The 2019 Venezuelan Blackout and the consequences of cyber uncertainty

O blecaute venezuelano de 2019 e as consequências da incerteza cibernética

Rev. Bras. Est. Def. v. 7, nº 2, jul./dez. 2020, p. 37-57
DOI: 10.26792/RBED.v7n2.2020.75204
ISSN 2358-3932

JOE DEVANNY
LUIZ ROGÉRIO FRANCO GOLDONI
BRENO PAULI MEDEIROS

INTRODUCTION[1]

Geopolitics and digital technologies are inextricably interconnected. This manifests in different ways, aligning with broader strategic issues, including: debates about foreign ownership or involvement in domestic infrastructure, such as the U.S.-led campaign to restrict the Chinese company Huawei's role in 5G communications networks across the globe; and concern about the potential for digital media, including social media platforms, to be exploited to pursue disinformation and subversion, as occurred during the 2016 U.S. presidential election campaign. Digital technology and geopolitics also combine in contemporary debates about the practice and limits of digital espionage and offensive cyber operations, particularly following the 2011-12 discovery of the U.S.-Israeli Stuxnet/Op OLYMPIC GAMES cyber operation against Iranian nuclear infrastructure (Sanger 2012; Zetter 2014) and the 2013 revelations by Edward Snowden about the extent of U.S. and allied digital surveillance capabilities (Ball, Borger & Greenwald 2013; Harding 2014; Harris 2014). State threats to digital infrastructure — and the strategic implications of those threats — were visible more recently in the major incidents regarding SolarWinds and Microsoft Exchange (Alperovitch and Ward 2021;

Joe Devanny — Lecturer in the Department of War Studies at King's College London and deputy director of the Centre for Defence Studies at King's.
Luiz Rogério Franco Goldoni — Professor in the Postgraduate Program in Military Sciences of the Meira Mattos Institute (PPGCM-IMM) at the Army Command and General Staff School (ECEME).
Breno Pauli Medeiros — PhD student in Military Sciences at the Army Command and General Staff School (ECEME).

Devanny 2021). The contemporary strategic impact of cyber (as threat and opportunity) on defense and security policies highlights the social, economic and political ubiquity of digital technologies and the Internet.

As digital technologies such as social media platforms accelerate the volume and velocity of "speech acts" in public diplomacy, it has become more difficult to control narratives surrounding controversial events or crises, and for publics to establish "truth" in a world of "alternative facts" and "fake news". This polluted information environment exacerbates the problem of determining truth in areas of technical complexity, in a global public sphere suffering from a "knowledge asymmetry" that undermines the ability of citizens (and some governments) to determine which party to believe in a contested narrative.

In the case of alleged cyber operations, this knowledge asymmetry is magnified by the high level of technical knowledge and capability necessary to conduct an exercise in attribution analysis. All but the most sophisticated state actors and private sector analysts are unable to conduct or comprehend such an analysis, meaning that most people are reliant on secondary sources for information and assessment, with all the caveats about the contemporary media environment that were highlighted above. This information environment complicates the contemporary trend towards coordinated public attribution (Egloff and Smeets 2021), taking place in a broader geopolitical context that shapes reception of the *cui-bono* logic of attribution (Cavelty 2015).

To illuminate these issues, this article adopts the starting point of Venezuelan President Nicolás Maduro's allegation that March 2019 energy outages in Venezuela were caused by a U.S. cyber attack. It argues that global public opinion about the Trump administration's Venezuela policy and its emerging cyber strategy potentially contributed to an information environment in which false claims of attribution were treated more credibly than they should have been. The article concludes by reflecting on the consequences of cyber uncertainty for international relations. As Martin Libicki — another author to recognise the illustrative potential of the Venezuela case — observed: "facts of cyberwar are becoming secondary to misperceptions that governments either shape or influence" (Libicki 2020, 85).

The article uses the Venezuela case to highlight the geopolitical impact of uncertainty in cyberspace. It argues that the instrumental value — and cost — of cyber uncertainty should inform decisionmaking about cyber strategy. The article is structured in four parts followed by a conclusion. First, it presents the Venezuelan case, situating Maduro's cyber allegation in the context of fraught bilateral relations between Venezuela and the United States. Second, it introduces the concept of cyber uncertainty, identifying the impact of knowledge asymmetries on broader public perceptions of perceived and real cyber operations. Third, it analyses the conduct and consequences of U.S. cyber operations, assessing the relevance of the recent shift in U.S. strategy. Fourth, it discusses the Trump administration's discernible strategy for Venezuela and the second-order diplomatic effects of U.S. cyber strategy. The article concludes by appraising the Venezuelan case as an illumination of emerging trends in cyber operations, disinformation and contested strategic narratives, all in the wider social context of knowledge asymmetries and prevailing cyber uncertainty.

ENERGY OUTAGE AND CYBER ALLEGATIONS IN VENEZUELA

Between March 7 and 14, 2019, a major blackout left many homes, businesses and public buildings in Venezuela without electricity (Daniels 2019). The blackout prompted the interruption of services at airports and in hospitals (Sequera and Buitrago 2019). It led to local businesses being ransacked and clashes between owners and looters. This occurred against a nationwide backdrop of on-going protests in opposition to Maduro (Casey 2019).

Some experts have speculated that the blackout was caused by a technical issue, particularly following the deterioration of national infrastructure during Venezuela's continuing economic and political crisis (Leetaru 2019; Jones 2019). There were other reports that Russian military personnel (reportedly including cybersecurity experts) arrived in Venezuela later in March (Gunia 2019). The reported presence of Russian cyber experts indicated support to the Maduro regime, perhaps including digital surveillance of opponents, as well as infrastructure cyber security (Spetalnick 2019).

