Cybersecurity Policy, Punctuated Equilibrium Theory, and the Biden Administration

Jacob Shively

University of West Florida

Email: jshively@uwf.edu

This paper extends research on national cybersecurity policy by testing whether punctuated equilibrium theory (PET) effectively explains the Biden administration's early positions on cyber and national security. Debate persists regarding whether and to what degree new administrations are able to chart new directions in major policy areas. Cybersecurity presents a particularly pressing challenge. As a relatively new national security concern, observers might expect a high degree of flexibility as strategic concepts, technical capabilities, and organization structures continue to evolve. Further, in the United States, transitions between presidential administrations and political parties represent major putative policy change. An earlier study found that, as predicted in PET, the Trump administration's cybersecurity remained relatively constrained within existing policy frameworks despite an express effort to implement major change. This paper extends that work by testing whether the Biden national cybersecurity policy conforms to predictions made by punctuated equilibrium theory. It evaluates the origins and content of the Biden administration's major cybersecurity policies between early 2021 and mid-2022. These findings will deepen the growing scholarship on cybersecurity and policy change and contribute to early evaluations of the Biden administration's national security strategies.

Paper prepared for the American Political Science Association conference. Montréal, Québec, Canada. September 15-18, 2022.

Introduction

This paper extends research on the conditions under which national cybersecurity policy changes or remains stable. Debate persists regarding whether and to what degree new administrations are able to chart new directions in major policy areas. Observers often expect new technological capabilities to drive strategic and policy innovations (Brimley 2013, Saltzman 2013, Ruggie 1975). Cybersecurity presents a particularly pressing challenge. As a relatively new national security concern, observers might expect a high degree of flexibility as strategic concepts, technical capabilities, and organization structures continue to evolve. Further, in the United States, transitions between presidential administrations and political parties represent major putative policy change. Applying punctuated equilibrium theory (PET), a prior study of the Trump administration found that officials accepted much of the prior administration's cybersecurity frameworks during their early months, and even their later, more assertive "defending forward" approach "remained a modification of, rather than a break with, prior cybersecurity policies." (Shively 2022, 12) In short, US cybersecurity strategy is "constrained by existing conceptual, political, and strategic commitments." (Shively 2022, 2) Were these findings unique, or does the Biden administration appear to follow the same pattern of relative stability as predicted by PET? The following pages evaluate the origins and content of the Biden administration's overarching cybersecurity policies between early 2021 and mid-2022 as well as, specifically, the administration's policy approach to software supply chain (SSC) threats. In each, rather than revise policy categories and priorities (such as espionage, warfare or property rights), policy makers interpreted the cyber threat within existing categories. For instance, when officials sought to address newly perceived threats based in software supply chains, their efforts focused more on developing more efficient and effective coordination than radically new strategic or policy approaches.

These findings offer several contributions. They begin the vital, early process of description and assessment of the Biden administration's cyber and national security policies, but they also further develop the scholarship on emerging technology and cyber as they relate to policy and strategy formation. This work also demonstrates the utility of PET across cases and raises the potential for application across international actors. For policy makers, finally, this work helps illustrate the opportunities and constraints on policy change.

Theory[1]

Technology change and security policy inevitably interact (Akaev and Pantin 2014, Herrera 2006). Though many scholars have grown skeptical that technology alone drives war decisions, competing states' capabilities often drive threat perceptions, sometimes to the point of arms racing (Colaresi et al. 2008, Garfinkel and Dafoe 2019, Lieber 2005, Talmadge 2019). Access to new technology like cyber networking may not alter the basic likelihood of conflict, but it can embolden certain types of aggression (Slayton 2016/2017, Schneider 2019b, Valeriano and Maness 2015). Still, questions surround how such policy changes and how quickly it changes. Cybersecurity practitioners, tacticians, and other professionals constantly revise and update their practices and policies. Does that translate into constantly evolving national policies? Stated differently, is national cybersecurity policy flexible and easily moldable, or is it "sticky" and inflexible?

[1] Note: large portions of this and the following section are drawn directly from Shively 2021.

