presidential administrations and within them.

The first finding comes from looking at the gaps in when enforcement or response actions are reported and matching them up with events outside the dataset. In doing so, we find three major gaps when few enforcement actions were taken. The first gap falls from 2011 to 2014, when there were no enforcement actions taken at all. However, during this time the Obama Administration was determined to pursue engagement with China, repeatedly making diplomatic overtures culminating in a 2013 “shirt sleeves summit" in Sunnyside, CA between the two leaders. Once this diplomacy failed, however, the United States returned to its nascent policy of response, unleashing a barrage of responses to prior Chinese incursions as a signal of its seriousness. The second gap falls from June 2015 – August 2017, a period of two years with no response actions taken. This coincides with the conclusion and operation of the 2015 Memorandum of Understanding between Obama and Xi, a framework which sought to resolve disputes around cyberspace by coming to a set of common understandings about the norms and issues of cyber conduct. This Memorandum sought to cap the issue of cyberspace infringements, with both sides referring to the Memorandum as a near-binding piece of work in their public messaging through 2016. The Memorandum had not conclusively failed until 2017, when the Group of Governmental Experts convened under the Memorandum's auspices were unable to come to an agreement about the norms and principles which should underlie the Internet. Finally, the third gap falls from December 2018 to August 2020, when only one enforcement action was taken. This corresponds to the time during and immediately after Trump's trade deal with China was confirmed, representing another diplomatic breakthrough with China. In all three cases, the United States waited until options for diplomacy were exhausted, and for proof that the previously agreed agreements were no longer in force, before agreeing to resume carrying out responses against cyberattacks in an extra-diplomatic way. This failure to achieve diplomatic frameworks seems to be the first level of US response, overriding any other considerations. It is important to note, however, that the lack of a public response when the United States has recently concluded diplomatic talks with China does not imply the lack of any response whatsoever, but merely the lack of a public response.

The second finding comes from the way in which election season interacts with highly public responses to Chinese cyberattacks. Under both the Obama and Trump administrations, the frequency of US responses to cyberattacks ticked up dramatically around elections, with relatively few incidents in between. In fact, the only time in which an election did not coincide with an uptick in responses was

2016, when the United States was still working under the diplomatic framework established by the Memorandum of Understanding. In general, we find from this dataset that a full 11 out of 17, or 64% of responses were carried out during an election season. This is despite the fact that over time, Chinese aggression has remained relatively constant per CSIS, and that election seasons only account for about half of the time elapsed in the dataset. There are potential reasons for this: the electoral benefits of seeming to take a strong stance against hostile actors means that American presidents may be more willing to engage in highly public acts of retribution around election time, where in other times they seek more damaging responses which cannot be disclosed to the public. In addition, the role of China as a rising power has been present in all of the elections in this dataset, most notably in 2020. This framing of China as a nascent threat might also induce politicians to appear "tough on China" through the authorization of highly public, politically favorable action.

Finally, in general the dataset seems to note a trend towards increasing action over time. This trend reveals itself both in the number and kinds of actions taken by the United States against China. First, the number of actions taken per year has gone up. For instance, despite only accounting for four years of the time elapsed in the dataset, President Trump accounts for an astonishing ten cases in the dataset, or 58.8% of all cases. At a more granular level, 2020 represented the most responses per year, with four. While these sorts of high intensity years are still interspersed with low intensity years (for instance, 2019 only had one response noted), the overall average number of responses per two year period has been going up steadily throughout the model except when interrupted by the cessation of responses during the period when the Memorandum of Understanding was understood to be in force. This suggests a continuing pattern of increasing tensions between the United States and China. This escalation extends to the type of responses used by the United States as well as the frequency of responses. In the Obama Administration, American foreign policy consistently strove to find areas of common understanding with China, and tried to provide incentives for the Chinese government to normalize to the West's conception of what a free and open Internet should look like. In addition, the Obama Administration was far more reluctant to take strong action on China than the Trump Administration. This was visible both in the large gaps in between and the types of enforcement actions taken by Obama to respond to instances of Chinese aggression. Especially in the beginning of his term, Obama frequently chose to try and alter Chinese action through public statements of disapproval, the weakest form of international pressure applicable by an American leader. Further, the only uses of internal responses happened under the Obama Administration, which chose to focus more on American security failings than on punishing Chinese malfeasance in certain intelligence related cases. In contrast, the Trump Administration took a much more confrontational stance towards China, which showed up as an increased willingness to deploy indictments and even consulate closures, combined with far more bellicose public addresses by high-ranking officials including the Secretary of State and Director of the FBI.

