‘Madman Theory’ or ‘Persistent Engagement’? The Coherence of US Cyber Strategy under Trump

Joe Devanny

Department of War Studies, King’s College London, London, UK

ABSTRACT
The Trump administration authorized an assertive cyber strategy of persistent engagement and defending forward. Less a radical break than an evolution, it reflected the impact of bureaucratic politics, emerging theories about cyber competition and arguments about improving the Obama-era strategy. This article employs recent research into “madman tactics” to reject claims that “Madman Theory” improves understanding of persistent engagement. The new strategy was a coherent, albeit bold, response to the operating environment. Under Trump it was undermined by political contingencies. Pursued prudently under Biden, it could yet achieve its objectives: preserving US superiority, promoting stability and security in cyberspace.

KEYWORDS
Cyber strategy; National security; US politics; persistent engagement

Introduction
One of the signature features of Donald Trump’s presidency was his penchant for disintermediated communication with voters and the world at large (Cooper, 2019, p. 804). His most favored medium, the social media platform Twitter, provided direct reach to millions of followers—until, that is, he was banned from the platform two days after his incitement of the violent mob of his supporters that occupied the U.S. Capitol building on January 6, 2021 (Tiku et al., 2021). Trump’s use of social media shaped the ways in which the traditional news media covered his administration (Cammaerts, 2020, pp. 244–246). Trump often used Twitter to signal his views on foreign policy, departing from traditional diplomatic practice to tweet in intemperate language and sometimes issued extreme threats. Indeed, Trump had reportedly claimed that his unpredictability was a deliberate performance to increase chances of success in international negotiations (McManus, 2019, p. 977; Swan, 2017).
Emanuel Boussios argued recently in this journal that US cyber strategy had shifted under the Trump administration, toward a more aggressive “offense-first” approach (Boussios, 2020, p. 2). Boussios directly invoked “Madman Theory” as an explanation of the administration’s underlying approach to cyber strategy. He distinguished between Trump’s approach and a more defensive strategy discernible under the two previous presidents, Barack Obama and George W. Bush.

The distinction between Trump-era cyber strategy and its predecessors is incontestable and well-documented, notwithstanding the boldness of Op OLYMPIC GAMES/Stuxnet, a now-famous cyber operation against Iranian uranium enrichment facilities that was reportedly developed and implemented, with Israeli assistance, under the Bush and Obama presidencies (Sanger, 2012; Zetter, 2014). Boussios is right to argue that US cyber strategy under Trump became more assertive, but this article suggests that his use of “Madman Theory” undermines rather than strengthens his assessment of the strategy and its implications.

This recent turn in US cyber strategy should not be too closely associated with Trump himself, particularly with the more irascible, unpredictable aspects of his executive behavior. This is not to argue that “Madman Theory” is inapplicable to other areas of Trump’s policy. Seitz and Talmadge in particular have argued persuasively that “Madman Theory” can be applied to Trump’s policies toward North Korea and Iran, albeit concluding that Trump’s adoption of “madman tactics” produced policy failure in each case (Seitz & Talmadge, 2020). It is furthermore a contention of this article that Trump’s unpredictable and politically self-serving behavior actually undermined the efficacy of US cyber strategy.

Similarly, Boussios is right to highlight concerns about the possible adverse impact of this more assertive turn in US cyber strategy. The advent of the Trump administration—with its rapid turnover in senior national security appointments—should be interpreted as a conjuncture in which the balance of forces shaping US cyber strategy could be reshaped by senior officials, producing realignment toward a more active, but no less predictable or rational strategy than was pursued under Obama or Bush. Whilst genuine risks remain, these should not be attributed to the impact of Trump’s personal unpredictability, but instead to the foreseeable impact of a more aggressive US posture on the emerging norms of acceptable state behavior in cyber competition. It is increasingly argued by critics of “persistent engagement” that it has potentially grave system effects, including deleterious influence on the cyber strategies of both allies and adversaries (Healey, 2019; Healey & Caudill, 2020; Klimburg, 2020; Schneider, 2020; Smeets, 2020).

This article proceeds in four parts. First, it briefly outlines the assumptions of “Madman Theory,” drawing on recent scholarship (McManus, 2019;
Seitz & Talmadge, 2020) to identify the different ways in which it might be used to explain the Trump administration’s cyber strategy. Second, it focuses on the context—historical and theoretical—of persistent engagement strategy, its subsequent bureaucratic development and operational implementation. It argues that “Madman Theory” is ill-suited to explain the strategic logic of persistent engagement. In the third section, prominent criticisms of persistent engagement are identified and analyzed, arguing that although persistent engagement is robust to Boussios’s “Madman Theory” critique, it has nonetheless provoked skepticism, particularly about its potentially adverse system effects. Fourth, it assesses the implications for US cyber strategy of a series of developments during the post-election transition between the Trump and Biden administrations, including the adverse impact of Trump’s self-serving “stolen election” narrative, his dismissal of senior cyber officials, and the administration’s response to the SolarWinds breach. This final section concludes with a preliminary assessment of the impact of the SolarWinds breach on debates about the efficacy of US cyber strategy. In the wake of the SolarWinds breach, the conclusion assesses the likely impact of a Biden presidency on persistent engagement’s longevity, scope and bureaucratic processes. It argues that continuity of cyber strategy is more likely than significant change under Biden and will further highlight the gap between the logic of persistent engagement and “Madman Theory.” Legitimate concerns will, however, continue within the scholarly and policy communities, and indeed amongst US allies worried about the potentially deleterious system effects of the strategy, particularly on the behavior of hostile state actors in cyberspace.

**Theorizing “madman tactics”**

As Roseanne McManus observes in her nuanced analysis of the impact of perceived madness on coercive negotiations, there is a long history of reflection on its potential benefits—with Machiavelli being the earliest strategist cited by McManus (McManus, 2019, p. 979). In modern times, McManus highlights the contributions of Daniel Ellsberg and Thomas Schelling, both of whom recognized the contingent strategic benefits of perceived madness. The theory is perhaps most commonly associated with President Richard Nixon—not least because of Nixon’s explicit articulation of this approach as a means to secure a settlement of the conflict in Vietnam (Haldeman & DiMona, 1978, p. 83).

McManus employs a specific typology of perceived madness that distinguishes between two dimensions: whether or not a leader deviates from “rational consequence-based decision-making” or merely calculates rationally but on the basis of “extreme preferences”; and, second, whether a leader is perceived as suffering from “situational” or “dispositional” madness, i.e.
whether the perceived madness is limited to specific issues or circumstances, or is instead all-consuming (McManus, 2019, p. 978). Plausibly, McManus suggests that perceptions of “situational” madness are likely to be more useful in negotiations than are those of “dispositional” madness, arguing that the latter can even be counterproductive (McManus, 2019, p. 1007).

There is significant doubt about the applicability of “madman theory”—and indeed, about precisely what this theory entails—to Trump’s wider foreign policy, although little doubt that Trump himself invoked elements of it in his social-media and other pronouncements (McManus, 2019; Seitz & Talmadge, 2020). Seitz and Talmadge define “madman tactics” as “meaning a leader’s deliberate attempts to defy the expectations of foreign counterparts, particularly by conveying extreme preferences and/or appearing impervious to the costs of war” (Seitz & Talmadge, 2020, p. 32). They regard the contemporary and historical record as evidence that such tactics rarely succeed, due to problems with signaling, credibility and assurance: “clearly signaling extreme preferences” credibly is often difficult and can even backfire, “by making a leader appear impossible to placate and therefore making the target more likely to stand firm or even escalate” (Seitz & Talmadge, 2020, p. 32). As they conclude, “madman tactics must strike an almost impossible balance—crazy enough to get an opponent’s attention, but not so crazy that they lose credibility or provoke escalation rather than concessions” (Seitz & Talmadge, 2020, p. 37). Surveying the consequences of Trump’s “madman” foreign policy approach to North Korea and Iran, Seitz and Talmadge judge that both adversaries concluded: “that negotiating from a position of strength—nuclear strength—is the best move against a US president who seems incapable of negotiating in good faith. Unpredictability has yielded predictably little leverage and has even backfired” (Seitz & Talmadge, 2020, p. 42).