Reporting of technical analysis regarding the cause of the blackout occurred in a contested media environment. One striking feature was the diplomatic disagreement via social media between Venezuelan president Maduro and then U.S. Secretary of State Mike Pompeo. Maduro and Pompeo traded insults on the social media platform Twitter, after Maduro had alleged that the U.S. was responsible for a cyber attack against Venezuela's energy infrastructure, using this as the explanation for the blackouts (Maduro 2019). Pompeo responded quickly, rejecting the allegation and countering that regime-change would occur in Venezuela (Pompeo 2019). The Trump administration's special representative for Venezuela, Elliott Abrams, also said that the outages were: "a reminder that the country's once quite sophisticated infrastructure has been plundered and allowed to decay under Maduro's misrule" (Sheridan and Zuniga 2019).

This heated exchange via social media was part of a longer period of deterioration in U.S-Venezuela bilateral relations. In early 2019, the

Trump administration had recently officially recognised the head of the national assembly, Juan Guaidó, as the interim president of Venezuela. Guaidó's presidency would subsequently be recognised by 58 nations. The bilateral relationship had already been antagonistic: in November 2018 the then US national security adviser, John Bolton, had publicly grouped Venezuela with Cuba and Nicaragua as countries regarded as regional threats, denouncing:

> This Troika of Tyranny, this triangle of terror stretching from Havana to Caracas to Managua…[as] the cause of immense human suffering, the impetus of enormous regional instability, and the genesis of a sordid cradle of communism in the Western Hemisphere (Rogin 2018; Bolton 2020, 249).

Although the Trump administration had not publicly threatened Venezuela with cyber attacks prior to the March 2019 energy outages, it is clear from other evidence that it possessed both the capability and willingness to target infrastructure using this instrument to pursue national policy. For example, Trump would reportedly authorize a cyber operation against Iran just three months later (Nakashima 2019) and had previously streamlined the authorization process to make it easier for U.S. Cyber Command and the Central Intelligence Agency to conduct cyber operations than it had been under the Obama administration (Devanny 2021, 11).

According to John Bolton's memoir, the Trump administration wanted to remove Maduro from office, but suffered from an ineffective strategy, "bureacratic footdragging", disagreement amongst senior figures and President Donald Trump's tendency to change his mind, including after a persuasive conversation with Russian President Vladimir Putin (Bolton 2020, 271–4, 282–3). Similarly, efforts by the opposition to create splits in Maduro's regime, particularly with the military, were reportedly proceeding at the time of the energy outages, culminating in a failed attempt by Guaidó in late April 2019 to secure military support in his bid to replace Maduro (Faiola 2019a). The failure of this move led Maduro's intelligence chief, with whom the opposition had collaborated, to flee to Colombia, after which the U.S. government lifted sanctions against him (Faiola 2019b) in exchange for cooperation against Maduro. Throughout the rest of 2019, the opposition suffered from increasing weakness, harassed and divided by the government, with splits developing between opposition parties, and dissension and corruption allegations surfacing within Guaidó's own party (Faiola 2019c).

The opposition lost further momentum in January 2020 when the Maduro government arranged for a rival to Guaidó to be sworn in as head of the national assembly — the position from which Guaidó derives legitimacy for his claim to be the interim president (Krygier and Faiola 2020). As the opposition experienced these setbacks, the US government pursued alternative approaches, tightening economic sanctions and deciding in March 2020 to indict Maduro and five others on criminal charges of narco-terrorism, offering US$15m in reward for Maduro's capture (Faiola, Zapotosky, and DeYoung 2020). In this context, in May 2020 two U.S. former Special Operations soldiers were arrested in Venezuela, reportedly following a failed *coup d'etat* (Tharoor 2020).

There is no evidence that the Trump administration was involved in this failed effort, or indeed in the March 2019 energy outages, but bilateral relations were then so poor that no trust existed between the two governments. Indeed, following the arrest of the two former U.S. soldiers after the failed coup in May 2020, the U.S. State Department said: "There is a major disinformation campaign underway by the Maduro regime, making it difficult to separate facts from propaganda" (DeYoung, Faiola, and Horton 2020).

The 2019 episode in Venezuela thus offers an interesting case in the diplomatic and geopolitical consequences of the emerging global public understanding about US cyber operations. As the U.S. government increasingly talks about its cyber capabilities and their place in national security strategy, so too do U.S. adversaries accuse it of conducting cyber attacks. This diplomatic risk is explicitly recognised in one authoritative official U.S. statement about the shift in cyber strategy (US Cyber Command 2018, 10). The new cyber strategy — with its prescription of more frequent cyber operations against adversaries — developed organically and should not be associated with the politics or objectives of the Trump administration. Nevertheless, it unfolded against a backdrop of reduced public trust in the office of the presidency under the Trump administration, in light of its association with "fake news" and "alternative facts", its hostility towards journalism and even towards parts of the US federal government, such as the intelligence community, that Trump referred to derisively as the "deep state" and which he claimed were part of an effort to undermine his presidency (Rohde 2020). This created a less favorable information environment for the reception of this strategic shift, increasing the risk of misunderstanding about what the new strategy was trying to achieve.

THE UNCERTAINTY PRINCIPLE OF THE CYBER DOMAIN

In view of the complexity of physical and virtual layers that make up cyberspace, identifying causative activities and attributing them to specific actors requires significant technical and analytical capabilities. These capabilities exist in both private (cybersecurity companies) and public sectors (most commonly in defense, intelligence and security agencies). But the level of sophistication and resourcing of cyber forensics differs widely, creating severe knowledge asymmetries both between governments and between governments and their publics.

This becomes more complicated when perpetrators go further than masking their acts, fabricating to mislead — even seeking to incriminate others in false flag operations. Given the inconclusiveness of certain forensic efforts, the attribution of actors often employs *cui-bono* logic, i.e.: given the political, economic, military and/or social context, the actor who would benefit the most from a cyber operation would be more likely to perpetrate it (Cavelty 2015, 93).