The next column to uncover is the role of attack type in determining American responses to a given Chinese cyberattack. Under the framing of this paper, China largely pursues four major types of cyberattacks – those meant to buttress domestic political ends (herein “Political” attacks), those meant to steal intellectual property and trade secrets from American firms (herein “Trade Secrets” attacks), those meant to gain valuable intelligence on United States military capability and planning (herein “Intel” attacks), and those meant to gain sensitive information on Americans and government workers for the purposes of blackmail (herein “Personal” attacks). Curiously, the United States does not seem to react very strongly to Political attacks. These attacks seemingly tend to be concentrated during times when the Chinese Communist Party faces some internal threat to its stability or rule, and tend to only involve American companies tangentially insofar as they are required for the suppression of internal dissent. This lack of direct malicious intent to American companies may help explain why the United States is less willing to engage directly with Political cases, preferring to engage in denunciation or even studiously avoiding the situation without a response.

In contrast to Political attacks, intelligence and trade secrets cases tend to provoke strong reactions to the attack by American policymakers. These two types of hacks tend to go together – hacks of military contractors, for instance, provide both key intelligence and trade secrets benefits, benefitting both Chinese contractors and the government. This connection has become more obvious in recent years, as many cases coded as Trade Secrets involved the likely loss of valuable intelligence on American military or security vulnerabilities. In addition, there seems to be a distinction within Intelligence hacks between those done for diplomatic benefit (such as the 2011 Chamber of Commerce hack) and those done for military benefit (such as the 2014 Boeing hack). Intel cases show the biggest point of divergence between the Obama and Trump Administrations. Of the three Intel cases Obama responded to, two of the responses were domestic efforts led by Congress in the form of hearings, and the third resulted in a public denouncement. By contrast, of the three cases involving Intelligence which Trump responded to, two resulted in indictments and the third resulted in an acknowledgement of the hack. This use of indictments assigns real consequences to the perpetrators of the attack and acts as a powerful diplomatic signal to China of the unacceptability of these actions. Both Administrations did treat Trade Secrets cases seriously, however, an unsurprising development given the continuous concern of business. Both Administrations frequently levied indictments against those thought to be stealing trade secrets from American companies in an attempt to dissuade such behavior.

Finally, Personal cases reached their crescendo under the Trump Administration, and as such their response tells us much about the way in which the Trump Administration specifically tries to address problems related to Chinese hacking. The only Personal hack the Obama Administration faced was the OPM hack, which resulted in a public hearing and nothing more. Under the Trump Administration, however, the OPM hack was revisited, and those responsible were indicted under US charges. This pattern of indictments continued with later personal hacks China executed under President Trump.

Another key pattern which bears noting is the kind of company targeted. Notably, and perhaps surprisingly, hacks which target the government make up a surprisingly small portion of the hacks that are responded to. Instead, the majority of hacks which the government publicly responds to concerns hacks on private companies. This discrepancy makes sense – the ways in which the government responds to government hacks are likely to be highly secret functions of diplomacy or of counter-striking which would be made unavailable to the public on the grounds of national security. With public companies, by contrast, the information is already public and the government's obligation is to ensure a public response. This public response allows other companies to learn about the vulnerabilities they could face, and allows for the government to publicly warn China and her companies of the costs of infringing on intellectual property. Contractors live in a middle space – their work tends to be highly classified in nature, but the government does lean towards a public response to put both the wider business community and China on notice.

This impulse towards allowing companies to protect themselves also explains the patterns seen in the Targeted/Widespread column, which suggests that the United States is far more open about what occurred when it appears to have happened to specific companies. When an attack is widespread, the nature of US response tends to be more focused on broader lessons learned, through venues such as a Senate Hearing or a Consulate Closure. These responses also tend to be more damaging than an indictment, as they provide a full accounting of China's role as a specific nation-state, rather than narrowly focusing on (albeit Chinese nationals) individuals within China as those primarily responsible.

The final, and perhaps most reasonable, factor in determining how an American response plays out is the simple fact of whether or not the specific actor behind a given attack can be isolated. This is a crucial prerequisite to being able to levy indictments, by far the United States' most favored tool when dealing with Chinese cyberattacks. In cases where the actor cannot be identified, the United States defaults to using hearings and general acknowledgements where possible, as these responses do not require a specific entity be targeted to be effective.

Policy Implications and Conclusions

The US approach to China has clearly changed many times over the course of the 21st Century. In its current incarnation, however, the United States faces the task of engaging with a peer competitor who is willing to engage in asymmetric cyer-attacks as a means of chipping away at the United States' technological, military, and geopolitical advantages. At the same time, however, the old Cold War paradigm of complete opposition to an enemy state fails in the face of global problems which require Sino-American cooperation. In addition, there are both domestic constraints and impulses towards a forceful response to China in the American business and political communities. The American response to cyberattacks is borne from these contradictions, and reflects an attempt to marry the competing incentives of American policymakers with the geopolitical imperatives of response to a rising competitor to form a coherent foreign policy. This policy is ultimately one focused on the domestic front, with the United States's responses dictated more by internal concerns rather than by external foreign policy or national security objectives.