According to the punctuated equilibrium theory (PET), policymaking tends to display both leaps and stasis (Baumgartner et al. 2014). Under this framework, public discourse defines salient issues and affects whether existing policies are either reinforced or questioned. In turn, policy entrepreneurs and others setting policy agendas will find change either inhibited or facilitated, respectively. Through that process, public and elite images of a given policy tend to be stable. In any given situation, policy stability is more likely than policy change. One reason for this lies in a bounded rationality approach to change. At most, humans can only focus on a few issues at once; thus, "collectively, a shift in the object of attention can lead to a disjointed change in preferred alternatives, even when the alternatives are well defined" (Baumgartner et al. 2014, 69). Policy change is more often than not constrained by the complexity of agreeing upon alternatives, by existing beliefs and images, and by the normal limitations of human cognition. Overall, policymaking is "a continual struggle between the forces of balance and equilibrium, dominated by negative feedback processes, and the forces of destabilization and contagion, governed by positive feedback processes" (Jones and Baumgartner 2012). These insights join an extensive literature on policy and institutional inertia (Cioffi-Revilla 1998; Goertz 2003; Levinthal 1998; Pierson 2004).

Existing scholarship on foreign policy and on technology innovation also offer insights into how cybersecurity may emerge and change as a national security policy. Like PET, this work reveals a propensity for relative policy stability and occasional moments of dramatic change amidst constant pressure. First, at any given point in time, inertia is likely to define the broadest levels of national security policy. Whereas a new technology like cyber introduces pressure for adaptation, a government's articulation of change—such as policies, institutions, strategies, and implementation—often lags or remains basically stable. David Welch's (2005) study of foreign policy, for instance, finds that loss-aversion discourages leaders from enacting major change. Jeffrey Legro's (2005) theory of foreign policy idea change finds that unless an existing idea is perceived to have dramatically failed and a single alternative is available, the status quo is likely to remain in place. In a more recent study, Patrick Porter (2018) argues that after the shocks of the 1930s and 1940s, the US foreign policy establishment adopted a new set of norms and conventional wisdoms that have been consistently replicated by the foreign policy elite. Second, when policy and other change happens, it tends to occur in big steps rather than incrementally. Of course, incremental adjustments are common, but incrementalism is often constrained within larger parameters. Jeffrey Lantis (2016), for instance, finds that state leaders enjoy relatively wide agency to push new international norms when new technologies challenge existing standards and practices. Actual change, though, is often constrained within a limited window of opportunity. Mark Zachary Taylor (2016) finds that domestic political interests will favor policy and innovative inertia unless and until they perceive a serious external threat. He dubs this "creative insecurity." This dovetails with older work (Samuels 1994) on "technonationalism," which describes, for example, Meiji Japan's willingness to abruptly adopt an ideology fusing disruptive technological innovation and military expansionism.

Such findings reveal two patterns. In each, inertia tends to dominate outcomes. Whereas individuals, organizations, businesses, or even governments themselves may push relentless technological innovation, the professional incentives and ideational frameworks of policy makers and bureaucracies prove far more "sticky." Changing them even under direct pressure is difficult. Adjustments are possible and common, but fundamental or structural change tends to occur in dramatic, stepwise corrections. Relative stability tends to dominate unless and until the environment experiences radical or systemic

transformation. If plotted on an x-y axis, technical capabilities would steadily increase with time. By contrast, strategies and policies related to cyber—not the technologies themselves—are likely to fit a stepwise profile. They are relatively stable, and the area between technical capabilities and actual strategy and policy grows. Then, at occasional inflection points, policy makers revise their policies to better match current capabilities, practices, and threats (Doran 1991). In short, as a country's power or technical capabilities change in a continuous flow, actual strategic policies will look like a series of steps along the arc as policy makers occasionally adjust to match reality.

Regarding cybersecurity, then, a fundamental break with prior approaches would likely require that several factors align. Without those conditions, any given administration is likely to be constrained to adjusting existing policy frameworks. Only by converging during the same temporal window do these variables create the conditions for major change. This paper posits that these variables are

- Sustained leader attention: the executive or another decisive policy figure must advance or support the policy change consistently over time rather than during either a single spike in attention or intermittently/unevenly.
- Systemic technological change: an emerging technology that affects interstate interaction capacity.
- Systemic security change: baseline interstate threat perceptions change due to an emerging issue or crisis.