Thus, the uncertainty principle often implies a speculative context that weighs political issues. Sophisticated cyber actors can exploit this uncertainty for operational advantage, but, as the Venezuela case implies, uncertainty also has its costs. This is, of course, less straightforwardly the case in instances of cyber deterrence or compellence, when perpetrators presumably need to signal responsibility to achieve deterrence or compellence, a precondition for which is that the targeted state should understand the purpose of the attack, namely to dissuade/compel a specific response (Valeriano, Jensen, and Maness 2018, 47).

Cyberspace is operationally contested. State actors typically do not disclose their digital espionage activities, in order to retain surveillance access. Active digital surveillance, involving presence on a network, also affords the opportunity to develop an exploit of a vulnerability on that network to achieve a different effect, e.g. to degrade or destroy the network, wholly or in part. This duality is the cause of much of the policy debate and controversy surrounding the SolarWinds incident (Devanny 2021). Similarly, covert access to a network potentially enables criminal activities, e.g. data theft or ransoming individuals or organisations in exchange for re-enabling access to their devices or networks — a major consequence of the Microsoft Exchange incident (Alperovitch and Ward 2021; Poznansky and Perkoski 2018, 7–8). This duality of potential, juxtaposing cyber espionage and offensive cyber operations, creates uncertainty that could produce severe strategic consequences.

Medeiros and Goldoni (2020) see uncertainty, deterritoriality and multiplicity of actors as key elements to understand the operationalization of cyberspace. Acccordingly, when cyber operations are detected, widespread public acceptance of the attribution analysis will rest on the tension between *cui-bono* logic and (im)plausible deniability (Cormac and Aldrich

2018). Attribution occurs in a political context: it is not a neutral, purely technical exercise. The geopolitical competition of strategic narratives, exacerbated by digital media, is rendered more acute in cases of uncertainty over (alleged) cyber operations.

Cyber uncertainty and the potential to carefully calibrate operational effects, reducing the risk of casualties and managing the risk of escalation, have made cyber operations an increasingly attractive option in geopolitical competition. Recent reports of reciprocal cyber operations conducted by Iran and Israel highlight this practice (Baram and Lim 2020). As the world's most militarily capable state, the United States has also shaped behavior in the cyber domain, developing and using sophisticated digital espionage and offensive cyber capabilities (Harris 2014).

U.S. STRATEGY AND CYBER OPERATIONS

The United States has endorsed voluntary, non-binding norms of responsible state behavior in peacetime cyberspace, including "prohibitions against damaging civilian critical infrastructure" (US DOD 2018, 5). Notwithstanding, it is not an outlandish proposition to assert that there are circumstances in which the U.S. government might conduct a cyber operation against an adversary's critical infrastructure. For example, just three months after the Venezuelan energy outages, it was reported that the Trump administration had authorised penetration of the Russian energy network, signalling the sophistication of U.S. capabilities to conduct just such an attack (Sanger and Perlroth 2019). This operation's stated intent was to deter Russian operations against the United States. In contrast, the hypothetical value of cyber (or other covert) operations against Venezuelan energy infrastructure would be to exacerbate domestic socio-economic problems, intensifying opposition to Maduro and ultimately facilitating regime-change.

One operation was reportedly designed to deter, the other would have been designed to complement other, non-cyber measures implemented by the US government to bring about regime change in Venezuela. Whilst there is no evidence that the US conducted cyber operations in Venezuela, the problem is one of perception compounded by actual policy: the US was engaged in a broad-based effort to increase pressure on Maduro's regime, and has signaled the capability to conduct cyber operations against energy infrastructure in pursuit of other strategic objectives. The use of cyber operations in support of wider policy would follow the logic of "additive" cyber operations that "complement rather than replace traditional forms of coercion" (Valeriano, Jensen, and Maness 2018, 42). Perhaps for many observers, without access to or comprehension of technical reports into the origins of energy outages in Venezuela, allegations of US complicity might not be so readily dismissed, particularly in light of a pre-existing pattern of strategic behavior arguably consistent with the conduct of such an operation. Another relevant factor shaping the information environment is the impact of history, particularly US policy towards Latin America during (and before) the Cold War (Crandall 2008; Grow 2008).

This aligns with Robert Jervis's observation about the polysemous nature of cyber operations, given the existence of multiple audiences within and between states: "Not only is no state completely unified, but the perceptions of numerous third parties are also important. What would seem like an under-reaction to some allies, for example, could be seen as a dangerous over-reaction by others" (Jervis 2016, 71). The combination of declaratory posture, rhetoric and reported US activities in cyberspace under the post-2018 strategy have collectively created the impression of a more permissive approach to cyber operations. This has implications for the ways in which other states and their publics will likely perceive the U.S. as a strategic actor.

The June 2019 reported signaling operation against Russian infrastructure was part of the new US strategy to "defend forward" in cyberspace and embrace "persistent engagement." Jacquelyn Scheider situates this turn towards a more assertive strategy in the context of an emerging pattern of behavior by US adversaries, which highlighted "the increasingly front-line role of critical infrastructure in state-led cyber attacks" (Schneider 2020, 161). The cases cited by Schneider include Russian interference in the 2016 US presidential election; cyber attacks against energy infrastructure in Ukraine; and cyber crime against financial networks reportedly conducted by Iran and North Korea. Schneider does not mention the U.S.-Israeli cyber operation against Iranian nuclear infrastructure, which pre-dates her examples and arguably deserves a more prominent place in the chronology of cases demonstrating the increasing number of infrastructure-targeted cyber operations conducted by state actors (Zetter 2014).