The American response frameworks outlined here have real implications for President Biden's responses to China. Based on these frameworks, the hope is that this paper will be able to effectively predict how President Biden would respond to a given cyberattack, and what considerations the United States as an institution takes into account when formulating a response. From his remarks, we can glean that President Biden will be more hawkish on China than President Obama but less so than President Trump; we can also discern from his general statements that he intends to use international alliances and national power to punish China for its malfeasance in cyberspace.

In general, the United States' hierarchy for decision making around Chinese responses appears to look something like the following decision-making tree (Figure 2). In this flowchart, arrows to the left indicate an affirmative response "Yes"; arrows to the right indicate a negative response "No" to the question posed above. If multiple questions are placed side by side, they should be evaluated in a left to right order in the following way. If the left-most question has a positive answer, then carry out the instruction. If it does not, then carry out the negative instruction and refer back to the next question, following its instructions as well.

There are two pieces to how this decision-making tree was constructed. First, this paper had to consider the actual decisions that resulted from a given factor, which could easily be confused by the numerous other factors at play with any given case. Second, it had to consider the order of the decision-making hierarchy: clearly some factors were more important than others in the decision-making process, and it was imperative to determine the order of importance of these factors to arrive at an accurate model of United States decision-making.

This flowchart was designed by comparing different combinations of factors present in the data to see what diplomatic actions occurred in response. The rise of a given variable in this analysis is determined by the frequency of its correlation with a given outcome. From this process, we were able to tease out a set of principles which governed US responses by putting different combinations of factors in conflict to isolate meaningful differences. Indeed, by contrasting these differing outcomes and determining what factor differences caused them, we could then determine by implication what factors play a key role in the determination of specific outcomes. The important implication of this is the ability to effectively generate response option sets dependent only on one or a few factors, simplifying the tree-making process considerably.

The order of importance is modelled in this flowchart by the order of the linear decision tree, which most accurately mimics the way human decision-making works. To determine this ordering, a more macro-level view was required, in which different factors seemed to most consistently dominate other decisions in a hierarchy. For instance, in every time period where the United States was negotiating diplomatically with China, no retaliatory actions were recorded; in every time period where that was not true, the United States recorded retaliations. This was true regardless of any other variable, suggesting that the state of diplomatic negotiations with China is the first, most important factor considered in determining whether to respond or not. This process was performed recursively, removing the most important factor and determining the newly most important factor as the next level in the tree.

The final tree was then placed through a sanity check which asked whether the outlined process contained a legible through-line doctrine. In this case, it did – the doctrine proposed states that the United States retains a preference to engage China diplomatically if possible. Beyond that, the United States government seemingly places domestic considerations at the forefront of response considerations, with political concerns and the risk of other public attacks coming before national security implications of attacks in determining whether a public response will be carried out. This doctrine may seem bleak – in its telling, the United States will act first and foremost as a self-interested party, with petty domestic considerations placed at a higher level than the actual effects of the hack. However, it does provide a consistent, internally coherent account of the incentives that the United States government responds to.

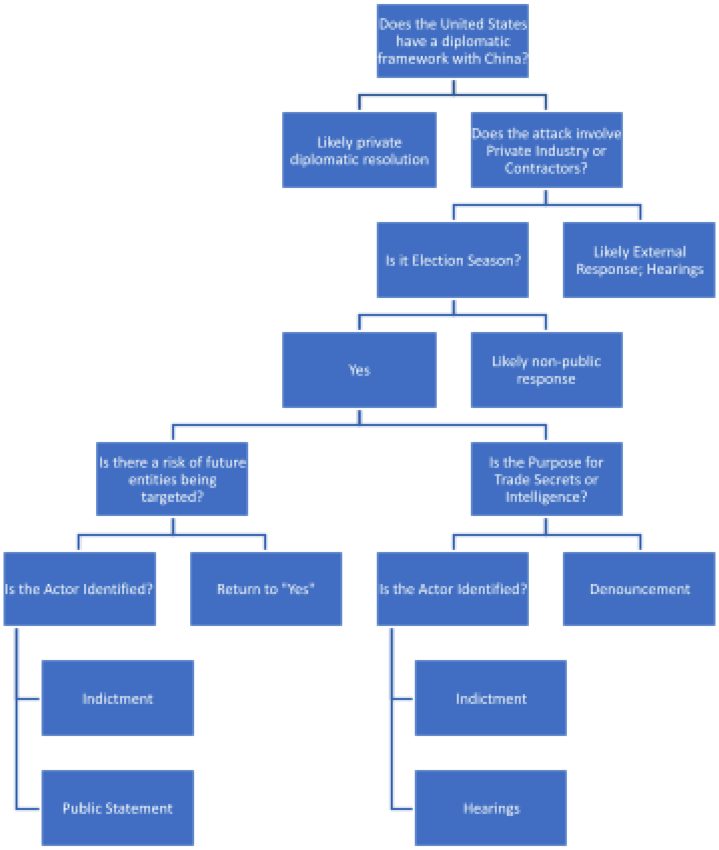

Does the United States have a diplomatic framework with China?
Likely private diplomatic resolution
Does the attack involve Private Industry or Contractors?
Is it Election Season?
Likely External Response; Hearings
Yes
Likely non-public response
Is there a risk of future entities being targeted?
Is the Purpose for Trade Secrets or Intelligence?
Is the Actor Identified?
Return to "Yes"
Is the Actor Identified?
Denouncement
Indictment
Public Statement
Indictment
Hearings