Given these variables, if PET does offer useful predictions regarding national cybersecurity policy, the case studies will track with one of the three following scenarios. In the first, (1) sustained leadership attention along with systemic political, technical and security change creates the conditions for a "punctuated equilibrium" and the administration achieves a dramatic break with "business as usual." In other words, systemic conditions align with policy entrepreneurship. In the second and third scenarios, those conditions do not exist and Trump's administration would have either (2) modified existing cybersecurity policy or (3) attempted major change that proved abortive or limited. Here, ongoing adjustments and evolutionary adaptations are possible within policy inertia, but they will be constrained or limited within the preexisting framework.

Alternative explanations of strategic policy change emphasize regular adjustments and gradualism rather than periods of step-wise change. This paper cannot actively test these alternatives; however, they set the context in which PET may be a relatively more effective theoretical framework. One ideal type, often associated with rationalism, would hold that officials carefully respond to threats and changing circumstances. They consult experts, work out cost-benefit calculations and so forth and then implement the new strategy (Head and Alford 2013). The policy's relative success or failure then leads to ongoing adjustments. Periods of dramatic change are possible, but between such moments, adjustments persist and policy at point B is not necessarily constrained by policy set at point A. Second, an incremental or evolutionary view of policy change assumes that policy makers, policy entrepreneurs, bureaucrats, and other agents push for their preferred changes even as the issue and the surrounding conditions continue to change. Though largely abandoned among theorists, aspects of this "muddling through" framework persist in applied fields (Bendor 2015). Policy "learning" is another framework in which incremental or continuous change occurs (Moyson, et al. 2017). Over time, dramatic changes emerge from this process. In fact, PET itself is a form of evolutionary theory developed as an alternative to this gradualist concept of change. If the PET predictions do not hold or display only weak correlations with the cases, then it likely holds less explanatory power than these alternatives.

Materials and Methods

This paper highlights two possible predictions for cyber as a new security challenge. First, policy makers are likely to reach first for familiar or established frameworks rather than a radically new approach to accommodate the new technology. Second, in turn, that new technology is more likely to be deployed to supplement or reinforce an existing national security strategy than it is to directly undermine or change that strategy. Stated differently, new tactical capabilities will allow greater opportunities to pursue an existing strategy *rather than* force policy makers to dump the old and build a new strategy. New technology use is more likely to be constrained by existing policy and strategic frameworks *rather than* drive changes in those policies and strategies. Whereas the Trump administration—and President Trump in particular—had sought to introduce dramatic change into US politics and policy, the incoming Biden administration expressly vowed to turn from what they considered self-defeating turmoil and back toward the expertise and proceduralism of the Obama years. Still, cybersecurity threats continued to proliferate and new geopolitical challenges emerged. Conventional wisdom might hold that any US administration must implement constant updates and changes. Ideally, they will carefully evaluate their options and act accordingly. If nothing else, policy is likely to constantly evolve to meet ongoing challenges. PET, by contrast, anticipates that most strategic and policy approaches—for better and worse—will typically remain stable around certain fixed forms unless and until several factors converge on cascading, stepwise change.

This paper evaluates the first two years of the Biden administration's cybersecurity strategy and policy. First, it observes the Biden team's overall policies, executive actions, and statements on national cybersecurity with a particular focus on foreign policy and national security. Second, it observes a particular issue that had emerged as a particular danger during the months after the 2020 general election: software supply chains. After the SolarWinds hack (described below) emerged, senior US officials and cyber professionals considered the event a wake-up call demanding action.

This study defines *cybersecurity* in broad terms. *Cybersecurity* refers to efforts to secure and protect digital networks, information systems, and electronically-linked devises and infrastructure. Example threats for national security policy range from espionage against US government databases to direct attacks on military or civilian infrastructure to theft of private intellectual property to influence operations on social media. As an analytical category, this approach is potentially unwieldy; however, as an emergent technological and policy category, national level "cybersecurity" typically includes all those threat categories, as the strategy documents below illustrate.