The intellectual justification for "persistent engagement" is closely associated with Michael Fischerkeller and Richard Harknett, who have argued that the previous US approach of deterrence and restraint was ill-suited to the cyber domain: "A strategy of deterrence seeks to avoid operational contact, whereas cyberspace participants are interconnected, and consequently, all operations in cyberspace always involve operational contact. Cyberspace is a perpetually contested space" (Fischerkeller and Harknett 2017, 386). Fischerkeller and Harknett's analysis of cyberspace and consequent prescription for US responses is independent of U.S. policy objectives: the analyses and recommendations advanced by advocates of persistent engagement and defend forward are as adoptable by the Biden administration as they were by the Trump administration (Devanny 2021). They flow from an appraisal of the "offense-persistent" nature of cyberspace and the reality of "constant contact with the enemy" (Harknett and Goldman 2016, 86).

This analysis has heavily influenced U.S. Cyber Command, with its commander describing a shift from being a "response" force to becoming a "persistence" force, appropriate for a new reality in which: "Continuous action in cyberspace for strategic effect has become the norm, and thus the command requires a new strategic concept" (Nakasone 2019, 12). This shift is most visible in two documents produced by the U.S. government in 2018: the command vision for Cyber Command (US Cyber Command 2018) and the National Cyber Strategy (US DOD 2018). These documents explain a strategic shift to position the United States to succeed in cyberspace competition with its most capable adversaries. The new strategy is a "roadmap…to achieve and maintain superiority in cyberspace" (US Cyber Command 2018, 2). It is therefore a misapprehension to interpret the new strategy as evidence of greater likelihood that the U.S. would conduct cyber operations to sabotage non-cyber infrastructure of less cyber-capable adversaries such as Venezuela. Infrastructure-targeting is one example of cyber operations, but it is not the principal focus of the new turn in U.S. strategy.

The new strategy envisaged a higher tempo and greater risk appetite for US cyber operations — according to the Command Vision, the new approach is "risk aware, not risk averse" (US Cyber Command 2018, 7). This was conceived, however, as a specific response to the nature of competition in cyberspace. It did not imply reckless disregard for consequences and was rather calibrated to achieve specific effects. More broadly, the Trump administration continued the Obama administration's approach of using cyber operations to manage the risk of escalation, e.g. in responding to alleged Iranian attacks on oil tankers and an unmanned US surveillance drone in mid-2019 (Valeriano and Jensen 2019). This reflects the flexibility of cyber operations as an instrument of national strategy, a flexibility stemming partly from the aforementioned elements of cyber uncertainty.

The contemporary debate about U.S. strategy focuses understandably on its impact on stability and whether the broader strategy is overly focused on its offensive dimensions to the detriment of defense (Healey 2020). Holistic appraisal of the new strategy also requires analysis of its wider system effects, including its impact on the dynamics of policy issues that were not considered as part of the process of strategic development (Jervis 1998).

One of these second-order effects is the potential impact of U.S. strategy on other states' (both allies' and adversaries') perceptions of false allegations regarding U.S. cyber operations. During the Trump administration, the combination of a broadly pro-active cyber strategy and a unpredictable White House prone to making seemingly provocative statements, injected an element of uncertainty and doubt about what the U.S. might or might not have been doing, in spite of the emerging body of policy-oriented literature — drawn from in this section — that explores and explains U.S. cyber strategy. This unusual conjuncture made the antagonism between the Trump and Maduro administrations an interesting case in the analysis of the implications of the Trump administration's approach to diplomacy and cyber operations.

THE TRUMP ADMINISTRATION, VENEZUELA AND CYBER UNCERTAINTY

In the context of severe economic crisis, the failure of Venezuelan energy infrastructure in March 2019 can plausibly be attributed to domestic shortcomings. These include the compound impact of years of underfunding and poor maintenance, possibly exacerbated by an exodus of skilled personnel from the sector as part of the wider sharp increase in emigration from Venezuela as many citizens try to escape from its crisis. This is a simpler explanation than the alternative of a protracted and expensive effort to develop and deploy U.S. cyber capabilities to undermine the electricity supply. There is a further doubt about the cyber explanation, when the U.S. might have been expected to have had cheaper, less high-tech options, such as non-cyber sabotage. Most relevantly, however, it is simply unclear precisely what strategic effect such an operation would have been intended to produce and how proportionate infrastructure-sabotage would have been as an instrument to achieve it.

Whilst the above will be sufficient to persuade many observers that the Trump administration probably did not conduct a cyber (or indeed a non-cyber) operation against Venezuelan critical infrastructure, the juxtaposition of two factors — (i) the Trump administration's discernible preference for a Venezuela under different governance and (ii) the second-order effects of the new cyber strategy — created the potential for a contested narrative, invoking the inherent uncertainty of cyberspace. This is particularly true in an era characterised by the proliferation of false narratives on social media and concerted efforts by state actors to pollute the information environment and undermine public confidence in the media.

In the context of John Bolton's rhetoric designating Venezuela as part of a "troika of tyranny", the Trump administration's policies towards Venezuela were inevitably evocative of the rhetorical inheritance of the "axis of evil." The latter phrase was coined during a previous US administration in which Bolton had served, namely the George W. Bush presidency. That presidency was indelibly associated with military intervention and regime-change (Mann 2004). Bolton's choice of rhetoric therefore generated an implicit expectation that more coercive instruments would be employed than had yet been employed by the Trump administration against Venezuela. Indeed, military action was explicitly stated to be "an option" by Trump himself, in apparently off-the-cuff remarks, both in August 2017 and February 2019 (Ellsworth 2019).

