Media Fields JOURNAL

Blocked Ports:

Sanctions and Software in Networked Cuba

Sam P. Kellogg

This essay analyzes port blocking as a modular geopolitical technology targeting the disruption of circulation in our networked contemporary. It examines how the US embargo against Cuba manifests in software, where port blocking is adopted by US technology firms as a readymade technique for adhering to aggressive US state sanctions, excising Cuban users from the Internet's connective tissue. After providing a general introduction to port blocking in the context of digital networking today, I turn to the case of the embargo, examining how the appearance of blocked ports and error states in the course of everyday computing in Cuba indexes the US sanctions regime. I describe how blocked ports are often ambiguously encountered by Cubans as generic technical failures rather than as results of a specific foreign regime's policies. I further outline a general theory of port blocking as a modular technology for intervening in flows within networks, one which can be weaponized to enforce political and economic compliance up and down the stack through infrastructural parameters, protocols, and code.

The adoption of the term *port* to designate a conceptual object in computing is closely tied to the Internet's growth and computer networking more broadly. Introduced during the development of the TCP protocol (transmission control program) in 1974—one of two primary protocols (the other being IP) which functionally define the Internet protocol suite—ports are means of defining, differentiating, and organizing inbound and outbound traffic, and are elementary infrastructural components of the Internet.[1] Every data packet sent over the Internet includes a header with an address and port number to ensure it arrives at its intended destination; different protocols and applications are assigned dedicated ports on a single machine (each machine has numerous ports). Successfully sending and receiving data across the network requires that the appropriate ports at either end and those of intermediary machines are open and properly configured. Open ports are a precondition for the transmission and circulation of data online.

Port blocking does precisely what it sounds like, describing a generic and flexible means of severing signal traffic to or from an entity by closing an associated port. This disallows the flow of data to an application, address, user, or location. Common contemporary use cases include network security (blocking ports otherwise vulnerable to attack, as with a firewall) and enforcing terms of service (blocking traffic to an application or machine when a TOS violation is detected, commonly used by ISPs to thwart piracy). Port blocking may "fail loudly," producing evidence of inoperability by inducing an error state, though at times, it is not immediately clear what is wrong. Operating on an infrastructural and protocological register, port blocking tends to occur out of sight of the average user, only indirectly interpretable and diagnosable via graphical interface.

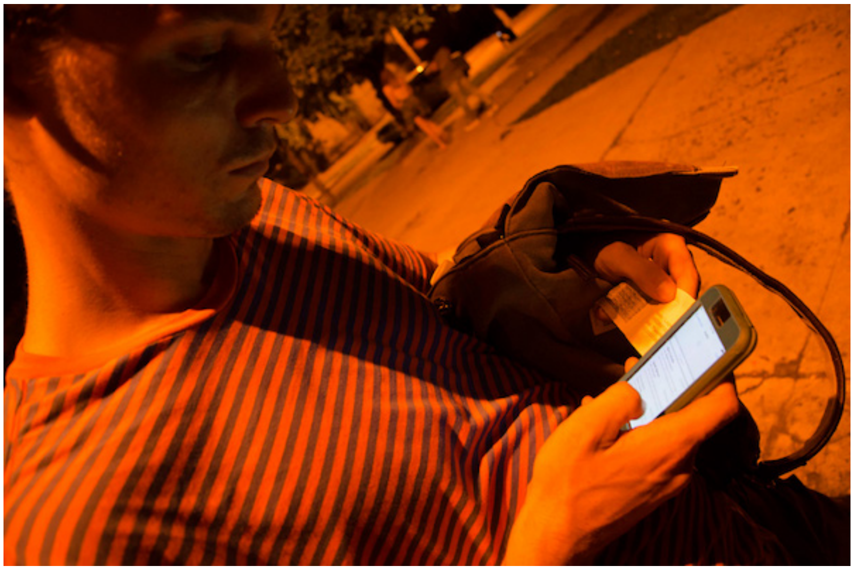
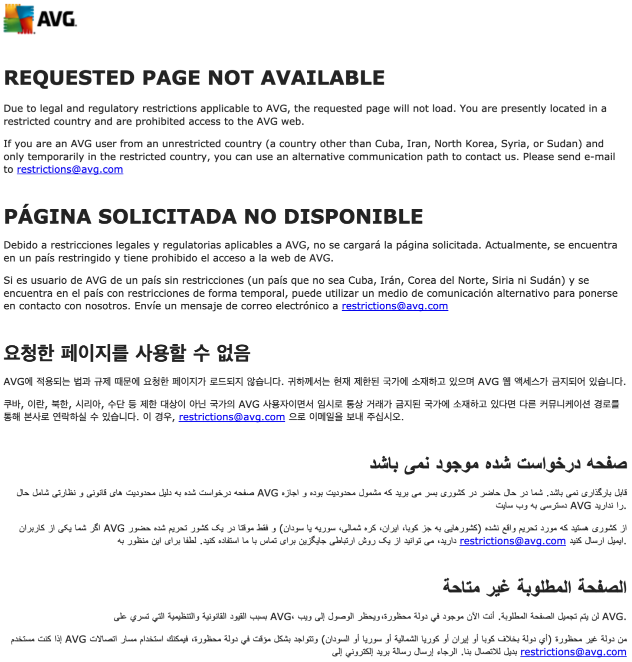