Rather than a fully developed theoretical test, this case study approach is best understood as a "plausibility probe." It seeks to determine if the theoretical claims fit the empirical reality. Such work is a stepping stone to greater theoretical and empirical development and more formal structured, focused case comparison. A plausibility probe is appropriate, here, for several reasons. As Levy (2008) argues, this approach is designed to "sharpen a hypothesis or theory" as well as provide a "feel" for a theoretical argument. A relatively new case of presidential policy, the Trump administration and software supply chain policy are ripe for theory development and refinement. Similarly, the PET approach to cybersecurity policy is new. Levy admits that plausibility probes are often pressed into service as an all-purpose case study approach; nevertheless, they are a valuable intermediary step between identifying a possible theoretical pattern and intensive testing or case comparison (Eckstein 1975). In addition, isolating specific causal relationships, such as in a process tracing approach, will be

difficult with a vast number of possible inputs, some or many of which may still be classified. In addition, there are a relatively limited number of possible observations, particularly regarding this new technology. Overall, as Mahoney and Goertz (2006) argue, along with others (Holsti and Rosenau 1986), such qualitative approaches are appropriate where "the research goal is the explanation of particular outcomes." PET predicts that most cybersecurity strategy and policy changes will occur within a preexisting framework. Is that, in fact, what happened? By addressing this question, the paper seeks to determine whether PET is a plausible theoretical account of national cybersecurity policy change.

2020-2021: From Trump's Approach to Biden's Early Executive Actions

The Trump-Biden presidential transition was dramatic. The election and its campaigns themselves unfolded during the height of the COVID-19 pandemic, government responses to that crisis and the social energy those unleased. Still, the election itself was later defined by its aftermath, when President Trump attempted to challenge the election results. Despite that drama, US national cybersecurity strategy remained relatively stable. Whereas the 2016 election was later characterized by investigations into whether and how malicious actors, particularly the Russian government, may have spread mis- and disinformation to shape the outcome, such attacks remained relatively marginal. Indeed, agents like US Cyber Command later received relative freedom to seek out and proactively strike likely cyber threats to the election process. Meanwhile, a series of startlingly large cyber attacks, capped by SolarWinds, drove policy makers to add software and hardware supply chains to their ballooning list of national cybersecurity fears. Convinced that many Trump administration initiatives were ill-conceived, the Biden administration moved quickly once in office to commission internal executive branch policy and threat reviews as well elevate cyber to a higher priority level than had the Trump administration. Despite all this movement, neither the strategic posture nor the guiding policies for cyber saw dramatic change.

Through the latter half of the Trump administration, the US government developed a more assertive cyber strategy for national security. The Trump administration did carry forward broad cybersecurity frameworks inherited from prior presidencies, and when confronted with major geopolitical challenges, it reached for more traditional levers of power. (Shively 2021) Still, it's marginally more assertive approach to cyber threats grew to become a pervasive aspect of US cybersecurity strategy and policy. Logically, observers might worry that more aggression might spark spiraling escalation, but many policy makers and scholars remained skeptical that direct tit-for-tat escalation was likely. (Borghard 2019) Both the targets and the technical realities of these attacks, they reasoned, left one-to-one response difficult for any party to achieve. Perhaps the most well-articulated such strategy in the latter Trump and early Biden years was "defending forward." Promulgated and applied most visibly by Gen. Paul Nakasone, commander of US Cyber Command, the concept started with a presumption of "constant contact with our adversaries." ("An Interview with Paul Nakasone," 2019) In such an environment, Nakasone and others reasoned that "persistent engagement" is a meaningful strategic solution because seeking to attack and disable adversaries shifts many of their resources from offense to defense. (Nakasone 2019; Nakasone and Sulmeyer 2020) Publicly, their most significant target remained Russian trolls and hackers. Leading up to and during the 2018 and 2020 US elections, US Cyber Command launched dozes of attacks to threaten, undermine, or disable known attack sources affiliated with the Russian government. (Nakshima 2019; Gazis 2020) Elsewhere, US officials described to reporters their increased incursions into Russia's power grid and other infrastructure. (Sanger and Perlroth 2019) The Central Intelligence Agency (CIA) conducted a wide range of covert cyber operations against Iran and other targets after President Trump signed a national security memorandum authorizing more latitude for "offensive cyber

operations." (Dorfman et al. 2020; Chesney 2020) Supporting policies included more concerted Department of Justice actions against Chinese intellectual property theft and pressuring companies and allied governments to resist adopting inexpensive technology hardware from Huawei, a Chinese corporation many US officials believed to be vulnerable to Chinese government infiltration. (Nakashima 2018; Pomfret 2019) This more assertive posture saw relatively little backlash from domestic audiences, bureaucratic players, or international partners. One reason is that Trump's team sought to hand agencies like US Cyber Command greater autonomy to conduct attacks and other actions. This was possible partly because Trump himself displayed little direct interest in cybersecurity issues. (Shively 2021, 744)