Moreover, the January 2019 appointment of the controversial neoconservative Elliott Abrams as the administration's special envoy for Venezuela provoked memories of an even earlier US administration. Abrams was assistant secretary of state for inter-American affairs during the Reagan administration. He was personally implicated in the Iran-Contra scandal (Borger 2019). When exploring global perceptions of the Trump administration's Venezuela strategy, it is important to contextualise debates about contemporary policies with reference to the substantial history of U.S. covert actions and regime-change policies in Latin America, for example during the Cold War (Grow 2008). Also relevant are tensions between the objectives of U.S. post-Cold War "democracy promotion" programmes and the domestic politics of specific states in the region, with Venezuela being a particularly acute and prominent case (Clement 2005).

The most plausible interpretation of the available evidence is that there was a counterproductive gap between the Trump administration's rhetoric and the policies it was prepared to pursue. As Hal Brands noted regarding Trump's 2017 comments about the military "option" in Venezuela: "the president's apparently improvised threats of military action against Venezuela served mainly to wrong-foot regional critics of President Nicolás Maduro's government (and to distract attention from that government's own failings) by raising the prospect of unwanted US intervention" (Brands 2017, 25–6). Throughout most of Trump's term in office, his Venezuela policy was coercive in intent, including significant economic sanctions (Main 2020, 34–5), but within limits notionally calibrated to facilitate negotiated settlement, most probably by splitting Maduro's constituency of support. Unsealed criminal indictments of Maduro and other senior figures in early 2020 appeared to indicate a loss of confidence that such an objective was achievable (Ramsey 2020). The juxaposition of bombastic rhetoric and loose talk about military options did little to amplify or enhance the effectiveness of the administration's strategy: coercive economic sanctions undoubtedly had a severe impact on the Venezuelan economy, but the Maduro government entrenched itself and called the Trump administration's bluff regarding what appeared ultimately to be empty and ill-conceived threats of military action.

The blunt instrument of economic sanctions had increased pressure on Maduro's government, but the real victims were of course the millions of Venezuelan citizens who directly suffered from the impact of the economic crisis. In this sense, the hypothesis that the U.S. government would sabotage Venezuelan critical infrastructure did not appear to be a difference in kind: the human cost of the 2017 and 2019 economic sanctions arguably outweighed the specific consequences of the time-limited disruption to the electricity supply in March 2019. Just as the totality of instruments that comprised the Trump administration's Venezuela strategy militated against arguments that a limited cyber operation affecting critical infrastructure would cross an ethical line of conduct, the perceptual impact of "persistent engagement" — particularly reporting of U.S. pre-positioning of implants inside Russian energy infrastructure — perhaps contributed to already-fertile conditions in which counter-narratives could grow. This case-specific context arguably overshadowed in this instance the wider debate about the ethical implications of cyber operations targeting civilian infrastructure (Devanny 2020).

Cyber uncertainty is exacerbated by knowledge asymmetry, in which the circumstances surrounding incidents such as the Venezuelan energy outages are virtually impossible for most people to establish definitively. Such an assessment would require technical expertise to comprehend and would otherwise rely on diverse readerships' or audiences' willingness to trust the reliability of the secondary sources that explained it. Indeed, John Bolton himself recounts in his memoir that, on hearing of the outages, his "first thought was that Guaidó or someone had decided to take matters into their own hands…whatever the cause or the extent or duration of the outage, it had to hurt Maduro". Bolton quickly qualifies this equivocal note, however, highlighting that "the national power grid had disintegrated over two decades of Chavista rule" (Bolton 2020, 270).

In this era of disinformation operations and cyber uncertainty, the perceived benefits of "implausible deniability" should be weighed against the residual cost of a situation of "implausible culpability", in which the more assertive turn of U.S. cyber strategy combined with the Trump administration's broader policies of coercion and its use of threatening rhetoric, creating an opportunity for one U.S. adversary to seek to capitalize by deflecting blame for domestic infrastructure failure onto the spectre of coercive U.S. behavior in cyberspace.

Following Jacquelyn Schneider (2020), this is arguably a reason for the U.S. government to review not only its declaratory posture in cyberspace, but also more broadly, the ways in which it publicly articulates its strategies and fuses its rhetoric and broad array of coercive policy instruments to pursue national strategic objectives. As mentioned above, this is an issue explicitly recognised by U.S. Cyber Command as requiring mitigation, partly through more effective communication (US Cyber Command 2018, 10). For the Biden administration, recalibrating rhetoric and reviewing the policy objectives that cyber and non-cyber instruments are used to pursue could mitigate shortcomings in the Trump administration's implementation of cyber strategy (Devanny 2021).

CONCLUSION

The last decade has seen an emerging pattern of cyber operations conducted by states against adversaries' critical infrastructure. It is this emerging pattern, or specifically the perceived failure of U.S. efforts to deter this behavior, that provided a significant part of the justification for U.S. adoption of a new cyber strategy in 2018. As states continue to develop and use national offensive cyber capabilities, it is likely that a continuation of existing policies will lead to further such operations.

Further complexity is added by the second-order effects of these operations. The system effects of this strategic turn in cyber operations are not limited to those that stem from the conduct of operations. They also include the effects of the competitive development process of offensive cyber capabilities by rival states, and indeed the very act of governments communicating about these capabilities. As persistent engagement's advocates argue, practice will shape the *de facto* norms of state behavior in cyberspace. This extends to the impact on perceptions caused by the potential complementarity of infrastructure-targeted cyber operations with other, non-cyber coercive instruments of policy or associated rhetorical threats. It also extends to the (unintended) strategic consequences of the duality between active cyber espionage and the potential to conduct offensive operations. This has been recently evident in the furore surrounding the SolarWinds breach.

As Robert Jervis has noted, the potential for misperceptions and corresponding errors of judgement in cyberspace is pronounced. This is particularly true in light of asymmetries of knowledge and the tendency for nuance to be winnowed out for decision-makers in the policy process (Jervis

2016). Another shaping factor is the distorted prism of the contemporary information environment. Competing narratives (both state narratives and proxy- or non-state narratives) proliferate more quickly and embed themselves more durably due to the analytical affordances and disintermediation of digital media platforms and the deterritoriality of the internet. The cumulative impact of these different strands is that states will likely struggle to control the perception of their intentions in cyberspace, not only amongst governments but across the many national audiences that comprise the global public sphere.