These recent contributions to understanding of “Madman Theory” and its applicability to some Trump administration policies can be employed to clarify its inapplicability to persistent engagement strategy in cyberspace. To conform to the principles of “Madman Theory” the Trump administration’s cyber strategy would have tried to exploit adversaries’ perception of Trump’s unpredictability, extreme preferences or situational departure from the conventions of rational decision-making. The next section explains the origins and development of persistent engagement strategy and situates it contextually as a response to perceived shortcomings in the precursor strategy. This follows the late Colin Gray’s insight that a historical approach to strategic theory is necessary to understand contemporary developments in cyber strategy (Gray, 2013). It argues that, in neither its theoretical origins, bureaucratic development nor operational execution, should persistent engagement be regarded as a practical exercise in “Madman Theory.”
The rise of persistent engagement strategy

To deter possible Russian cyber operations to disrupt the 2018 midterm elections, US cyber command conducted an operation to block the internet access of arguably the most infamous Russian troll factory, the Internet Research Agency, as well as a parallel operation to send “direct messages” to Russian hackers—revealing that the US knew their identities—to deter them from disrupting the midterm elections (Barnes, 2018; Nakashima, 2019). Cyber Command also reportedly pre-positioned an implant on Russian energy infrastructure, an effort to signal to Russia the costs it could incur if it continued to conduct cyber operations against US energy infrastructure (Goodin, 2019; Nechepurenko, 2019). Boussios argues that these reported operations were collectively “reminiscent of a ‘Madman Theory’ foreign policy strategy undertaken by President Nixon in an attempt to end the Vietnam War” (Boussios, 2020, p. 2). In contrast, it is argued in this article that the specific and limited operations conducted to date under the rubric of persistent engagement are different in kind and extent from the ineffective theatrical steps taken by Nixon to elicit Soviet perceptions of his madness thereby to obtain a more favorable outcome in Vietnam.

Contrasting the Trump administration’s cyber strategy with its antecedents, Boussios observes that: “The US military and US government traditionally has been pretty cautious when it pertains to cyber operations, and in particular the Obama administration specifically in cyber was known for weighing every possible consideration before taking action” (Boussios, 2020, p. 6). This view conforms with those articulated elsewhere by both critics and advocates of the persistent engagement strategy. From 2012 until 2018, when it was replaced by National Security Presidential Memorandum 13 (NSPM-13), offensive cyber operations and active cyber defence operations were overseen by an interagency coordination process mandated by Presidential Policy Directive 20 (PPD-20). The PPD-20 process proceeded cautiously, on the premise that cyber operations “may raise unique national security and foreign policy concerns that require additional coordination and policy considerations because cyberspace is globally connected” and because cyber operations could have “potential unintended or collateral consequences that may affect US national interests in many locations” (White House, 2012, p. 6). It required specific presidential approval for any offensive cyber operation that was “reasonably likely to result in ‘significant consequences’” (White House, 2012, p. 9).

According to one prominent critic of persistent engagement theory, Jason Healey: “This interagency process was in place to ensure civilian control over the military; limit potential escalation; allow other agencies that might be affected by cyber operations to have a say; and to confirm the military had a reasonable degree of certainty their operation would succeed,
not be too destabilizing or embarrassing, and not cause undue collateral
damage” (Healey, 2019, p. 3). Healey noted that this interagency process
was criticized for being slow and restrictive, although he also observed that:
“Cyber operations in an existing warzone had a smoother [authorization]
process” (Healey, 2019, p. 3).

According to one of persistent engagement’s most notable advocates—
and arguably its most senior serving architect—the current head of US
Cyber Command and the National Security Agency (NSA), General Paul
Nakasone, this precursor process suffered shortcomings and failed to
adapt to a contested operating environment. In a recent article, Nakasone
argued that the strategic concept of cyber command “has
evolved from a ‘response force’ to a ‘persistence force’” (Nakasone, 2019,
p. 11). Nakasone clarifies that: “Persistence should not be mistaken for
engagement for engagement’s sake; instead, it is an approach that
empowers US cyber forces to achieve more decisive results in pursuit of
objectives set by national leaders” (Nakasone, 2019, p. 11). Persistent
engagement is thus conceived as more assertive, but nonetheless tied to
rational, consequence-based reasoning and deliberate calibration of oper-
ations to achieve objectives.

Moreover, whilst persistent engagement is a strategic prescription for the
US, it flows from an analysis of adversaries’ behavior in cyberspace:
“Continuous action in cyberspace for strategic effect has become the norm,
and thus the command requires a new strategic concept” (Nakasone, 2019,
p. 12). Nakasone argues that the more defensive posture of previous US
strategy meant that: “In response, increasingly cyber-capable governments
escalated their operations against their own citizens and ours. They
mounted global surveillance of opposing views and are stealing unprece-
dented quantities of intellectual property and personal data, disrupting
democratic processes, holding critical infrastructure at risk, and eroding US
power” (Nakasone, 2019, p. 11).

The arguments articulated by Nakasone are consistent with the develop-
ment of official US strategy during the Trump administration, including
the National Security Strategy (2017), National Defense Strategy (2018) and
the Command Vision for US Cyber Command (2018). The 2018
Command Vision, in particular, emphasizes that persistent engagement
should not be interpreted as an offense-only or offense-first strategy. It is
instead an effort to integrate more assertive operations, defending forward
and imposing “tactical friction and strategic costs on our adversaries, com-
pelling them to shift resources to defense and reduce attacks,” alongside
concomitant effort to improve existing cyber defense and threat intelli-
gence-sharing processes, working with partners in government, the private
sector and US allies (US Cyber Command, 2018, pp. 6–10).
The intellectual origins of persistent engagement

The more assertive turn in US cyber strategy is articulated in a body of official publications and statements from 2018 onwards. Its provenance is, however, older and involves contributions from both insiders such as Nakasone and outsiders from within the wider policy and academic community (Graff, 2020). It is perhaps worth mentioning the close professional associations with US Cyber Command, the National Security Agency (NSA) and wider Department of Defense (DoD) that are discernible in the careers of prominent academic and policy-research advocates of persistent engagement theory. For example, in 2016 Richard Harknett was the first scholar-in-residence at Cyber Command; Emily Goldman is both a scholar and a government official, currently serving as a cyber strategist and cyber persistence subject matter expert at Cyber Command and the NSA; and Michael Fischerkeller is a researcher at the Institute for Defense Analyses, where he has experience providing research in support of DoD and the US military. It is more difficult to disentangle the “origins story” of persistent engagement strategy—whether outsiders brought these perspectives into DoD, or their collaboration involved a degree of cross-pollination and co-production. Regardless, the fact of co-development should be acknowledged and presumably it accounts in part for the eventual adoption of persistent engagement as US cyber strategy. These advocates continue to shape the policy-relevant debate about cyber strategy, for example about how to perceive and respond to strategic competition in cyberspace and the need for the US to improve its cyber diplomacy (Goldman, 2020; Harknett 2020; Harknett & Smeets, 2020). Harknett also spent 2017 as the inaugural US-UK Fulbright Scholar in cybersecurity, perhaps representing an initiative of Track 2 cyber diplomacy—complementing already close Track 1 ties between the NSA and its UK counterpart, GCHQ—to improve UK understanding of emerging US thinking about persistent engagement and what it might mean for UK cyber strategy.

Amongst contemporary cyber powers, the US is relatively rare in the existence of this publicly-accessible, policy-relevant debate about cyber strategy sustained in part by those closely associated with the cyber-relevant parts of the US military and intelligence community. Its existence is surely a positive development in public understanding of important developments in US cyber strategy, potentially also helping to reduce the risk, highlighted in the academic literature, of adversaries’ misinterpreting US moves in cyberspace (Jervis, 2016, p. 66).

Leading advocates of persistent engagement theory, such as Fischerkeller and Harknett, have emphasized the flexibility, responsiveness and bespoke development of cyber operations—the antithesis of a crude “Madman Theory” approach (Fischerkeller & Harknett, 2017, p. 390). Fischerkeller
and Harknett argued that: “In an environment of constant contact [in cyberspace], a strategy grounded in persistent engagement is more appropriate than one of operational restraint and reaction for shaping the parameters of acceptable behavior and sustaining and advancing US national interests” (Fischerkeller & Harknett, 2017, p. 381). Harknett in particular has long been associated with criticism of the previous iteration of US cyber strategy.

Harknett’s criticism of US cyber strategy started from the conviction that deterrence theory was not readily applicable to the cyber domain. Although his views evolved, he started with the belief that the cyber domain was characterized by offense dominance, arguing in a coauthored article in 2010 that: “cyberspace is an environment of offense dominance in which deterrence is easily overwhelmed. Therefore, anchoring national security around the goal of avoiding war is a recipe for defeat” (Harknett et al., 2010, p. 2). Developing the intimate connection between defensive and offensive measures in what was to become persistent engagement theory, Harknett and his coauthors argued that: “Basing US national security strategy on a framework fundamentally geared toward prevention will prove disastrous, when the strategic environment requires an attack posture of mitigating damage (defense) and undermining the attack capacity of opponents (offense)” (Harknett et al., 2010, p. 15).

Harknett subsequently developed his views, moving away from the principle of offense-dominance and toward the notion of offense-persistence at the heart of what became persistent engagement theory. He co-wrote an article with Emily Goldman in 2016, arguing that: “cyberspace is a realm of activity in which new security dynamics are at work due to the revolutionary character of digital technology.” They proposed “the organizing principle that cyberspace is an offense-persistent strategic environment” (Harknett & Goldman, 2016, p. 81). Harknett and Goldman explained that “offense-persistence” in cyberspace involved a “continual” contest between offense and defense, one in which “defense is in constant contact with the enemy” (Harknett & Goldman, 2016, p. 86). Harknett and Goldman clarified that offense-persistence should not be equated with the offense-dominance that Harknett had advocated earlier. In the former situation, whilst under constant stress, defenses are resilient, whereas, in the latter, there is an assumption that defenses will ultimately be overcome.