Figure 2. A flowchart depicting the rough decision-making process for American responses gleaned from this analysis. In general, this suggests that in order, diplomatic, domestic, and then national security considerations drive the decision making process.

From his statements, we see that President Biden does consider cyberattacks to be a serious threat, and that he does consider China to be a threat to the United States-led international order. In addition, President Biden has frequently touted his willingness to rely on the established procedures of Washington, instead of acting on the fly. Thus, we can reasonably conclude that if this is indeed the established operational procedure of United States foreign policy broadly, then it is likely that President Biden does subscribe to some form of this ideology.

From a *New York Times* report, it appears that President Biden does take the issue of cybersecurity seriously. In a first of its kind move, Biden elevated cybersecurity issues to the National Security Council, creating a deputy national security advisor specifically for cyber and emerging technologies[76]. Indeed, in its response to the Microsoft hack of March 2021, we can see some of how the Biden Administration plans to carry out its cyber policy vis a vis China. While the response is still in process at the time of writing, the evidence suggests that Biden will broadly follow the contours of established US decision making, while remaining more hawkish on the issue of China and cyberattacks more broadly than his predecessors.

In a sign of the increased primacy of cyber security in national security doctrines, the *New York Times* reports that the first major piece of business the Administration's national security staff is focusing on is how to harden American networks and deter future cyberattacks in the mold of past Chinese attacks or the Russian sponsored SolarWinds hack which compromised numerous federal systems in 2021[77].

If President Biden does follow these decision making processes, what does it mean for China and for America going forward? Biden has made no bones of the fact that he considers China a competitor to the US, frequently referring to it as a rising power which must be contained. However, he also openly believes that the Chinese state is a valuable partner in certain global challenges, including global warming and potentially the elevated risk of cyber hostilities.

For this theoretical exercise, we begin with an analysis of how Biden's evident foreign policy doctrine differs from that of his predecessors. First and foremost, Biden has made cybersecurity a core part of the National Security Council, naming a deputy National Security Advisor on cyber and emerging technologies. While this may be unsurprising, it does point to the Biden Administration placing a higher emphasis on cybersecurity to match their recognition of cyber as a pre-eminent issue in both the military

[76] Sanger, Barnes, and Perlroth, "Preparing for Retaliation Against Russia, U.S. Confronts Hacking by China."
[77] Ibid.

and national security spaces. Second, per New York Times reporting the Biden Administration has set cyber hardening and deterrence as its first priority, especially in light of the Microsoft and SolarWinds hack[78]. This is in part due to the vagaries of events around the Administration; however, it does also speak to a broader concern of National Security Advisor Jake Sullivan, who has consistently named cyber among the top threats facing America in the coming decade. As part of this impulse, the Biden Administration has extended a Trump-era memo giving United States Cyber Command authorization to engage in a wide range of cyber hostilities without Presidential authorization; while Biden has reportedly shrunk the scope of this memo, suggesting that he does desire a greater degree of oversight, this suggests that he does see cyberspace as a significant warfighting domain and wishes to preserve Cyber Command's response capabilities as far as possible. Notably, this restriction means that while CYBERCOM is able to engage in sub-hostilities retiliatory strikes and skirmishes in the grey zone of cyberspace, any meaningful response to major cyberattacks by China would require the approval of President Biden and his foreign policy advisors, putting the decision in the hands of this decision making tree. These changes run the risk of irritating China, who has denounced these changes as liable to further derail the project of cyber peace. Finally, Biden has expressed a desire to work more closely with traditional American allies in Europe and Southeast Asia to curb the rise of China through containment, expressing the view that this was not a project America could effectively take on alone due to China's position in the global order.

Despite all this, Biden does seem to broadly follow the contours of American foreign policy vis a vis China, even as he gives the issue of cybersecurity specifically broader pre-eminence. Much of his efforts, however, represent a turning away from the lack of nuance which characterized the Trump Administration, even as he maintains the focus on China as a pre-eminent threat which shaped much of Trump's interaction with China.

[78] Ibid.