By contrast, the new Biden administration sought to re-centralize cybersecurity strategy and policy as a national security priority. To do this, incoming officials reached for experienced personnel and familiar bureaucratic tools. For instance, Biden appointed Alejandro Mayorkas, an establishment figure from the Obama years promising to elevate cybersecurity, to head the Department of Homeland Security (DHS). (Hessen 2020; Miller 2021) Anne Neuberger, a rising figure overseeing the National Security Agency's Cybersecurity Directorate, would serve as the first deputy national security adviser for cyber and emerging technology. (Sanger 2021) The administration's cyber priorities did confront a bureaucratic complication from the outgoing Congress, which used the National Defense Authorization Act (§ 1752) to establish a new Office of the National Cyber Director (ONCD) with around 75 staff.[2] (Grotto 2021; H.R. 6395) A key goal in this move was to centralize national-level cyber strategy and accountability, or, as Senator Angus King (I-ME) described, "One throat to choke." (Nakashima 2021 ["Tension grows"]) Chris Inglis, a well-known figure with a military background, would ultimately be confirmed to head the office and flesh out its priorities on the administration's terms, but the effort lingered into July 2021 because White House officials preferred cyber strategy to be run out of the National Security Council where officials need not be confirmed by the Senate. (Nakashima 2021 ["Tension grows"]) Along the way, Biden proposed tens of billions of dollars to reinforce and expand capabilities at the Cybersecurity and Infrastructure Security Agency (CISA) and other agencies. The effort would pull thousands of new experts into the government and reinforce programs across threat vectors but in particular to stymie another SolarWinds-type hack.

Between immediate reactions to SolarWinds and confidence that Trump's decentralized, lower priority approach was counterproductive, Biden's administration brought energy to national cybersecurity policy, but it remained unfocused. The initial "strategic intent" for the ONCD, for example, largely restated existing concepts about coordination and resilience, and the administration delayed . ("A Strategic Intent Statement" 2021) DHS similarly released a broad set of actions, such as "driving urgent remediation risks" and government-private sector collaboration. ("DHS Announces Steps" 2021) In his first major foreign policy speech, Biden vowed to "elevate" cyber security but only mentioned personnel and offices. (Biden 2021 ["Remarks on America's place in the world"]) Officials may have hoped that installing established professionals at senior levels would foster clarity. (Bing and Menn 2021) Revelation of a massive software penetration had further unsettled already alarmed government officials but only generated marginal immediate responses. In late 2020, cybersecurity firm FireEye announced that hackers had inserted malicious code into a software update for a system called "Orion," owned by Texas-based firm SolarWinds. Tens of thousands of private and public organizations, up to the

[2] Notably, President Trump vetoed the bill, but Congress overrode the move—the only veto override of Trump's term—shortly before the session closed in early January 2021.

Department of Homeland Security and the Department of Defense, had been compromised and potentially exploited for months. Analysts eventually concluded that Russian intelligence was behind the attack. (Temple-Raston 2021) In short, hackers used the software supply chain (SSC, discussed more in the next section), which is sprawling and accessible at low-level, obscure points. Like a Shepherd tone, SolardWinds added to a sense of endlessly ascending threat, and US officials felt pressure to respond. (Newman 2021) President Biden expressly identified "Russian recklessness" as an issue of "collective security," and senior officials like Neuberger and National Security Advisor Antony Blinken promised interagency coordination and planning but did not specify a substantive response. (Biden 2021 [Remarks for Munich Security Conf]; Psaki and Neuberger 2021)

2021-2022: Software Supply Chain

Uncovered in late 2021, months before the Biden administration took office, the SolarWinds hack—and before that, NotPetya—captured a high degree of attention from government officials and private cybersecurity professionals. Software supply chain threats had become unusually prominent and politically salient during the early months of the Biden administration. Thus, the initial government assessment of the threat environment along with its strategic and policy response are a valuable baseline for researchers. Official studies and policy statements reveal the US government's positions on the general cybersecurity threat landscape and the specific SSC threat landscape. Most of this work focuses on technical and procedural issues related to supply chains, cyber infrastructure, and so forth. Presidential executive orders (EOs) and similar policy directives along with public statements and actions reported in the media can serve as a representative indicator of a given administration's perception of the threat landscape and articulate strategic and policy priorities.