Harknett developed this theory further with Michael Fischerkeller in 2017, arguing that: “In an environment of constant contact, a strategy grounded in persistent engagement is more appropriate than one of operational restraint and reaction for shaping the parameters of acceptable behavior and sustaining and advancing US national interests” (Fischerkeller & Harknett, 2017, p. 381). Fischerkeller and Harknett were clearly
foreshadowing much of what entered official Department of Defense—and specifically Cyber Command’s—statements regarding persistent engagement. They argued that the low cost of entry into cyber operations had led to a crowded field of actors; that many actors adopted a more aggressive posture of operational activities in cyberspace than did the US government; and, that “these actors have recognized that when the time comes for international discourse regarding codification, those who operationally dominate the domain will be in the strongest position to argue for norms supporting their positions” (Fischerkeller & Harknett, 2017, p. 383).

**Putting persistent engagement into practice**

The scholarly literature therefore emphasizes the intellectual hinterland of persistent engagement, founded in an analysis of adversaries’ behavior in cyberspace and an argument about how to address it. It is clear that the eventual shift in strategy by DoD was predicated on agreement with this analysis and its consequent operational prescriptions. For example, General Nakasone regards the year 2013 as “a strategic inflection point” that highlighted the shortcomings of the previous iteration of US cyber strategy. He notes that adversaries have, since then, increased the frequency and potency of their cyber operations against US targets and interests, always calibrating these operations to fall below the threshold of armed conflict, thus requiring a strategic response like persistent engagement:

Examples of their assaults included the Iranian denial-of-service attacks against the financial sector (2012–2013) and attack on the Sands Casino (2014), North Korea’s attack on Sony Pictures Entertainment (2014), and China’s disruption of GitHub (2015) and theft of security-related data from the Office of Personnel Management (2015). Russia raised cyberspace campaigns to a new level of boldness after 2015, launching a series of operations to interfere with the elections of the United States and its allies and sponsoring attacks on the Ukrainian power grid (Nakasone, 2019, p. 11).

What is perhaps interesting about Nakasone’s identification of 2013 as the “inflection point” is that he omits mention of two other events that occurred in a similar timeframe: the revelation that Stuxnet had targeted the Iranian nuclear programme and the separate revelations made by Edward J. Snowden regarding US cyber operations and digital espionage capabilities (Harding, 2014; Harris, 2014; Sanger, 2012; Zetter, 2014). It is not unreasonable to hypothesize that the exposure of the depth and scale of US activities might have catalyzed a shift in the behavior of its adversaries—a shift that persistent engagement then became the chosen strategy to counter. As Healey and Jervis have recently observed: “It is easy, when reading US official documents, to forget that the United States was a predator long before it was prey” (Healey & Jervis, 2020). This self-reflective
A note does not appear to have featured in the internal deliberations of the Trump administration in implementing the shift toward a more assertive cyber strategy. It may, indeed, be a moot point. Whatever the cause of the acceleration and intensification of adversaries’ behavior in cyberspace, persistent engagement is essentially forward-looking. From its assessment of shortcomings in the pre-2018 strategy it proposes an alternative way to achieve better outcomes. As the 2018 Command Vision emphasized, one metric for assessing the effectiveness of the new strategy would be to determine whether or not there was a reduction in the scale, pace and intensity of cyber operations conducted by the most capable state-actor adversaries (US Cyber Command, 2018, p. 6).

Whilst the academic and policy debate formed an influential context for the shift toward persistent engagement strategy in 2018, bureaucratic politics, hiring and firing decisions within the Trump administration also had an impact on how and when that shift took place. Regarding the implementation of that shift on the government side, important appointments included Nakasone’s promotion to become commander of Cyber Command and Director of the NSA, as well as the slightly earlier appointment of John Bolton as Trump’s third successive National Security Adviser. Describing the Trump administration’s cyber strategy in his memoir, Bolton observed that: “establishing cyber deterrence was easier said than done, since almost all the cyber-offensive operations we wanted to undertake necessarily remained classified. So, those directly affected would know they had been hit, but not necessarily by whom unless we told them” (Bolton, 2020, pp. 181–182). Consequently, he felt that: “there had to be some public discussion of our capabilities, to put our adversaries on notice that our years of passivity were over and to reassure our friends that America was on the march in cyberspace” (Bolton, 2020, p. 182). Whilst obviously in keeping with Bolton’s broader approach to national security policy, it is clear that these thoughts (brief though they were) aligned comfortably with preexisting advocacy within and beyond the administration for a more assertive cyber strategy. Bolton’s memoirs provide us with an early account of the bureaucratic politics that helped to turn that advocacy into the reality of a strategic shift.

Describing the inter-agency debate in 2018 about reforming cyber strategy and processes, Bolton observed that: “The interagency process was frozen solid. The Department of Homeland Security and others wanted to keep a stranglehold on the Defense Department, as did the intelligence community. The Pentagon didn’t want oversight from anyone, including the White House, and took an “all or nothing” approach in negotiations that only infuriated everyone else involved” (Bolton, 2020, p. 176). According to Bolton: “We needed not just a law-enforcement response to
international cyber threats, but substantial military and clandestine capabilities as well” (Bolton, 2020, p. 174). Bolton’s reference to clandestine capabilities highlighted a parallel track to Cyber Command, consistent with recent investigative reporting that the Central Intelligence Agency had also been authorized by the Trump administration to conduct covert offensive cyber operations (Dorfman et al., 2020).

Bolton unsurprisingly criticized the Obama administration for pursuing an insufficiently assertive cyber strategy, in so doing indicating that his theory of offensive cyber lies in a more traditional, realist interpretation of deterrence than the persistent engagement theory advocated by Harknett and his coauthors. Bolton explained that: “I didn’t understand why cyberspace should be materially different from the rest of human experience: initially a state of anarchy from which strength and resolve, backed by substantial offensive weaponry, could create structures of deterrence against potential adversaries that would eventually bring peace” (Bolton, 2020, p. 175). Bolton noted in his memoirs that his views were not considered “revolutionary” within the administration as, prior to his appointment as national security adviser, there had been “extensive interagency discussions to change the Obama-era rules governing cyber decision-making” (Bolton, 2020, p. 175). The difference Bolton credits to himself is that, prior to his appointment, the process had reportedly stalled: “bureaucratic inertia, turf fights, and some genuine unresolved issues paralyzed the Trump administration, month after month” (Bolton, 2020, p. 175). It is a matter of record that NSPM-13 was signed in August of 2018, four months after Bolton’s appointment and just three after Nakasone’s promotion to lead Cyber Command, so, whilst the shaping effort preceded Bolton’s arrival in the White House, it is not perhaps without foundation for Bolton to argue that his bureaucratic determination contributed to the delivery of the new process sooner than might otherwise have been the case. At the same time, other decisions in this period might have had unforeseen consequences: eliminating the senior White House cyber coordinator and homeland security advisor roles in 2018 arguably impaired the administration’s ability to respond coherently to the 2020 SolarWinds breach (Greenberg, 2020; Perlroth & Sanger, 2018).

The inapplicability of “Madman Theory” to persistent engagement

The inapplicability of “Madman Theory” to persistent engagement is demonstrated by this historical record of the scholarly and policy debates about the strategy that pre-dated by several years the evolution of US cyber strategy and the related reform of the authorization process under the Trump administration. It is also clear, from a review of the operational record to
date based on openly-available sources (with all the caveats that implies about limited public understanding in conditions of operational secrecy), that the strategy of persistent engagement is not premised in the theatrical gestures, signaling of extreme preferences, or deviation from rational consequences-based decision-making that are signature themes of “Madman tactics.” By devolving greater operational autonomy to Cyber Command, persistent engagement actually put more distance between offensive cyber operations and Trump’s mercurial, unpredictable social-media outbursts. The clarity, consistency and coherence of Nakasone’s communication about the new strategy were arguably antithetical to the “Madman theory.” Arguably, a true application of “Madman theory” would have been for Trump to retain the Obama-era process, tightly-focused on decisions made by the president, interpreting it in his inimitably unpredictable manner.

Furthermore, it is doubtful that the more assertive turn in specific cyber operations during the Trump presidency actually led to operations that would have provoked any sense of extreme, unpredictable US behavior in the minds of the targeted adversaries. On the contrary, all the operations that have so far made it into the public domain have been specific, limited and clearly intended to be interpreted as a signal that the US government was reacting to a particular act or pattern of behavior that it wanted to punish or deter. There is also a significant extent to which the cyber domain is an inappropriate arena for the application of Madman Theory and its connotation of total destruction. As a matter of historical observation, most cyber operations have inflicted degradation and recoverable damage, akin to a “cyber-skirmish” rather than a massive blow analogous to a nuclear strike (Betz & Stevens, 2011, p. 97; Devanny, 2020; Dipert, 2010, p. 403; Martin, 2020).