This balancing act begins with Biden recognizing that in some cases, China does serve a valuable role as a partner to the United States. On global issues such as global warming and international money crimes, Biden does recognize the central role China must play in any suitable resolution due simply to their status as a pre-eminent global power engaged in explosive growth. Thus, while Biden does recognize areas of friction in the Sino-US relationship, unlike Trump he does not preclude the possibility of engagement on areas of mutual benefit in his calculation. In terms of the decision making process outlined above, this recognition of areas of mutual benefit means that it is likely that Biden will at least try to conclude some kind of understanding or agreement with China in his term so as to avoid unnecessary conflict when dealing with issues of global importance; if this comes to pass, a provision focusing on cyber issues would not be surprising given the way cyberspace has evolved to be a key flashpoint in US-China relations. Indeed, this is largely the same path that the 2015 Memorandum of Understanding under President Obama took, with cyber issues folded into a larger set of understandings that were meant to serve as the bedrock of a new understanding between Presidents Obama and Xi. This path becomes more likely if, as seems to be the case, Biden lets Cyber Command impose real costs on the Chinese government for their malfeasance, demonstrating the costs of a lawless cyber sphere and driving the Chinese to the table for negotiations.

While Biden has stated his willingness to work with China on areas of common ground, however, he has been careful to note that the Biden Administration will treat cyberattacks harshly. In a Twitter video posted in the aftermath of the revelation of the SolarWinds hack, then-President-Elect Biden said that "cyberattacks must be treated as a serious threat by our leadership at the highest levels.[79]" In that statement, Biden went on to note that a core part of doing so was naming those responsible for a cyber attack, shaming them publicly for it, and imposing costs on them that would provide real consequences for their misbehavior. This suggests that Biden does consider cyberattacks the hallmark of a bad actor in

[79] @JoeBiden on Twitter, 23 Dec 2020

the international arena, and has little patience for working with those who would rely on them to harm American interests. In the statement, Biden continued to extol the virtue of official attributions as a core part of defending American interests, along with retaliation if warranted. This statement in one minute suggests Biden's overarching framework: engage in diplomacy as a key way to check cyberattacks through the power of international engagement, while reserving the right to use targeted forms of retaliation to continue to ensure that attacking American interests cannot be hand waved away as a fundamentally riskless endeavor.

In general, Biden's approach to the problem of Chinese cyberattacks will be far less dedicated to blunt force instruments than Trump's approach was, and will be far more interested in using surgical strikes to impose like for like costs which hopefully deter China from considering future action. These actions would, in theory, provide visible costs to the Chinese regime, even as their classified nature makes them more secretive and invisible to the American people. In sum, Biden's foreign policy can be summarized as focusing on diplomacy and areas of common ground, but preferring to use more specific responses which impose more consistent, cumulative costs for bad faith behavior in cyberspace. In doing so, a Biden foreign policy would be far more willing to engage a broader policy toolkit than the one suggested in this flowchart; without recognition, he is willing to step outside of the public arena.

Bibliography

"2018 Department of Defense Cyber Strategy Summary," n.d. https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF.

Barnes, Julian E. "U.S. Accuses Hackers of Trying to Steal Coronavirus Vaccine Data for China." *The New York Times*, July 21, 2020, sec. U.S. https://www.nytimes.com/2020/07/21/us/politics/china-hacking-coronavirus-vaccine.html.

Benner, Katie. "Chinese Intelligence Officers Accused of Stealing Aerospace Secrets." *The New York Times*, October 31, 2018, sec. U.S. https://www.nytimes.com/2018/10/30/us/politics/justice-department-china-espionage.html.

———. "Chinese Officer Is Extradited to U.S. to Face Charges of Economic Espionage." *The New York Times*, October 10, 2018, sec. U.S. https://www.nytimes.com/2018/10/10/us/politics/china-spy-espionage-arrest.html.

———. "U.S. Army Reservist Is Accused of Spying for China." *The New York Times*, September 26, 2018, sec. U.S. https://www.nytimes.com/2018/09/25/us/politics/ji-chaoqun-china-spy.html.

———. "U.S. Charges Chinese Military Officers in 2017 Equifax Hacking." *The New York Times*, February 10, 2020, sec. U.S. https://www.nytimes.com/2020/02/10/us/politics/equifax-hack-china.html.

Benner, Katie, and Nicole Perlroth. "China-Backed Hackers Broke Into 100 Firms and Agencies, U.S. Says." *The New York Times*, September 16, 2020, sec. U.S. https://www.nytimes.com/2020/09/16/us/politics/china-hackers.html.

Borghard, Erica D, and Shawn W Lonergan. "Cyber Operations as Imperfect Tools of Escalation." *Strategic Studies Quarterly*, no. Fall 2019 (n.d.): 122–39.

United States Department of State. "Briefing With Assistant Secretary for East Asian and Pacific Affairs David R. Stilwell and Acting Director of the Office of Foreign Missions Clifton C. Seagroves On Actions Taken to Counter PRC Influence Operations." Accessed March 13, 2021. https://2017-2021.state.gov/briefing-with-assistant-secretary-for-east-asian-and-pacific-affairs-david-r-stilwell-and-acting-director-of-the-office-of-foreign-missions-clifton-c-seagroves-on-actions-taken-to-counter-prc-i/.