REFERENCES

Alperovitch, Dmitri, and Ian Ward. 2021. "How Should the U.S. Respond to the SolarWinds and Microsoft Exchange Hacks?" *Lawfare* 12 (March). https://www.lawfareblog.com/how-should-us-respond-solarwinds-and-microsoft-exchange-hacks.

Ball, James, Julian Borger, and Glen Greenwald. 2013. "Revealed: how US and UK spy agencies defeat internet privacy and security". *The Guardian.* https://www.theguardian.com/world/2013/sep/05/nsa-gchq-encryption-codes-security.

Baram, Gil, and Kevjn Lim. 2020. "Israel and Iran Just Showed Us the Future of Cyberwar with Their Unusual Attacks," *Foreign Policy* 5 (June). https://foreignpolicy.com/2020/06/05/israel-and-iran-just-showed-us-the-future-of-cyberwar-with-their-unusual-attacks/.

Bolton, John. 2020. *The Room Where it Happened: A White House Memoir.* New York: Simon and Schuster.

Borger, Julian. 2019. "US diplomat convicted over Iran-Contra appointed special envoy for Venezuela," *The Guardian* 26 (January). https://www.theguardian.com/us-news/2019/jan/26/elliott-abrams-venezuela-us-special-envoy.

Brands, Hal. 2017. "The Unexceptional Superpower: American Grand Strategy in the Age of Trump," *Surviva*l 59, no. 6: 7–40.

Casey, Nicholas. 2019. "Venezuela Was Crumbling. A Blackout Tipped Parts of It Into Anarchy," *New York Times* (March). https://www.nytimes.com/2019/03/15/world/americas/venezuela-blackout-maracaibo.html.

Cavelty, Myriam. 2015. "The normalization of cyber-international relations," *Strategic Trends 2015.* ETH Zurich: Center for Security Studies: 81–98.

Clement, Christopher I. 2005. "Confronting Hugo Chávez: United States 'Democracy Promotion' in Latin America," *Latin American Perspectives* 32, no. 3: 60–78.

Cormac, Rory, and Richard J. Aldrich. 2018. "Grey is the new black: covert action and implausible deniability," *International Affairs* 94, no. 3 (May), 477–94, https://doi.org/10.1093/ia/iiy067.

Crandall, Russell. 2008. *The United States and Latin America after the Cold War.* Cambridge: Cambridge University Press).

Daniels, Joe. 2019. "Venezuela: widespread blackouts could be new normal, experts warn," *The Guardian* 23 (July). https://www.theguardian.com/world/2019/jul/23/venezuela-blackouts-new-normal/.

Devanny, Joe. 2020. "The Ethics of Offensive Cyber Operations," *Foreign Policy Centre.* https://fpc.org.uk/the-ethics-of-offensive-cyber-operations/.

_____. 2021. "'Madman Theory' or 'Persistent Engagement'"? The Coherence of US Cyber Strategy under Trump. *Journal of Applied Security Research.* DOI: 10.1080/19361610.2021.1872359.

DeYoung, Karen, Anthony Faiola, and Alex Horton. 2020. "U.S. denies involvement in alleged Venezuela invasion attempt as details remain murky," *The Washington Post* (May). https://www.washingtonpost.com/national-security/trump-venezuela-invasion-attempt/2020/05/05/8b4d64ec-8ee7-11ea-9e23-6914ee410a5f_story.html?utm_campaign=wp_main&utm_medium=social&utm_source=twitter.

Egloff, Florian J., and Max Smeets. 2021. "Publicly attributing cyber attacks: a framework," *Journal of Strategic Studies.* DOI: 10.1080/01402390.2021.1895117.

Ellsworth, Brian. 2019. "UPDATE 3-Trump says U.S. military intervention in Venezuela 'an option', Russia objects". *The Washington Post* (February). https://www.washingtonpost.com/world/trump-us-military-intervention-in-venezuela-is-an-option/2019/02/03/27bb6d42-27ec-11e9-984d-9b8fba003e81_story.html

Faiola, Anthony. 2019a. "Inside the secret plot to turn Venezuelan officials against Maduro," *The Washington Pos*t (May). https://www.washingtonpost.com/world/the_americas/inside-the-secret-plot-to-turn-senior-venezuelan-officials-against-maduro/2019/05/13/5ad022a8-737e-11e9-8be0-ca575670e91c_story.html.

_____. 2019b. "Maduro's ex-spy chief lands in U.S. armed with allegations against Venezuelan government," *The Washington Post* (June). https://www.washingtonpost.com/world/the_americas/maduros-ex-spy-chief-lands-in-us-armed-with-allegations-against-venezuelan-government/2019/06/24/b20ad508-9477-11e9-956a-88c291ab5c38_story.html.

_____. 2019c. "Juan Guaidó promised to save Venezuela. Now the flame he lit is petering out, and his U.S. backers are weighing their options". *The Washington Post* (December). https://www.washingtonpost.com/world/the_americas/juan-Guaidó-promised-to-save-venezuela-a-year-later-the-flame-he-lit-is-petering-out-his-us-backers-are-weighing-their-options/2019/12/17/48a1818-6-1495-11ea-80d6-d0ca7007273f_story.html.

Faiola, Anthony, Matt Zapotosky, and Karen DeYoung. 2020. "U.S. indicts Venezuela's Maduro on narcoterrorism charges, offers $15 million reward for his capture". *The Washington Post* (March). https://www.washingtonpost.com/world/the_americas/the-united-states-indicts-venezuelas-maduro-on-narco-terrorism-charges/2020/03/26/a5a64122-6f68-11ea-a156-0048b62cdb51_story.html.