The use of cyber operations by the Trump administration was certainly more assertive than under the Obama administration, but that use was still constrained within the bounds of a calibrated pursuit of signaling, behavior- and norm-shaping effects (Buchanan, 2020; Egloff & Maschmeyer, 2020). These activities ranged from the discrete and limited operations in 2018 against Russian disinformation infrastructure to more recent operations that aimed to degrade similar infrastructure, as well as relatively trivial “trolling” of Russian and Chinese government cyber operators by portraying them irreverently as animal cartoons in Cyber Command’s publications (Vavra, 2020). Put simply, if the Trump administration had intended to craft persistent engagement as the cyber element of a wider “Madman” strategy, senior figures in the administration would have proceeded to communicate differently about that strategy and would have implemented it in a less limited, more provocative manner. The reported use of cyber operations as part of the US response to Iranian provocation
in 2019 indicates, if anything, that the cyber instrument was used in a manner that might have actually reduced the potential for escalation (Barnes & Gibbons-Neff, 2019).

**Alternative criticism of persistent engagement**

Whilst his parallel with “Madman Theory” was not well-founded, Boussios was not wrong to highlight the potentially adverse consequences of the more assertive turn in US cyber strategy. Prominent critics, such as Jason Healey and Alexander Klimburg, have argued that its impact will be to intensify and escalate cyber competition between states, unless it is executed with considerable strategic subtlety and consistency (Healey, 2019, p. 2; Klimburg, 2020, p. 123). Healey observes the magnitude of the challenge that persistent engagement sets itself: to “simultaneously limit escalation and lock in US superiority” on the assumption that “the USA can have both superiority and overmatch as well as stability” (Healey, 2019, pp. 5, 6–7). Healey is particularly concerned about the potential system effects if adversaries reject the US objective of maintaining superiority in the cyber domain. He speculates about whether persistent engagement might instigate a cyber arms race between the US and its adversaries (Healey, 2019, p. 10). This is, of course, a counterfactual, and advocates of persistent engagement would, understandably, reply that the dynamic of competition to improve capabilities and achieve cumulative strategic effects was happening anyway, with the US laboring under a disadvantageous strategy (Harknett & Smeets, 2020)—and, indeed, that this formed an important part of their argument against the precursor strategy of restraint and reaction, on the basis that it was undermining US efforts to compete. This would indeed form part of Harknett’s subsequent effort to vindicate persistent engagement in response to the SolarWinds breach (Harknet, 2020). Given its essentially counterfactual nature, this is an argument that is likely to run and run, but highly unlikely to generate convergence on a shared analysis—indeed, even if the period of persistent engagement’s introduction saw a sharp reduction in the cyber operations of the most capable hostile state-actors, this should not, in itself, be taken immediately as evidence that persistent engagement had succeeded, given the possibility that other factors could have accounted for the relevant operational developments.

Healey and Robert Jervis have explored the impact of cyber capabilities on crisis stability, arguing that such impact is highly situational (Healey & Jervis, 2020). They emphasize the inherent uncertainty of the domain, the potential for miscalculation, and difficulty determining whether or not a chosen strategy is effective: “Because of compartmentalized knowledge, there are few who know what punches a country is taking, which it is
throwing, and the causal relationship between the two” (Healey & Jervis, 2020). Similarly, with Stuart Caudill, Healey has highlighted the implementa-
tional challenge implicit in persistent engagement, requiring as it does not only sufficient military capabilities and leadership, but also clear signal-
ing, the trust of partners, and a well-functioning interagency process (Healey & Caudill, 2020, p. 9).

As the recently-retired head of the U.K. National Cyber Security Center, Ciaran Martin, has observed, the development of formidable cyber capabil-
ities entails another risk, namely the consequences if these capabilities are lost and repurposed by other actors to perpetrate attacks of their own, as indeed happened in the case of exploits lost by the NSA that were subse-
quently used in cybercrime campaigns such as WannaCry (Martin, 2020). The repurposing for criminal ends of cyber capabilities developed within
the US intelligence community is not, strictly speaking, an argument against the strategy of persistent engagement. This is, rather, a risk posed by the development, stockpiling and operational use of these capabilities pursuant to any strategy. Decisions about the structure, posture and missions of US cyber forces are inherently political. They reflect an administra-
tion’s appetite for risk; its prioritization of strategic objectives; and its understanding of the complex system effects that might follow from opera-
tions conducted to achieve those objectives. The escalatory potential of per-
sistent engagement strategy could be determined in part by the administra-
tion’s decision about whether and to what extent to pursue counterforce (military and security) and countervalue (civilian infrastruc-
ture) targeting options (Devanny, 2020). The careful calibration and tacit bargaining envisaged by persistent engagement’s proponents is arguably easier to achieve if confined to counterforce targeting, but, as the strategy’s advocates correctly highlight, US adversaries have pursued countervalue targeting by penetrating civilian infrastructure such as energy networks.

The logic of persistent engagement in practice appears to be that the US should accept some degree of targeting symmetry in order to achieve intended effects in changing adversaries’ behavior. For example, efforts to reduce the number of adversarial penetrations of US civilian infrastructure appear to have involved demonstration of a reciprocal US capability to penetrate adversaries’ civilian infrastructure. This is a disturbing develop-
ment in this highly-networked, digital age. An alternative target-selection policy, still consistent with the principles of persistent engagement strategy, would be to try to achieve the same objectives by focusing solely on coun-
terforce targeting. This alternative, imposing the tactical friction and stra-
tegic costs on adversaries that was emphasized as a major priority in the 2018 Command Vision, could be achieved by penetrating, manipulating, degrading or destroying the infrastructure used by the military and other
cyber operators of adversary nations and their proxies. Consistent with the central logic of persistent engagement, this would not only force adversaries to invest more in defending their operational infrastructure, but would also aim to reduce the cost effectiveness and operational impact of their offensive investments. Embracing the theme of the operations to protect the 2018 midterm elections, this approach would also include publicly indicting the operatives tasked with conducting adversaries’ offensive cyber operations, with the aim of reducing the pipeline of talent attracted to this career path. All this might succeed in imposing higher—and precisely targeted—costs, sufficient to restrain the behavior of adversaries without exacerbating the contemporary competition between state and non-state actors to further compromise the integrity and functioning of critical civilian infrastructure. This narrower, but potentially no less assertive variant of persistent engagement might ultimately reduce the entrenchment and even reverse the apparently inexorably emerging norm of developing cyber capabilities to target civilian infrastructure.

**Presidential transition politics and US cyber strategy**

Madman tactics do not need to be consciously and carefully executed to produce favorable outcomes in individual instances—madmen can be lucky too. But for the description of madman tactics to be applied credibly to Trump’s cyber strategy, there does need to be something extra, beyond juxtaposition of Trump’s erratic behavior and the assertive turn in cyber strategy under his administration. This juxtaposition never appeared to be more than circumstantial, reflecting tensions between Trump’s personal idiosyncrasies and political priorities and the strategic thinking about cyber that had developed elsewhere in the administration. If anything, the coherence and integrity of US cyber strategy was itself a victim of Trump’s madman tactics. This became increasingly clear in the months immediately following Trump’s presidential election defeat.

**The “stolen election” narrative and post-election personnel changes**

In the final days of his administration, instead of conceding defeat to Joe Biden, Trump systematically cast doubt on the integrity of the electoral process - leading to the extraordinary and violent events at the Capitol on January 6, 2021. Trump repeatedly cited unsubstantiated claims of fraud and pursued a series of failed legal challenges in multiple states. These post-election tactics also led to further evidence that Trump’s idiosyncratic behavior was not calibrated to enhance the effectiveness of national cyber strategy. In three cases, Trump’s behavior appeared to conflict with the
effective implementation of US cyber strategy. First, on November 18 Trump subjected Christopher Krebs, then the director of the Cybersecurity and Infrastructure Security Agency (CISA), to the ordeal of fire-by-tweet. Trump claimed his justification was that Krebs had made “highly inaccurate” claims by expressing confidence in the security of the very electoral process that Trump was determined to undermine as compromised by “massive improprieties and fraud” (Trump, 2020a, 2020b).

Trump’s dismissal of Krebs from CISA had been anticipated following Trump’s election defeat. The Trump White House had reportedly been angered by CISA’s “Rumor Control” website that had debunked election misinformation during the campaign and had refused to revise or delete accurate information when asked to do so by the White House (Bing et al., 2020). Insofar as countering online mis- and dis-information aimed at undermining the democratic process is an important strand of national cyber strategy, Trump’s decision to dismiss Krebs was antithetical to that mission.