United States Department of State. "Briefing With Senior U.S. Government Officials On the Closure of the Chinese Consulate in Houston, Texas." Accessed December 11, 2020. https://www.state.gov/briefing-with-senior-u-s-government-officials-on-the-closure-of-the-chinese-consulate-in-houston-texas/.

Buchanan, Ben, and Robert D. Williams. "A Deepening U.S.-China Cybersecurity Dilemma." Lawfare, October 24, 2018. https://www.lawfareblog.com/deepening-us-china-cybersecurity-dilemma.

Cavaiola, Lawrence J., David C. Gompert, and Martin Libicki. "Cyber House Rules: On War, Retaliation and Escalation." *Survival* 57, no. 1 (January 2, 2015): 81–104. https://doi.org/10.1080/00396338.2015.1008300.

France 24. "China's Houston Consulate Closure Linked to Covid-19 Research, Says US Official," July 24, 2020. https://www.france24.com/en/20200724-china-s-houston-consulate-closure-linked-to-covid-19-research-says-us-official.

"Chinese Military Personnel Charged with Computer Fraud, Economic Espionage and Wire Fraud for Hacking into Credit Reporting Agency Equifax," February 10, 2020.

https://www.justice.gov/opa/pr/chinese-military-personnel-charged-computer-fraud-economic-espionage-and-wire-fraud-hacking.

U.S. Embassy & Consulates in China. “Communist China and the Free World’s Future,” July 24, 2020. https://china.usembassy-china.org.cn/communist-china-and-the-free-worlds-future/.

Council on Foreign Relations. “Connect the Dots on State-Sponsored Cyber Incidents - Operation Aurora.” Accessed December 11, 2020. https://www.cfr.org/cyber-operations/operation-aurora.

Cyber, Intelligence. “Proportional Response to Cyberattacks.” Accessed December 11, 2020. https://www.academia.edu/36264880/Proportional_Response_to_Cyberattacks.

whitehouse.gov. “FACT SHEET: President Xi Jinping’s State Visit to the United States,” September 25, 2015. https://obamawhitehouse.archives.gov/the-press-office/2015/09/25/fact-sheet-president-xi-jinpings-state-visit-united-states.

Fang, Xiaodong. “ANTI-CHINA RHETORIC, PRESIDENTIAL ELECTIONS AND U.S. FOREIGN POLICY TOWARDS CHINA.” Thesis, Georgetown University, 2016. https://repository.library.georgetown.edu/handle/10822/1041835.

Fifield, Anna, Carol Morello, and Ellen Nakashima. “China Tells U.S. to Shut Consulate in Chengdu, in Retaliation for Houston Closure.” *Washington Post*. Accessed December 11, 2020. https://www.washingtonpost.com/world/asia_pacific/china-tells-us-to-shut-consulate-in-chengdu-in-retaliation-for-houston-order/2020/07/24/839108d0-cd62-11ea-99b0-8426e26d203b_story.html.

Fischerkeller, Michael P., and Richard J. Harknett. “Persistent Engagement, Agreed Competition, and Cyberspace Interaction Dynamics and Escalation.” *The Cyber Defense Review*, 2019, 267–87.

U.S. Office of Personnel Management. “Freedom of Information Act.” Accessed March 13, 2021. https://www.opm.gov/information-management/freedom-of-information-act/#url=Cyber-Security-Records.

Friedberg, Aaron L. “Globalisation and Chinese Grand Strategy.” *Survival* 60, no. 1 (January 2, 2018): 7–40. https://doi.org/10.1080/00396338.2018.1427362.

Fruhlinger, Josh. “The OPM Hack Explained: Bad Security Practices Meet China’s Captain America.” CSO Online, February 12, 2020. https://www.csoonline.com/article/3318238/the-opm-hack-explained-bad-security-practices-meet-chinas-captain-america.html.

Gorwa, Robert, and Max Smeets. “Cyber Conflict in Political Science: A Review of Methods and Literature.” Preprint. SocArXiv, July 25, 2019. https://doi.org/10.31235/osf.io/fc6sg.

Graff, G. “The Problem Problem and Other Oddities of Academic Discourse.” *Arts and Humanities in Higher Education* 1, no. 1 (June 1, 2002): 27–42. https://doi.org/10.1177/1474022202001001003.

Hannas, William C., James C. Mulvenon, and Anna B. Puglisi. *Chinese Industrial Espionage: Technology Acquisition and Military Modernization*. Asian Security Studies. London ; New York: Routledge, 2013.

Hansel, Mischa. “Cyber-Attacks and Psychological IR Perspectives: Explaining Misperceptions and Escalation Risks.” *Journal of International Relations and Development* 21, no. 3 (July 1, 2018): 523–51. https://doi.org/10.1057/s41268-016-0075-8.