Stymied by direct penetration of an adversary's networks, governments and private actors over the preceding five to 10 years had reached for identifying gaps in software updates and open-source code libraries. (Breaking Trust 2020; NIST 2021, 4) Supply chains in general had already become a source of concern. In 2017, The Defense Cyber Board—an agency housed in the Department of Defense—concluded that whereas many US weapons systems are designed to serve for relatively long lifecycles, most "were developed, acquired, and fielded without formal protection plans." (Hoeper and Manferdelli, 2017) Targeting open-source software is particularly appealing because the effort is typically less expensive and less time consuming than direct attacks. (Nagle et al. 2020, 9) It explained that whereas attackers must execute a complex series of steps—from intelligence and planning to designing and creating the attack to inserting the software to achieving the intended effect—government defenders confronted even more complex supply chains vulnerable at the lowest levels of production, including overseas sourcing, that allow attackers to "bypass the costly and potentially risky process of malicious insertion." (Hoeper and Manferdelli 2017, 2) Researchers often argue that national-level cybersecurity strategies are necessary to prioritize and coordinate responses to software supply chain and other threats in the digital landscape. (Building a Defensible Cyberspace 2017, Deliver Uncompromised 2018, King and Gallagher 2020)

For example, observers often characterize NotPetya as the world's most destructive cyberattack to date (Greenberg 2018). The malware locked files with random encryption on computers across the globe, most notably in the global shipping firm Maersk; however, the attack itself spread outward from a widely-used, private tax application used by the Ukraine's government. Effects lingered for years and led to damages estimated around $10 billion. Consensus among officials in Ukraine, the United States and

elsewhere is that NotPetya—launched on Ukraine's Constitution Day—was either directly committed or commissioned by the Russian government, likely in an effort to intimidate its neighbor and Ukraine's trading partners. Three years later, Microsoft identified a similar malware attack named WhisperGate that targeted Ukrainian government agencies during a crisis in which Russia had massed over 100,000 troops along Ukraine's borders. (Lakshamanan 2022) With the SolarWinds attack, US officials confirmed that Russian government agents penetrated a software product used by the US government named Orion, which then propagated a "backdoor" during routine software updates. (SolarWinds Cyberattack 2021) Throughout most of 2020, Russian agents enjoyed extensive access to systems in agencies ranging from the Department of Homeland Security to the National Nuclear Security Administration to non-government corporations, hospitals, and universities. Espionage rather than strategic intimidation, this attack still led to widespread, and expensive, scrambling among high-level officials to address the immediate problem and rethink existing approaches to software supply chain security.

The Trump administration in 2019 declared a state of emergency to address threats to supply chains for information and communications technology and services. (EO 13873, 2019) Previously, researchers in 2014 revealed that the open-source "Heartbleed" vulnerability in the programming library OpenSSL affected hundreds of thousands of websites and millions of hospital patient records. The US Congress eventually convened industry leaders to address this now glaring supply chain threat that could affect a huge portion of national and global infrastructure. (Walden and Harper 2018) Trump's EO cited increasing espionage and similar attacks from adversaries, and it held that these attacks posed a direct threat to the US economy and its national security. Also revealingly, it highlighted a tension between the United States' traditionally internationalist, open approach to commerce and economic growth and the administration's nationalist emphasis on sovereign prerogatives and fears of security exposure. The order sought to prohibit US agencies from acquiring or using foreign software and devises that may be compromised by a foreign government. In effect, it sought to marginalize the use of Chinese information technology. Indeed the next year, Trump executive orders effectively banned several Chinese applications, such as the video social networking application TikTok and several applications developed by the company TenCent, such as WeChat.