In addition to Krebs’s dismissal, CISA’s deputy and assistant director both resigned in the weeks immediately after the election. The removal of CISA’s senior leadership mirrored the administration’s wider effort to replace senior leaders from other departments with acting appointees between the election and Biden’s inauguration, including the top officials in the Departments of Defense and Justice. This approach was consistent with Trump’s pattern of using acting appointees to replace senate-confirmed appointments throughout his administration (Taylor, 2020). The post-election moves drew particular criticism, however, because they occurred during a controversial period in which Trump had refused to concede defeat to Biden and was amplifying unsubstantiated claims of election fraud. Trump’s post-election personnel changes at the Pentagon had reportedly “prompted alarm among some officials that the administration would use its final days to carry out proposals that defy the advice of military officials” (Nakashima & Ryan, 2020). None of this was evidence of a cultivation of madman tactics against foreign adversaries in US cyber strategy. It suggested an administration at war with itself, as the defeated president lashed out against officials and institutions he deemed insufficiently loyal or on-message as he propagated a “stolen election” narrative.

**The Trump administration’s response to the SolarWinds breach**

The second example of this post-election collision between Trump’s personal political imperatives and the execution of US cyber strategy occurred barely one month later, when Trump’s focus on pursuing his electoral fraud narrative undermined the national response to a major incident of
cyber espionage. This cyber campaign was reportedly conducted by hackers associated with the Russian foreign intelligence service, the *Sluzhba Vneshney Razvedki* (SVR), specifically the advanced persistent threat (APT) actor known as APT29 or Cozy Bear (Nakashima & Timberg, 2020). The espionage campaign had affected at least half a dozen US federal agencies and departments as a result of an exploited supply-chain vulnerability in widely-used IT administration software produced by the company SolarWinds (Bing, 2020a).

On December 8, the US cybersecurity company FireEye announced that it had been the victim of a major hacking incident, most probably the work of a state actor. The FireEye breach had reportedly led to the theft of some of the company’s “red team” hacking tools (Bing & Menn, 2020). Just five days later, on December 13, it became clear that FireEye had not been the only victim of this major hacking incident. Reuters reported, without initially connecting it to the FireEye incident, that hackers had successfully gained access to the internal email of the US Treasury and Commerce Departments (Bing, 2020a). The hack reportedly compromised an email system used by the Treasury Department’s most senior officials, albeit with no indication that this access extended to more highly-classified systems (Sanger & Rappeport, 2020). Reporting subsequently established that the hacking campaign extended to at least half a dozen federal agencies and departments, including the Departments of State, Energy and Homeland Security, and the National Institutes of Health, as well as other enterprise networks at state and local levels of government, critical infrastructure operators and associated supply-chain companies, and thousands of other private companies worldwide (Bing et al., 2020; Nakashima & Ryan, 2020; Satter, 2020; Timberg & Nakashima, 2020b; Zetter, 2020).

The very dominance of a software company in its market, such as SolarWinds’ network management products, can be exploited as a liability and a potential vector for digital espionage campaigns (Satter, Bing & Menn, 2020). Supply-chain software vulnerabilities are highly-prized vectors for digital espionage and this was particularly evident in the case of SolarWinds, which was reportedly subject to two separate malware compromises of its Orion software (Bing, 2020b). The SolarWinds hack was also sufficiently novel and ingenious that it evaded (the, in retrospect, perhaps not-so-smartly named) Einstein, CISA’s defensive system that monitored government networks for evidence of known malware (Timberg & Nakashima, 2020a).

The Trump administration’s public statements about the SolarWinds breach were slow, disorganized and undermined by Trump’s own remarks on Twitter. In fact, they were also preempted by Biden’s transition team. Before Trump or any other senior official had commented on the
SolarWinds breach, the Biden-Harris transition released a statement pledging, once in office, to elevate the priority of cybersecurity across government, improve collaboration with the private sector and enhance resilience against what it called “malicious cyber attacks” (Biden-Harris Transition 2020). The Biden-Harris statement then pivoted into language mirroring the defend forward strategy, emphasizing that “a good defense isn’t enough” and that disruption and deterrence were also needed, including by cost-imposition and coordinated action with allies (Biden-Harris Transition 2020).

The next day (December 18)—five days after the first public report of the breach of Treasury and Commerce Department networks—Secretary of State Mike Pompeo became the most senior US official to publicly state that Russia was most likely responsible for the incident (Fedor, 2020). The same day as Pompeo’s remarks, White House officials had reportedly prepared a similar statement attributing the hack to Russia, but did not publish it after being ordered to stand down (Bing & Landay, 2020). Furthermore, the following day Trump used his Twitter account to cast doubt on Russian responsibility for the hack. Trump tweeted that: “Russia, Russia, Russia is the priority chant when anything happens because Lamestream is, for mostly financial reasons, petrified of discussing the possibility that it may be China (it may!)” (Trump, 2020c, 2020d). Trump also connected the SolarWinds hack with his wider post-election narrative about his defeat being attributable to fraud (Trump, 2020d).

Washington Post reporters Ellen Nakashima and Josh Dawsey noted that Trump’s outburst followed an established pattern of his presidency: “Trump’s aversion to calling out the Kremlin for its malign activities in cyberspace and his deference to Russian President Vladimir Putin has become a hallmark of his presidency. He has repeatedly trusted the word of Putin over the assessments of his own intelligence community, including its conclusion that Russia waged a sophisticated campaign to interfere in the 2016 presidential election—a verdict Trump believes calls into question the legitimacy of his victory four years ago” (Nakashima & Dawsey, 2020). Nakashima and Dawsey also quoted former senior US intelligence official Gregory F. Treverton as describing—in extraordinary terms—Trump’s behavior on issues related to Russia, as less an instance of madness than that Trump: “behaves so much like a paid Russian agent…If you look at the string of his actions and pronouncements…the only consistent interpretation that you can logically draw is that he’s in their thrall” (Nakashima & Dawsey, 2020). Given the salience of the Russian cyber threat, Trump’s persistent failure to take it seriously must count as further
evidence against the claim that the administration uniformly pursued a coherent, consistent and well-calibrated cyber strategy.

**SolarWinds and calls to separate the NSA-Cyber Command “double-hatted” leadership**

The third example of tensions in US cyber policies during the late Trump era also occurred in the wake of the SolarWinds hack. It was widely reported that Trump would continue to use the final month before Biden’s inauguration to make consequential decisions about senior cyber personnel and reorganizing cyber-relevant institutions, including separating the “dual hatted” command of the NSA and Cyber Command (Bing, 2020c). Critics of this last proposal expressed concern at the prospect of a Trump loyalist being appointed as the civilian head of NSA and also at the potential disruption such a reorganization would entail at a time when the federal government was coordinating its response to the SolarWinds incident (Nakashima & Ryan, 2020). This followed earlier concern that the administration was trying to “burrow” a political loyalist into the senior civil service post of NSA General Counsel (Hennessey, 2020).

Whilst there were and remain valid reasons in principle to support the separation of NSA and Cyber Command, there was a widespread sense that this was a premature move that failed to satisfy the requirements mandated by Congress for Cyber Command to be able to demonstrate full operating capability independent of the NSA before the separation could take place (Chesney, 2020). In this context, the move appeared hasty and political. As Brandon Valeriano concluded in his critical appraisal of Trump’s cybersecurity legacy: “While there is merit to the idea, completing the massive task on the way out the door, in the middle of the massive fallout from the SolarWinds incident, complicates the ability of President-Elect Biden to organize cybersecurity defenses” (Valeriano, 2020). This episode highlighted ill-conceived efforts by the Trump administration to pursue institutional reforms in the wake of the SolarWinds breach and before leaving office, but it is necessary to conclude with an assessment of the overall implications of the breach for US cyber strategy.

**The implications of the SolarWinds breach for US cyber strategy**

The initial debate following the SolarWinds revelation, as the scale of the compromise of federal targets became increasingly clear, encompassed disagreements about whether the operation was simply a case of “espionage as usual” or instead represented an attack on the United States (Smith, 2020). Others speculated about the implications of the SolarWinds breach for the
effectiveness of US cyber strategy (Goldsmith, 2020; Harknett 2020; Lawson & Valeriano, 2020). Pursuing the latter issue, Jack Goldsmith connected the successful breach with a critique of the efficacy of US cyber strategy, suggesting that a posture of greater restraint might ultimately be more effective in reducing the frequency and intensity of adversary cyber operations (Goldsmith, 2020). Another reason for pursuing a relatively restrained response to the SolarWinds breach was offered by Herb Lin, who noted that the US government was not without blame in this field: “The U.S. has conducted and continues to conduct a host of activities in cyberspace against other nations that, were they done to the U.S., would prompt outrage and anger” (Lin, 2020). Accordingly: “Given the United States’s past actions and its publicly documented intentions in cyberspace, the U.S. could risk severe escalation if it goes much further in response to the SolarWinds breach” (Lin, 2020).

In stark contrast, prominent advocates of persistent engagement such as Harknett argued that SolarWinds should be perceived as evidence that the US “must accelerate” its adoption and implementation of the existing strategy—the breach demonstrated the reality of persistent engagement in cyberspace and the US must therefore embrace the existing strategy because it takes this competition seriously (Harknett 2020). As such, the SolarWinds breach, notwithstanding its magnitude and the hyperbole of some of the surrounding commentary, provided little more than a new talking point for engaged participants in the strategic debate. Initially at least, it was consistently interpreted in line with preexisting viewpoints. Its medium term significance appeared less likely to emerge in a shift in this strategic debate than in its shaping of the political context in which strategic choices would be made by the incoming Biden administration.