Harold, Scott Warren, Martin C. Libicki, and Astrid Stuth Cevallos. “The ‘Cyber Problem’ in U.S.-China Relations.” In *Getting to Yes with China in Cyberspace*, 1–16. RAND Corporation, 2016. https://www.jstor.org/stable/10.7249/j.ctt1cx3vfr.6.

Healey, Jason. “The Implications of Persistent (and Permanent) Engagement in Cyberspace.” *Journal of Cybersecurity* 5, no. 1 (January 1, 2019): tyz008. https://doi.org/10.1093/cybsec/tyz008.

Twitter. “Https://Mobile.Twitter.Com/Joebiden/Status/1341768024806797313.” Accessed March 13, 2021. https://mobile.twitter.com/joebiden/status/1341768024806797313.

Inkster, Nigel. “The Chinese Intelligence Agencies: Evolution and Empowerment in Cyberspace.” In *China and Cybersecurity*, edited by Jon R. Lindsay, Tai Ming Cheung, and Derek S. Reveron, 29–50. Oxford University Press, 2015. https://doi.org/10.1093/acprof:oso/9780190201265.003.0002.

Jacobs, Lawrence R., and Benjamin I. Page. “Who Influences U.S. Foreign Policy?” *The American Political Science Review* 99, no. 1 (2005): 107–23.

“Joint Statement for the Record on Foreign Cyber Threats to the U.S. to the SASC.” Accessed March 13, 2021. https://www.dni.gov/index.php/newsroom/congressional-testimonies/congressional-testimonies-2017/item/1614-joint-statement-for-the-record-on-foreign-cyber-threats-to-the-u-s-to-the-sasc.

Kahn, Herman. *On Escalation: Metaphors and Scenarios*. New Brunswick, N. J: Transaction Publishers, 2010.

Kamphausen, Roy. Hearing on “The Chinese View of Strategic Competition with the United States” (2020). https://www.uscc.gov/sites/default/files/Kamphausen_Opening_Statement.pdf.

Landler, Mark. “Clinton Urges Global Response to Internet Attacks.” *The New York Times*, January 21, 2010, sec. World. https://www.nytimes.com/2010/01/22/world/asia/22diplo.html.

———. “Clinton Urges Global Response to Internet Attacks (Published 2010).” *The New York Times*, January 21, 2010, sec. World. https://www.nytimes.com/2010/01/22/world/asia/22diplo.html.

Lin, Herbert. “Escalation Dynamics and Conflict Termination in Cyberspace.” *Strategic Studies Quarterly*, no. Fall 2012 (n.d.): 46–68.

Lyu, Jinhua. “A Chinese Perspective on the Pentagon’s Cyber Strategy: From ‘Active Cyber Defense’ to ‘Defending Forward.’” Lawfare, October 19, 2018. https://www.lawfareblog.com/chinese-perspective-pentagons-cyber-strategy-active-cyber-defense-defending-forward.

Meyer-Fong, Howard W. French, Ian Johnson, Jeremiah Jenne, Pamela Kyle Crossley, Robert A. Kapp, Tobie. “How China’s History Shapes, and Warps, Its Policies Today.” *Foreign Policy* (blog). Accessed December 11, 2020. https://foreignpolicy.com/2017/03/22/how-chinas-history-shapes-its-foreign-policy-empire-humiliation/.

Nakashima, Ariana Eunjung Cha and Ellen. “Google China Cyberattack Part of Vast Espionage Campaign, Experts Say,” January 14, 2010. http://www.washingtonpost.com/wp-dyn/content/article/2010/01/13/AR2010011300359.html.

Texas National Security Review. “Preparing the Cyber Battlefield: Assessing a Novel Escalation Risk in a Sino-American Crisis,” October 15, 2020. http://tnsr.org/2020/10/preparing-the-cyber-battlefield-assessing-a-novel-escalation-risk-in-a-sino-american-crisis/.

Rappeport, Alan. “Justice Department Charges Chinese Company With Espionage.” *The New York Times*, November 1, 2018, sec. U.S. https://www.nytimes.com/2018/11/01/us/politics/chinese-company-espionage-charges.html.

Sanger, David E., Julian E. Barnes, and Nicole Perlroth. “Preparing for Retaliation Against Russia, U.S. Confronts Hacking by China.” *The New York Times*, March 7, 2021, sec. U.S. https://www.nytimes.com/2021/03/07/us/politics/microsoft-solarwinds-hack-russia-china.html.

Sanger, David E., and Katie Benner. "U.S. Accuses Chinese Nationals of Infiltrating Corporate and Government Technology." *The New York Times*, December 20, 2018, sec. U.S. https://www.nytimes.com/2018/12/20/us/politics/us-and-other-nations-to-announce-china-crackdown.html.