In his first year in office, President Biden signed several EOs that directly or indirectly addressed SSC threats. These shifted the tone but not the underlying logic of the Trump administration's relatively nationalist approach. They also explicitly overlapped two strategic agendas: 1) reinforcing domestic supply chains for national security and 2) supporting domestic economic development. Indeed, a key piece of leverage for the U.S. government is its market power. Even without Congressional legislation, the Executive may drive national standards because its purchasing power in the private market is so large that developers may find that following federal standards is more profitable than either withdrawing from government sales or developing only some products to meet those standards.

For instance, in June 2021, Biden revoked Trump's blanket ban on specific Chinese-owned smart phone applications; yet, the EO explicitly reaffirmed the Trump language about national security threats and the dangers of unguarded supply chains. (EO 14034, 2021) Earlier, within days of taking office (EO 14005, 2021), the administration initiated a policy review to press government agencies on acquisition of "Made in America" services, hardware, and computer technology. A month later, the "Executive Order on America's Supply Chains" (14017, 2021) activated a 100-day, interagency process to review critical goods, materials, agricultural, and manufacturing resilience alongside cyber risks. After reviewing critical energy infrastructure, the White House also released a national security memorandum (Biden 2021) updating and clarifying methods for the Federal Government and private industry to "monitor

control systems to detect malicious [cyber] activity" and then to share information and coordinate response practices.

Perhaps the most expansive executive order (14028) cast a broad agenda to "improve the nation's cybersecurity." It included processes to create "baseline security standards" for software purchased by the US government and to develop an "energy star"-type designation "so the government – and the public at large – can quickly determine whether software was developed securely." (White House, FACT SHEET 2021) (In a follow-up presidential memorandum (2022), software remained only an incidental concern.) Overall, as Jean Camp at Indiana University summarized, EO 14028 "addresses the information asymmetries central to the security market." (Camp 2022) These inequalities include the indistinguishability between high- and low-quality components at purchase, the opacity of who may update code, and just how likely it is that given vulnerabilities might be exploited. Still, Camp concludes that EO 14028 represents only "the survey" for a map to take substantive action on securing software supply chains.

Beyond executive orders and presidential fiats, administration officials—particularly in the White House, Department of State, Department of Defense, and CISA—set out a wide range of high-level policy solutions. During a White House meeting between major government agency heads and industry leaders, participants emphasized basic procedures and practices, such as code signing, prioritizing the most important open source software projects, and Software Bills of Material. (Readout of White House Meeting on Software Security 2022) In interpreting EO 14028, NIST developed minimum standards for verifying code from vendors and developers. Fitting with its mission, these were a set of specific techniques organized into existing classes, from threat modeling to fixing bugs. ("Recommended Minimum Standards," 2021) Similarly, in 2022, the National Security Agency and CISA released technical guidance for protecting Kubernetes, an open-source software used for managing applications across hosts. ("Kubernetes Hardening Guide" 2022) Though the guidance was intended for public use and a key threat vector was SSC, the guidance remained silent on threat landscape. Notably, international agreements to address SSC vulnerabilities remained underdeveloped. For instance, as mentioned above, the United States joined its "Quad" partners in "identifying and evaluating potential risks in supply chains for digitally enabled products and services" as well as "aligning baseline software security standards for government procurement," yet this effort largely emphasized existing efforts through CERT and establishing an unspecified "Quad Cybersecurity Partnership." (Quad Joint Leaders' Statement 2022; FACT SHEET 2022)

Results

The paper observes three proximate variables that affect the likelihood of national cybersecurity policy and strategic change: *leader attention*, *systemic technological change*, and *systemic security change*. If any one of these categories remains stable when an administration seeks to change cybersecurity policy, its efforts are likely to be constrained within the parameters of existing policies. These are drawn from a prior study that applied the same framework to the early Trump administration. That work found, consistent with predictions drawn from punctuated equilibrium theory, "Ambitious policy proposals were not sufficient to overcome both relatively low attention from the president himself and an administration more focused on traditional security threats." (Shively 2021, X) The current study observes two different cross-sections of the Biden administration's approach to cybersecurity. The first is a general overview of how cyber fit into the wider Biden foreign policy and administrative agenda, and the second is a more targeted observation of a new and particularly salient threat issue: software supply

chains. In both, President Biden displayed relatively more leader attention to cyber issues than President Trump, but as in the Trump administration, the other two variables remained relatively stable. Consequently, a in the Trump case, scenarios(2), as described above under "Theory," played out. By contrast, scenarios (1) and (3) never materialized.