Attentive to both this strategic debate and the threat-inflating vocabulary employed by some commentators, Sean Lawson and Brandon Valeriano rightly criticized the dangerous and distortive effects of “doomsday rhetoric” and the description of real or imagined threats as a “cyber Pearl Harbour” (Lawson & Valeriano, 2020). One US senator had described the SolarWinds hack as “virtually a declaration of war” and another declared: “America must retaliate, and not just with sanctions” (Bing et al., 2020). In a public intervention, the president of Microsoft, Brad Smith, described the SolarWinds campaign as “the world’s latest serious nation-state cyberattack…effectively an attack on the United States and its government and other critical institutions, including security firms” (Smith, 2020). Against this hyperbole, Lawson and Valeriano argued plausibly that the SolarWinds incident was not “the arrival of digital apocalypse” but was rather “another major incident of cyber espionage” (Lawson & Valeriano, 2020).
On one issue, however, Lawson and Valeriano’s analysis was less immediately persuasive, arguing that: “being distracted by the possibility of a major hack during the 2020 election led to a comprehensive violation of almost every government agency” (Lawson & Valeriano, 2020). This framing of the problem implies a direct causal link between the US investment of time and resources into defending the election from cyber threats and the failure to identify the SolarWinds breach before it had achieved successful penetration of multiple US government and other targets. It is arguably unfair to judge the effectiveness of US strategy on the basis of (the admittedly embarrassing success of) one high-profile espionage campaign. Inter-state espionage is a practice with hundreds of years of history. Reducing espionage to zero is not a feasible objective for US cyber strategy. That does not, of course, mean that it should be a consequence-free endeavor—in the words of former Obama administration State Department cyber coordinator Chris Painter, the US should not be expected to “sit still for it and say ‘good job’” (Nakashima & Timberg, 2020). As bad as the SolarWinds campaign incontestably was, it is worthwhile to note that what appeared to be a time-consuming and sophisticated espionage campaign potentially only had an active, intelligence-producing life-span of less than one year before it was reportedly first identified. Even if its perpetrators are able—as they well might be—to sustain intelligence collection into 2021 on at least some of the infected networks by relying on resilient access, it is reasonable to conclude that the peak of the operation was before the first press revelations of December 13. Cumulatively, the episode demonstrates both the significant espionage value of successful supply-chain vulnerabilityexploitation and the fragility and potential brevity of such operations—notwithstanding the reported longevity of other supply-chain attacks, such as the decades-long US compromise of the cryptography provider Crypto AG (Miller, 2020). This should not distract, of course, from the other negative consequences of the operation in the form of disruption, distrust and displaced effort over a long period of time as the breach of federal and other networks is remediated—all of which have rightly been identified as additional costs inflicted by the operation (Harknett, 2020).

The post-Trump prospects for persistent engagement

These post-election developments highlighted the fraught intra-administration politics of the Trump presidency’s cyber strategy, especially the adverse impact of the White House. Some commentators reflected that Trump’s “inattention to and ignorance of cyber issues” had led to a “surprisingly mixed bag” because, in the absence of active management from the White House, the president had decided: “to empower and then largely ignore
leaders at agencies like CISA, the NSA, and Cyber Command, allowing them to carry out aggressive new tactics that often were effective, if uncoordinated” (Greenberg, 2020). On this basis, some argued that the Biden administration should not reject entirely the legacy of the previous four years and should instead build from the starting point of “some things that the Trump administration unintentionally did correct” (Greenberg, 2020). This is hardly a strong endorsement of an executive incurious about details and content to adopt a laissez-faire approach to managing subordinate officials. There was an even worse aspect of the Trump administration’s management of cyber strategy, namely the extent to which Trump’s self-serving political agenda came into conflict with the personnel, institutions and strategic preferences of the US cyber defense and cybersecurity establishments.

The disconnect between presidential priorities and broader administration cyber strategy resulted in friction that impaired the coherence and active management of the US government’s response to the SolarWinds breach. This was clear even before Trump’s spate of post-election changes in senior positions, for example in the elimination of senior cyber-focused White House advisory roles in 2018 that appeared to reduce executive bandwidth to deal with an eventuality like the SolarWinds breach. Rather than mitigate this deficiency, Trump actually exacerbated it by firing Krebs and pursuing premature institutional reforms before Biden’s inauguration, such as re-floating the separation of NSA and Cyber Command. These post-election issues perpetuated the impression of a White House less interested in effective government than in punishing perceived disloyalty—and arguably in trying to tie the Biden administration up in knots before it had even taken office. They did not appear, however, to represent a significant threat to the established direction of national cyber strategy, even though the SolarWinds breach in particular had intensified preexistent debates about whether that strategy was fit for purpose.

**Conclusion**

President Trump’s irascible and temperamental behavior, particularly his Twitter activity, was a signature feature of his administration. Seitz and Talmadge have argued persuasively that there is evidence of failed “madman tactics” at work in some of Trump’s foreign policy efforts (Seitz & Talmadge, 2020). Trump’s behavior led directly to significant turnover in senior staff throughout his administration, including in the months after his election defeat to Joe Biden (Baldor, 2020; Miroff & Nakashima, 2020). It also led some commentators to fear longer term damage to the norms associated with the office of the presidency (Hennessey & Wittes, 2020). It is, however, questionable to what extent, if any, a direct line can be drawn
between Trump’s evident idiosyncrasies—what the political scientist and commentator Daniel Drezner has coined as Trump’s “Toddler-in-Chief” tendencies (Drezner, 2020)—and a conscious, coherent strategy to employ this well-deserved reputation to produce strategic effects in the cyber domain.

Situated properly in its historical context, the shift in US cyber strategy between the Obama and Trump administrations should be seen as the result of a longer term evolution of strategic thinking within and beyond the US government about the appropriate role of offensive cyber operations within the totality of US strategy (Graff, 2020; Harris, 2014). This evolution was precipitated and accelerated by an interpretation of adversaries’ behavior in cyberspace, which generated a perception that the Obama-era strategy was not fit for purpose. By incorporating relevant contextual analysis, this article argues that the evolution of US cyber strategy under the Trump administration was also more nuanced and carefully calibrated than is implied by efforts to associate it with notions of “Madman Theory.” Indeed, arguably the biggest victim of Trump’s unpredictability in this context was the coherence and efficacy of US cyber strategy, undermined by Trump’s dismissal of senior officials and particularly during the “stolen election” phase prior to Biden’s inauguration.

The Biden administration’s choices will determine whether the future implementation of persistent engagement strategy leads to severe system effects, particularly if it provoked patterns of escalating activity between adversaries and the US government, and especially if it exacerbated the apparent turn toward cyber targeting of civilian infrastructure. Under a Biden presidency, there is reason to hope that the strategy will be subject to more prudent and focused executive direction. Certainly, in the context of more restrained executive rhetoric there will be even less justice in implying that the strategy has connotations of “Madman Theory.” As far as possible, the new administration should reduce uncertainty and potential for misperception, improve the coherence between senior civilian and military statements about the strategy, and pursue an evidence-led approach to assessing its effectiveness and determining how to proceed in its next phase.

**Disclosure statement**

No potential conflict of interest was reported by the author(s).

**ORCID**

Joe Devanny [http://orcid.org/0000-0001-6031-2397](http://orcid.org/0000-0001-6031-2397)
References

Baldor, L. C. (2020, November 11). Trump loyalists get top Pentagon jobs after Esper firing. Washington Post. https://www.washingtonpost.com/world/national-security/trump-loyalists-get-top-pentagon-jobs-after-esper-firing/2020/11/10/9287323c-23b2-11eb-9c4a-0dc6242c4814_story.html

Barnes, J. E. (2018, October 23). US begins first Cyberoperation against Russia Aimed at protecting elections. New York Times. https://www.nytimes.com/2018/10/23/us/politics/russian-hacking-usa-cyber-command.html

Barnes, J. E., & Gibbons-Neff, T. (2019, June 22). US carried out cyberattacks on Iran. New York Times. https://www.nytimes.com/2019/06/22/us/politics/us-iran-cyber-attacks.html

Betz, D., & Stevens, T. (2011). Cyberspace and the State: Toward a strategy for cyber-power. Routledge for the International Institute for Strategic Studies.