"SASC Investigation Finds Chinese Intrusions into Key Defense Contractors | United States Commitee on Armed Services." Accessed March 13, 2021. https://www.armed-services.senate.gov/press-releases/sasc-investigation-finds-chinese-intrusions-into-key-defense-contractors.

United States Department of State. "Secretary Michael R. Pompeo at a Press Availability With Secretary of Defense Mark Esper, Australian Foreign Minister Marise Payne, and Australian Defence Minister Linda Reynolds." Accessed March 13, 2021. https://2017-2021.state.gov/secretary-michael-r-pompeo-at-a-press-availability-with-secretary-of-defense-mark-esper-australian-foreign-minister-marise-payne-and-australian-defence-minister-linda-reynolds/.

Shane, Scott, and Andrew W. Lehren. "Leaked Cables Offer Raw Look at U.S. Diplomacy." *The New York Times*, November 28, 2010, sec. World. https://www.nytimes.com/2010/11/29/world/29cables.html.

———. "Leaked Cables Offer Raw Look at U.S. Diplomacy (Published 2010)." *The New York Times*, November 28, 2010, sec. World. https://www.nytimes.com/2010/11/29/world/29cables.html.

Shinkman, Paul D. "Houston Consulate Closure Deterred China, But Not Before It Meddled With Vaccine Efforts: U.S. Intel Sources." U.S. News, July 31, 2020. https://www.usnews.com/news/national-news/articles/2020-07-31/houston-consulate-closure-deterred-china-but-not-before-it-meddled-with-vaccine-efforts-us-intel-sources.

"Significant Cyber Incidents | Center for Strategic and International Studies." Accessed December 11, 2020. https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents.

Sutter, Robert G. *The United States and Asia: Regional Dynamics and Twenty-First-Century Relations*. Asia in World Politics. Lanham ; Boulder: Rowman & Littlefield, 2015.

U.S. Embassy & Consulates in China. "The Chinese Communist Party's Ideology and Global Ambitions," June 27, 2020. https://china.usembassy-china.org.cn/the-chinese-communist-partys-ideology-and-global-ambitions/.

"The Chinese Dissident's 'Unknown Visitors,'" January 15, 2010. https://www.ft.com/content/c590cdd0-016a-11df-8c54-00144feabdc0.

Texas National Security Review. "The Escalation Inversion and Other Oddities of Situational Cyber Stability," September 28, 2020. http://tnsr.org/2020/09/the-escalation-inversion-and-other-oddities-of-situational-cyber-stability/.

United States House Committee on Oversight and Government Reform. "The OPM Data Breach: How the Government Jeopardized Our National Security for More than a Generation." Accessed March 13, 2021. https://republicans-oversight.house.gov/report/opm-data-breach-government-jeopardized-national-security-generation/.

Federal Bureau of Investigation. "The Threat Posed by the Chinese Government and the Chinese Communist Party to the Economic and National Security of the United States." Speech. Accessed March 13, 2021. https://www.fbi.gov/news/speeches/the-threat-posed-by-the-chinese-government-and-the-chinese-communist-party-to-the-economic-and-national-security-of-the-united-states.

Tiezzi, Shannon. “US Senate: Chinese Hackers Targeting US Military Contractors.” Accessed March 13, 2021. https://thediplomat.com/2014/09/us-senate-chinese-hackers-targeting-us-military-contractors/.

Council on Foreign Relations. “Tracking State-Sponsored Cyberattacks Around the World.” Accessed December 11, 2020. https://www.cfr.org/cyber-operations.

“Two Chinese Hackers Associated With the Ministry of State Security Charged with Global Computer Intrusion Campaigns Targeting Intellectual Property and Confidential Business Information,” December 20, 2018. https://www.justice.gov/opa/pr/two-chinese-hackers-associated-ministry-state-security-charged-global-computer-intrusion.

“UN GGE on Cybersecurity: The End of an Era?” Accessed December 11, 2020. https://thediplomat.com/2017/07/un-gge-on-cybersecurity-have-china-and-russia-just-made-cyberspace-less-safe/.

United States of America v. Zhu Hua and Zhang Shilong (n.d.).

“U.S. Charges Five Chinese Military Hackers for Cyber Espionage Against U.S. Corporations and a Labor Organization for Commercial Advantage,” May 19, 2014. https://www.justice.gov/opa/pr/us-charges-five-chinese-military-hackers-cyber-espionage-against-us-corporations-and-labor.

“U.S. Charges Three Chinese Hackers Who Work at Internet Security Firm for Hacking Three Corporations for Commercial Advantage,” November 27, 2017. https://www.justice.gov/opa/pr/us-charges-three-chinese-hackers-who-work-internet-security-firm-hacking-three-corporations.

“US Report: China Hacked Into Key US Defense Contractors Site | Voice of America - English.” Accessed March 13, 2021. https://www.voanews.com/east-asia/us-report-china-hacked-key-us-defense-contractors-site.