Fischerkeller, Michael P. and Richard J. Harknett. 2017. "Deterrence is Not a Credible Strategy for Cyberspace". *Orbis* 61, no. 3: 381–93.

Grow, Michael. 2008. *U.S. Presidents and Latin American Interventions: Pursuing Regime Change in the Cold War.* Lawrence: University of Kansas Press.

Gunia, Amy. 2019. "Venezuela Blames U.S. For Blackout, Asks Diplomats To Leave". *Time.* https://time.com/5550481/venezuela-maduro-blackout-cyber-sabotage/.

Harknett, Richard J. and Emily O. Goldman, 2016. "The Search for Cyber Fundamentals," *Journal of Information Warfare* 15, no. 2: 81–8.

Harris, Shane. 2014. *@War: The Rise of Cyber Warfare.* London: Headline.

Harding, Luke. 2014. *The Snowden Files: The Inside Story of the World's Most Wanted Man.* London: Guardian Faber Publishing.

Healey, Jason. 2020. "The Cyber Budget Shows What the U.S. Values — And It Isn't Defense". *Lawfare* (June). https://www.lawfareblog.com/cyber-budget-shows-what-us-values%E2%80%94and-it-isnt-defense

Jervis, Robert. 1998. *System Effects: Complexity in Political and Social Life.* Princeton, NJ: Princeton University Press, 1998.

_____. 2016. "Some Thoughts on Deterrence in the Cyber Era," *Journal of Information Warfare* 15, no. 2: 66–73.

Jones, Sam. 2019. "Venezuela blackout: what caused it and what happens next?" *The Guardian* (October). https://www.theguardian.com/world/2019/mar/13/venezuela-blackout-what-caused-it-and-what-happens-next.

Krygier, Rachelle, and Anthony Faiola. 2020. "Venezuela's last democratic institution falls as Maduro attempts de facto takeover of National Assembly". *The Washington Post* (January). https://www.washingtonpost.com/world/the_americas/venezuelas-last-democratic-institution-falls-as-maduro-stages-de-facto-takeover-of-national-assembly/2020/01/05/8ba496fe-2d8f-11ea-bffe-020c88b3f120_story.html.

Leetaru, Kalev. 2019. "Could Venezuela's Power Outage Really Be A Cyber Attack?" *Forbes* (March). https://www.forbes.com/sites/kalevleetaru/2019/03/09/could-venezuelas-power-outage-really-be-a-cyber-attack/#581f687b607c.

Libicki, Martin. 2020. "Cyberwar is What States Make of It". T*he Cyber Defense Review* 5, no. 2, Special Edition: Information Operations/Information Warfare (Summer): 77–88.

Maduro, Nicolás. 2019. "La guerra eléctrica anunciada y dirigida por el imperialismo estadounidense en contra de nuestro pueblo será derrotada. Nada ni nadie podrá vencer al pueblo de Bolívar y Chávez. ¡Máxima unidad de los patriotas!". @NicolasMaduro, *Twitter* (March). https://twitter.com/NicolasMaduro/status/1103822286422003713.

Main, Alexander. 2020. "Out of the Ashes of Economic War: Sanctions and other forms of economic warfare have long caused serious harm for countries on the receiving end of Washington's efforts to impose its policy agenda. Could a progressive US administration marshal economic power at the service of people, not capital?". *NACLA Report on the Americas* 52, no. 1: 33–40.

Mann, James. 2004. *Rise of the Vulcans: The History of Bush's War Cabinet* (London: Penguin).

Medeiros, Breno Pauli, and Luiz Rogério Franco Goldoni. 2020. "The Fundamental Conceptual Trinity Of Cyberspace," *Contexto Internacional* 42, no. 1: 31–54. https://www.scielo.br/j/cint/a/WYHRGNsY5mpWzjCwsSfrTZv/?lang=en.

Nakashima, Ellen. 2019. "Trump approved cyber-strikes against Iranian computer database used to plan attacks on oil tankers," *The Washington Post* (June). https://www.washingtonpost.com/world/national-security/with-trumps-approval-pentagon-launched-cyber-strikes-against-iran/2019/06/22/250d3740-950d-11e9-b570-6416efdc0803_story.html.

Nakasone, Paul M. 2019. "A Cyber Force for Persistent Operations," *Joint Force Quarterly*, no. 92 (1st Quarter): 10–4, http://cs.brown.edu/courses/csci1800/sources/2019_01_22_JFQ_CyberRoleForPersistentOperations_Nakasone.pdf.

Pompeo, Mike. 2019. "No food. No medicine. Now, no power. Next, no Maduro," @SecPompeo, *Twitter* (March). https://twitter.com/SecPompeo/status/1103872530450771968.

Poznansky, Michael, and Evan Perkoski. 2018. "Rethinking secrecy in cyberspace: The politics of voluntary attribution". *Journal of Global Security Studie*s 3, no. 4: 402–16.

Ramsey, Geoff. 2020. "By indicting Maduro, Trump is kneecapping a transition in Venezuela," *The Washington Post* 27 (March). https://www.washingtonpost.com/opinions/2020/03/27/by-indicting-maduro-trump-is-kneecapping-transition-venezuela/.

Rogin, Josh. 2018. "Bolton promises to confront Latin America's 'Troika of Tyranny'". *The Washington Post* (November). https://www.washingtonpost.com/opinions/global-opinions/bolton-promises-to-confront-latin-americas-troika-of-tyranny/2018/11/01/df57d3d2-ddf5-11e8-85df-7a6b4d25cfbb_story.html.

Rohde, David. 2020. *In Deep: The FBI, the CIA, and the Truth about America's "Deep State"*. New York: W.W. Norton.