Biden-Harris Transition. (2020, December 17). Statement by president-elect joe biden on cybersecurity. https://buildbackbetter.gov/press-releases/statement-by-president-elect-joe-biden-on-cybersecurity/

Bing, C. (2020a, December 13). EXCLUSIVE-Hackers spied on U.S. Treasury emails for a foreign government – sources. Reuters. https://uk.reuters.com/article/usa-cyber-treasury/exclusive-hackers-spied-on-u-s-treasury-emails-for-a-foreign-government-sources-idUSL1N2IT0KK

Bing, C. (2020b, December 19). Second hacking team was targeting SolarWinds at time of big breach. Reuters. https://uk.reuters.com/article/us-usa-cyber-solarwinds/second-hacking-team-was-targeting-solarwinds-at-time-of-big-breach-idUKKBN28T0U1

Bing, C. (2020c, December 19). Congress, experts worry about potential spy agency reorganization amid hack response. Reuters. https://uk.reuters.com/article/uk-usa-cyber-nsa/congress-experts-worry-about-potential-spy-agency-reorganization-amid-hack-response-idUKKBN28T100

Bing, C., & Landay, J. (2020, December 19). Trump downplays impact of massive hacking, questions Russia involvement. Reuters. https://uk.reuters.com/article/uk-u-s-cyber-breach/trump-downplays-impact-of-massive-hacking-questions-russia-involvement-idUKKBN28T0QI

Bing, C., & Menn, J. (2020, December 8). U.S. cybersecurity firm FireEye discloses breach, theft of hacking tools. Reuters. https://uk.reuters.com/article/fireeye-cyber-u-s-cybersecurity-firm-fireeye-discloses-breach-theft-of-hacking-tools-idUKKBN28I34H

Bing, C., Menn, J., & Satter, R. (2020, November12). Exclusive: Top official on U.S. election cybersecurity tells associates he expects to be fired. Reuters. https://www.reuters.com/article/us-usa-cyber-officials-exclusive-idUSKBN27S2YI

Bing, C., Menn, J., Satter, R., & Stubbs, J. (2020, December 19). ‘Powerful tradecraft’: How foreign cyber-spies compromised America. Reuters. https://uk.reuters.com/article/uk-global-cyber-usa-insight/powerful-tradecraft-how-foreign-cyber-spies-compromised-america-idUKKBN28T0XX?utm_medium=email&utm_source=USD&utm_campaign=Global&utm_term=US

Bolton, J. R. (2020). The room where it happened: A white house memoir. Simon & Schuster.

Boussios, E. G. (2020). Hacking back: Trump’s ‘Madman Theory’ approach to cybersecurity. Journal of Applied Security Research. https://doi.org/10.1080/19361610.2020.1832860

Buchanan, B. (2020). The Hacker and the State: Cyber attacks and the new normal of geopolitics. Harvard University Press.

Cammaerts, B. (2020). The neo-fascist discourse and its normalisation through mediation. Journal of Multicultural Discourses, 15(3), 241–256. https://doi.org/10.1080/17447143.2020.1743296
Chesney, R. (2020, December 20). Ending the ‘Dual-Hat’ arrangement for NSA and cyber command? Lawfare. https://www.lawfareblog.com/ending-dual-hat-arrangement-nsa-and-cyber-command

Cooper, A. F. (2019). The disintermediation Dilemma and its impact on diplomacy: A research agenda for Turbulent Times. Diplomacy & Statecraft, 30(4), 799–807.

Devanny, J. (2020, December 3). The ethics of offensive cyber operations. Foreign Policy Centre. https://fpc.org.uk/the-ethics-of-offensive-cyber-operations/

Dipert, R. R. (2010). The ethics of cyberwarfare. Journal of Military Ethics, 9(4), 384–410. https://doi.org/10.1080/15027570.2010.536404

Dorfman, Z., Zetter, J., McLaughlin, K., & Naylor, S. D. (2020, July). Exclusive: Secret Trump order gives CIA more powers to launch cyberattacks. Yahoo News. https://news.yahoo.com/secret-trump-order-gives-cia-more-powers-to-launch-cyberattacks-090015219.html

Drezner, D. W. (2020). The Toddler in Chief: What Donald Trump teaches Us about the Modern Presidency. University of Chicago Press.

Egloff, F. J., & Maschmeyer, L. (2020). Shaping not signaling: Understanding cyber operations as a means of espionage, attack, and destabilization. International Studies Review, viaa086. https://doi.org/10.1093/isr/viaa086

Fedor, L. (2020, December 19). Trump contradicts officials by playing down cyber attack. Financial Times. https://www.ft.com/content/a05889b5-e802-4da1-b8f6-2ab7b8ca2567

Fischerkeller, M. P., & Harknett, R. J. (2017). Deterrence is not a credible strategy for cyberspace. Orbis, 61(3), 381–393. https://doi.org/10.1016/j.orbis.2017.05.003

Goldman, E. O. (2020). From reaction to action: Adopting a competitive posture in cyber diplomacy. Texas National Security Review, Fall. https://tnsr.org/2020/09/from-reaction-to-action-adopting-a-competitive-posture-in-cyber-diplomacy/

Goldsmith, J. (2020, December 14). Quick thoughts on the Russia Hack. Lawfare. https://www.lawfareblog.com/quick-thoughts-russia-hack

Goodin, D. (2019, June 17). Russia warns of “cyberwar” following report the US attacked its power grid. Ars Technica. https://arstechnica.com/information-technology/2019/06/russia-warns-that-reported-us-attacks-on-its-power-grid-could-trigger-cyberwar/

Graff, G. M. (2020, October 13). The man who speaks softly – and Commands a Big Cyber Army. Wired. https://www.wired.com/story/general-paul-nakasone-cyber-command-nsa/

Gray, C. S. (2013). Making sense of cyber power: Why the sky is not falling. Strategic Studies Institute, US Army War College.

Greenberg, A. (2020, December 23). 2020 Shows the Danger of a Decapitated Cyber Regime. Wired. https://www.wired.com/story/2020-shows-danger-decapitated-cyber-regime/

Haldeman, H. R., with DiMona, J. (1978). The ends of power. Times Books.

Harding, L. (2014). The snowden files: The inside story of the World’s Most Wanted Man. Guardian Faber Publishing.

Harknett, R. J. (2020, March 23). Progress is the promise in National Cybersecurity Strategy. Lawfare. https://www.lawfareblog.com/progress-promise-national-cybersecurity-strategy

Harknett, R. J. (2020, December 23). SolarWinds: The need for Persistent Engagement. Lawfare. https://www.lawfareblog.com/solarwinds-need-persistent-engagement

Harknett, R. J., & Goldman, E. O. (2016). The search for cyber fundamentals. Journal of Information Warfare, 15(2), 81–88.

Harknett, R. J., Callaghan, J. P., & Kauffman, R. (2010). Leaving deterrence behind: War fighting and national cybersecurity. Journal of Homeland Security and Emergency Management, 7(1), 1–24. https://doi.org/10.2202/1547-7355.1636
Harknett, R. J., & Smeets, M. (2020). Cyber campaigns and strategic outcomes. *Journal of Strategic Studies*. https://doi.org/10.1080/01402390.2020.1732354

Harris, S. (2014). *@war: The rise of the Military-Internet Complex*. Houghton Mifflin Harcourt.

Healey, J. (2019). The implications of persistent (and permanent) engagement in cyberspace. *Journal of Cybersecurity*, 5(1), 1–15. https://doi.org/10.1093/cybsec/tyz008

Healey, J., & Jervis, R. (2020). The escalation inversion and other oddities of situational Cyber Stability. *Texas National Security Review*, Fall. https://tnsr.org/2020/09/the-escalation-inversion-and-other-oddities-of-situational-cyber-stability/

Healey, J., & Caudill, S. (2020). Success of Persistent Engagement in Cyberspace. *Strategic Studies Quarterly*, 14(1), 9–15.

Hennessey, S. (2020, November 13). How did a Trump loyalist come to be named NSA General Counsel—And What Should Biden Do About It? *Lawfare*. https://www.lawfareblog.com/how-did-trump-loyalist-come-be-named-nsa-general-counsel-and-what-should-biden-do-about-it

Hennessey, S., & Wittes, B. (2020). *Unmaking the Presidency: Donald Trump’s War on the World’s Most Powerful Office*. Farrar, Straus and Giroux.

Jervis, R. (2016). Some thoughts on deterrence in the Cyber Era. *Journal of Information Warfare*, 15(2), 66–73.

Klimburg, A. (2020). Mixed signals: A flawed approach to Cyber Deterrence. *Survival*, 62(1), 107–130. https://doi.org/10.1080/00396338.2020.1715071

Lawson, S., & Valeriano, B. (2020, December 18). The Russian ‘Cyber Pearl Harbor’ that wasn’t. *The American Conservative*. https://www.theamericanconservative.com/articles/the-russian-cyber-pearl-harbor-that-wasnt/

Lin, H. (2020, December 22). Reflections on the SolarWinds Breach. *Lawfare*, http://www.lawfareblog.com/reflections-solarwinds-breach.