Under scenario (1)—sustained leadership with systemic political, technical, and security change—Biden and his team did place greater formal prioritization on cybersecurity by creating or elevating offices, seeking to coordinate across agencies from the White House level, and having the president himself regularly include cyber issues as a point of national concern. Even Congress displayed some level of policy entrepreneurship by creating the ONCD. Despite all this, administration officials themselves tended to portray their effort as restoring cyber as a priority rather than revolutionizing its practice, and indeed their policy efforts reflect this. For this reason, scenario (3)—attempted but abortive or failed dramatic change—also did not occur. Software supply chain efforts reflected this. Though they perceived the threat to be relatively novel, or at least newly serious, they drew upon and expanded existing solutions and procedures. At the system level, the familiar roster of adversaries with familiar agendas remained the same. Most tellingly, when Russia invaded Ukraine in February 2022 and the United States helped coordinate a global response, many observers expected a wave of cyber attacks based in or supported by Moscow. In fact, that dog did not bark. The cyber component of that conflict displayed only marginally more activity than the prior baseline. Neither technological nor behavioral patterns displayed notable change. Whatever the reason for this, interstate relations and the international system remained relatively stable in the minds of US policy makers.

Instead, scenario (2) emerged: modifications to existing policy. Recall that this prediction is distinct from, say, slow, directional change or evolution toward new types. In fact, the fundamental strategies and policies remained relatively stable. In response to general threats and long-standing threats, the administration sought to elevate and facilitate existing programs and capabilities. Officials did not seek out new strategic approaches. Their logic seems to have been that existing capabilities were sufficient for the overall threat; however, those capabilities were insufficiently coordinated. (Whether and how the overall US cybersecurity strategy itself was sufficient is a vital but separate analytical question.) Thus, on SSC, administration officials recognized a persistent challenge and began a process of determining solutions, but these remained technical and organizational. Indeed, the threat itself was procedural and slow. No new conceptual approach emerged. When US officials agreed to high level cooperation with "Quad" partners, the concept remained vague with little indication even of who might manage

Conclusion

PET anticipates long periods of relative stability and infrequent, cascading or stepwise change when several factors align. In both this study and the prior study of the Trump administration on which this is based, officials did recognize a serious and persistent threat, and they sought to match that with innovative solutions. During Biden's first two years, this innovation enjoyed the president's direct support and efforts of well-established policy leaders. Still, all things being equal, strategic and policy approaches will remain stable without strong systemic pressures or incentives. Though cybersecurity and, specifically, software supply chain threats were "systemic" in that they were an inevitable fact of a networked world and often driven by a specific set of adversarial states, those realities had remained stable for some time. No new technological or geopolitical impetus energized a collapse of existing

approaches. Instead, policy makers reached for improving, streamlining, and coordinating existing capabilities. Similarly, though the "defending forward" agenda appeared to continue into the Biden administration, as a strategy, it remained marginal and targeted rather than a core logic driving US cybersecurity policy.

One deficit of this study is that whereas these findings correlate with PET predictions, the study has not set out to identify, test, and compare, say, an evolutionary or rational actor model. Future scholarship might seek to develop a parsimonious comparative framework for these models. Though US cybersecurity strategy and policy may appear relatively stable, different analytical or observational approaches may reveal more change in presidential administrations' baseline assumptions and approaches.

For policy makers, these findings are not necessarily a condemnation to existing strategic and policy patterns. Innovation is possible, and it did occur at the widest level of policy implementation and oversight as well as with SSC policy. Rather, PET suggests that policy makers would be prudent to expressly identify existing parameters and, even if behind closed doors, recognize that decisions and approaches of prior administrations are now part of the landscape. Further, when stepwise or ecological change occurs in the strategic or policy environment, actors are more likely to prosper if they have already developed long record of seeking to anticipate or shape that change. (This is why, for instance, governments are racing to develop and lead in artificial intelligence innovations.) In observing partners and adversaries, similar dynamics occur. Analysis and commentary on cybersecurity tends toward worst-case assumptions, yet other governments and private actors are typically just as constrained as the United States. To be clear, potential for calamitous or widespread attacks and other penetrations are real, but PET suggests that at any given moment, the threat is more about the extent rather than the type of threat.