Roth, Andrew, and Ellen Nakashima. 2017. "Massive cyberattack hits Europe with widespread ransom demands". *The Washington Post* (June). https://www.washingtonpost.com/world/europe/ukraines-government-key-infrastructure-hit-in-massive-cyberattack/2017/06/27/7d22c7dc-5b40-11e7-9fc6-c7ef4bc58d13_story.html?utm_term=.6f52ad40e788/.

Sanger, David E. 2012. *Confront and Conceal: Obama's Secret Wars and Surprising Use of American Power*. New York City: Crown Publishing Group.

Sanger, David E., and Nicole Perlroth. 2019. "U.S. Escalates Online Attacks on Russia's Power Grid". *New York Times* (June). https://www.nytimes.com/2019/06/15/us/politics/trump-cyber-russia-grid.html.

Schneider, Jacquelyn. 2020. "A Strategic Cyber No-First-Use Policy? Addressing the US Cyber Strategy Problem". *The Washington Quarterly* 43, no. 2: 159–75.

Sequera, Vivian, and Deisy Buitrago. 2019. "Venezuela, blaming U.S. for six--day blackout, orders diplomats to leave". *Reuters* (March). https://www.reuters.com/article/us-venezuela-politics/venezuela-blaming-u-s-for-six-day-blackout-orders-diplomats-to-leave-idUSKBN1QT25W/.

Sheridan, Mary Beth, and Mariana Zuniga. 2019. "In Venezuela, massive blackout continues as Maduro blames U.S. for outages". *The Washington Post* (March). https://www.washingtonpost.com/world/the_americas/venezuelas-devastating-blackout-stretches-into-friday/2019/03/08/10ea8812-4198-11e9-9361-301ffb5bd5e6_story.html.

Spetalnick, Matt. 2019. "Russian Deployment in Venezuela Includes 'Cybersecurity Personnel': U.S. Official". *Reuters* (March). https://www.reuters.com/article/us-venezuela-politics-russians-idUSKCN1R72FX.

Tharoor, Ishaan. 2020. "A Bay of Pigs-style fiasco in Venezuela". *The Washington Post* (May). https://www.washingtonpost.com/world/2020/05/06/bay-pigs-style-fiasco-venezuela/.

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

U.S. Department of Defense. 2018. *Summary: Department of Defense Cyber Strategy 2018.* https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF.

Valeriano, Brandon, and Benjamin Jensen. 2019. "How cyber operations can help manage crisis escalation with Iran". *Washington Post* (June). https://www.washingtonpost.com/politics/2019/06/25/how-cyber-operations-can-help-manage-crisis-escalation-with-iran/.

Valeriano, Brandon, Benjamin Jensen, and Ryan C. Maness. 2018. *Cyber Strategy: The Evolving Character of Power and Coercion.* Oxford: Oxford University Press.

Volz, Dustin. 2018. "Trump, Seeking to Relax Rules on U.S. Cyberattacks, Reverses Obama Directive; Administration has faced pressure to show that it is taking seriously national-security cyberthreats". *The Wall Street Journal* (August). https://www.wsj.com/articles/trump-seeking-to-relax-rules-on-u-s-cyberattacks-reverses-obama-directive-1534378721.

Zetter, Kim. 2014. *Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon.* New York: Crown.

NOTAS

1. This article is part of the project 'Science, Technology and Innovation in Defense: Cybernetics and National Defense,' approved by Public Notice 27/2018, Support Program for Teaching and Scientific and Technological Research in National Defense – PRO-DEFENSE IV.

THE 2019 VENEZUELAN BLACKOUT AND THE CONSEQUENCES OF CYBER UNCERTAINTY

ABSTRACT

In March 2019, Nicolás Maduro claimed that the blackout in Venezuela was caused by U.S. cyber-attacks. This statement was promptly denied by Mike Pompeo, the U.S. Secretary of State. Irrespective of the truth of Maduro's allegation, this episode highlights the diplomatic challenges for states in the contemporary information environment, in which contested narratives proliferate and embed themselves more durably because of the deterritoriality and disintermediation of the Internet. This is particularly true in the context of an emerging pattern of state actors conducting cyber operations against critical infrastructure in other states. The cumulative impact of these different strands is that states will likely struggle to control the perception of their intentions in the cyber domain, not only amongst governments but across the many national audiences that comprise the global public sphere. Focusing on Maduro's allegation, this article analyses the political utility of cyber uncertainty, and its corresponding implications for states' cyber strategies and decisionmaking.

Keywords: Cyberspace; Uncertainty; Cyber Operations; Cyber Defense; Digital Diplomacy.

RESUMO

Em março de 2019, Nicolás Maduro afirmou que o blecaute na Venezuela foi causado por ciberataques perpetrados pelos EUA. Esta declaração foi prontamente negada por Mike Pompeo, Secretário de Estado norte-americano. Independentemente da verdade da alegação de Maduro, este episódio destaca os desafios diplomáticos para os Estados no ambiente de informação contemporâneo, no qual as narrativas contestadas proliferam e se incorporam de maneira mais durável por causa da desterritorialidade e desintermediação da Internet. Isso é particularmente verdadeiro no contexto de um padrão emergente de atores estatais que conduzem operações cibernéticas contra a infraestrutura crítica em outros Estados. O impacto cumulativo dessas diferentes vertentes é que os Estados provavelmente terão dificuldades para controlar a percepção de suas intenções no domínio cibernético, não apenas entre os governos, mas entre os diversos públicos nacionais que compõem a esfera pública global. Focando na alegação de Maduro, este artigo analisa a utilidade política da incerteza cibernética e suas implicações correspondentes nas estratégias e decisões cibernéticas dos Estados.

Palavras-chave: Ciberespaço; Incerteza; Operações cibernéticas; Defesa cibernética; Diplomacia digital.

Recebido em 29/06/2020. Aceito para publicação em 19/04/2021.