Martin, C. (2020, November). Cyber-weapons are called viruses for a reason: Statecraft and security in the digital age. *King’s College London*. https://thestrandgroup.kcl.ac.uk/event/ciaran-martin-cyber-weapons-are-called-viruses-for-a-reason-statecraft-security-and-safety-in-the-digital-age/

McManus, R. W. (2019). Revisiting the Madman Theory: Evaluating the impact of different forms of perceived madness in coercive bargaining. *Security Studies*, 28(5), 976–1009. https://doi.org/10.1080/09636412.2019.1662482

Menn, J., & Bing, C. (2020, December 18). Trump fires top U.S. election cybersecurity official who defended vote. *Reuters*. https://uk.reuters.com/article/uk-usa-election-trump-krebs/trump-fires-top-u-s-election-cybersecurity-official-who-defended-vote-idUKKBN27Y01A

Miller, G. (2020, February 11). The intelligence coup of the century. *Washington Post*. https://www.washingtonpost.com/graphics/2020/world/national-security/cia-crypto-encryption-machines-espionage/

Miroff, N., & Nakashima, E. (2020, November 13). Two senior Homeland Security officials forced out as White House firings widen. *Washington Post*. https://www.washingtonpost.com/national/dhs-officials-fired-white-house/2020/11/12/98fddf24-2554-11eb-8599-406466dab8e_story.html

Nakashima, E. (2019, February 27). US Cyber Command operation disrupted Internet access of Russian troll factory on day of 2018 midterms. *Washington Post*. https://www.washingtonpost.com/world/national-security/us-cyber-command-operation-disrupted-internet-access-of-russian-troll-factory-on-day-of-2018-midterms/2019/02/26/1827fc9e-36d6-11e9-aff5-b517ff322e9_story.html
Nakashima, E., & Dawsey, J. (2020, December 19). Trump contradicts Pompeo in bid to downplay massive hack of U.S. government, Russia’s role. *Washington Post*. https://www.washingtonpost.com/national-security/russia-is-behind-the-broad-ongoing-cyber-spy-campaign-against-the-us-government-and-private-sector-pompeo-says/2020/12/19/8c850cf0-41b3-11eb-8bc0-ae155bee4aff_story.html

Nakashima, E., & Ryan, M. (2020, December 21). Trump’s acting Pentagon chief unlikely to advance plan for splitting NSA, Cyber Command leadership. *Washington Post*. https://www.washingtonpost.com/national-security/christopher-miller-cyber-command-nsa-paul-nakasone/2020/12/21/e694c338-430d-11eb-a277-49a6d1f9dff1_story.html

Nakashima, E., & Timberg, C. (2020, December 14). Russian government hackers are behind a broad espionage campaign that has compromised U.S. agencies, including Treasury and Commerce. *Washington Post*. https://www.washingtonpost.com/national-security/russian-government-spies-are-behind-a-broad-hacking-campaign-that-has-breached-us-agencies-and-a-top-cyber-firm/2020/12/13/d5a53b88-3d7d-11eb-9453-fc36ba051781_story.html

Nakasone, P. M. (2019). A cyber force for Persistent Operations. *Joint Force Quarterly*, 92(1), 10–14.

Nechepurenko, I. (2019, June 17). Kremlin warns of Cyberwar after report of US Hacking into Russian Power Grid. *New York Times*. https://www.nytimes.com/2019/06/17/world/europe/russia-us-cyberwar-grid.html

Perlroth, N., & Sanger, D. E. (2018, May 15). White House eliminates Cybersecurity Coordinator role. *New York Times*. https://www.nytimes.com/2018/05/15/technology/white-house-cybersecurity.html

Sanger, D., & Rappeport, A. (2020, December 21). Treasury Department’s Senior Leaders were targeted by hacking. *New York Times*. https://www.nytimes.com/2020/12/21/us/politics/russia-hack-treasury.html

Sanger, D. E. (2012). *Confront and conceal: Obama’s Secret Wars and surprising use of American Power*. Crown.

Satter, R. (2020, December 24). U.S. cyber agency says SolarWinds hackers are ‘impacting’ state, local governments. *Reuters*. https://uk.reuters.com/article/us-global-cyber-usa/u-s-cyber-agency-says-solarwinds-hackers-are-impacting-state-local-governments-idUKKBN28Y09L

Satter, R., Bing, C., & Menn, J. (2020, December 16). Hackers used SolarWinds’ dominance against it in sprawling spy campaign. *Reuters*. https://www.reuters.com/article/global-cyber-solarwinds/hackers-used-solarwinds-dominance-against-it-in-sprawling-spy-campaign-idINKBN28Q07P

Schneider, J. (2020). A strategic cyber no-first-use policy? Addressing the US Cyber strategy problem. *The Washington Quarterly*, 43(2), 159–175. https://doi.org/10.1080/0163660X.2020.1770970

Seitz, S., & Talmadge, C. (2020). The Predictable Hazards of unpredictability: Why Madman behavior doesn’t work. *The Washington Quarterly*, 43(3), 31–46. https://doi.org/10.1080/0163660X.2020.1810424

Smeets, M. (2020). US cyber strategy of persistent engagement & defend forward: implications for the alliance and intelligence collection. *Intelligence and National Security*, 35(3), 444–453.

Smith, B. (2020, December 17). A moment of reckoning: The need for a strong and global cybersecurity response. *Microsoft*. https://blogs.microsoft.com/on-the-issues/2020/12/17/cyberattacks-cybersecurity-solarwinds-fireeye/

Swan, J. (2017, October 1). Scoop: Trump urges staff to portray him as ’crazy guy’. *Axios*. https://www.axios.com/inside-trumps-crazy-train-2491643924.html
Taylor, M. (2020, March 10). Is it time to reform the Federal Vacancies Reform Act? *Lawfare*. https://www.lawfareblog.com/it-time-reform-federal-vacancies-reform-act

Tiku, N., Romm, T., & Timberg, C. (2021, January 9). Twitter bans Trump’s account, citing risk of further violence. *Washington Post*. https://www.washingtonpost.com/technology/2021/01/08/twitter-trumpdorsey

Timberg, C., & Nakashima, E. (2020a, December 16). The U.S. government spent billions on a system for detecting hacks. The Russians outsmarted it. *Washington Post*. https://www.washingtonpost.com/national-security/ruussian-hackers-outsmaerted-us-defenses/2020/12/15/3deed840-3f11-11eb-9453-fc36ba051781_story.html

Timberg, C., & Nakashima, E. (2020b, December 17). Federal investigators find evidence of previously unknown tactics used to penetrate government networks. *Washington Post*. https://www.washingtonpost.com/business/technology/government-warns-new-hacking-tactics-russia/2020/12/17/bba43fd8-408c-11eb-a402-fba110db3b42_story.html

Trump, D. (2020a, November 18). ‘The recent statement by Chris Krebs on the security of the 2020 Election was highly inaccurate, in that there were massive improprieties and fraud – including dead people voting, Poll Watchers not allowed into polling locations, “glitches” in the voting machines which changed…’ *Twitter*. https://twitter.com/realDonaldTrump/status/1328852352787484677

Trump, D. (2020b, November 18). ‘…votes from Trump to Biden, late voting, and many more. Therefore, effective immediately, Chris Krebs has been terminated as Director of the Cybersecurity and Infrastructure Security Agency.’ *Twitter*. https://twitter.com/realDonaldTrump/status/1328852354049957888

Trump, D. (2020c, December 19). ‘The Cyber Hack is far greater in the Fake News Media than in actuality. I have been fully briefed and everything is well under control. Russia, Russia, Russia is the priority chant when anything happens because Lamestream is, for mostly financial reasons, petrified of…’ *Twitter*. https://twitter.com/realDonaldTrump/status/1340333618691002368

Trump, D. (2020d, December 19). ‘…discussing the possibility that it may be China (it may!). There could also have been a hit on our ridiculous voting machines during the election, which is now obvious that I won big, making it an even more corrupted embar-rassment for the USA. @DNI_Ratcliffe @SecPompeo’ *Twitter*. https://twitter.com/realDonaldTrump/status/1340333619299147781

US Cyber Command (2018). Achieve and Maintain Cyberspace Superiority: Command Vision for U.S. *Cyber Command*. Fort Meade, MD: US Cyber Command. https://www.cybercom.mil/Portals/56/Documents/USCYBERCOM%20Vision%20April%202018.pdf

Valeriano, B. (2020, December 21). Assessing President Trump’s legacy of Cyber confusion. *Council on Foreign Relations*. https://www.cfr.org/blog/assessing-president-trumps-legacy-cyber-confusion

Vavra, S. (2020, November 12). How the Pentagon is trolling Russian, Chinese hackers with cartoons. *Cyberscoop*. https://www.cyberscoop.com/pentagon-cyber-command-trolling-russian-chinese-hackers-cartoons/

White House. (2012). Presidential Policy Directive/PPD-20. https://fas.org/irp/offdocs/ppd/ppd-20.pdf

Zetter, K. (2014). *Countdown to Zero Day: Stuxnet and the Launch of the World’s First Digital Weapon*. Crown.

Zetter, K. (2020, December 24). SolarWinds Hack infected critical infrastructure, including power industry. *The Intercept*. https://theintercept.com/2020/12/24/solarwinds-hack-power-infrastructure/