Figure 1. Connecting to public WiFi in Havana. Photo by author, 2017.

In what follows, I build upon past work on Internet-based and Internet-adjacent digital networking practices in Cuba, much of which addresses the resourcefulness of the Cuban digital media landscape under combined conditions of sanctions, governmental inertia, and material scarcity.[2] I situate my work between the intellectual milieus of Havana and New York, cities where I hear remarkably similar conversations about the creep of surveillance, the power of platforms, and the strange character of networked sociality. One of the many crucial differences is on which side of the embargo—or as the Cubans call it, *el bloqueo*—one finds oneself. This factor indelibly shapes one's experience of the Internet and the software used to traverse it. Here, I turn to how the US embargo is made manifest when transposed into the digital sphere, attending to how port blocking is enrolled by software companies as an adaptable and modular technical procedure used to bridge legal and political incongruencies.



REQUESTED PAGE NOT AVAILABLE

Due to legal and regulatory restrictions applicable to AVG, the requested page will not load. You are presently located in a restricted country and are prohibited access to the AVG web.

If you are an AVG user from an unrestricted country (a country other than Cuba, Iran, North Korea, Syria, or Sudan) and only temporarily in the restricted country, you can use an alternative communication path to contact us. Please send e-mail to restrictions@avg.com

PÁGINA SOLICITADA NO DISPONIBLE

Debido a restricciones legales y regulatorias aplicables a AVG, no se cargará la página solicitada. Actualmente, se encuentra en un país restringido y tiene prohibido el acceso a la web de AVG.

Si es usuario de AVG de un país sin restricciones (un país que no sea Cuba, Irán, Corea del Norte, Siria ni Sudán) y se encuentra en el país con restricciones de forma temporal, puede utilizar un medio de comunicación alternativo para ponerse en contacto con nosotros. Envíe un mensaje de correo electrónico a restrictions@avg.com

요청한 페이지를 사용할 수 없음

AVG에 적용되는 법과 규제 때문에 요청한 페이지가 로드되지 않습니다. 귀하께서는 현재 제한된 국가에 소재하고 있으며 AVG 웹 액세스가 금지되어 있습니다.

쿠바, 이란, 북한, 시리아, 수단 등 제한 대상이 아닌 국가의 AVG 사용자이면서 임시로 통상 거래가 금지된 국가에 소재하고 있다면 다른 커뮤니케이션 경로를 통해 본사로 연락하실 수 있습니다. 이 경우, restrictions@avg.com 으로 이메일을 보내 주십시오.

صفحه درخواست شده موجود نمی باشد

قابل بارگذاری نمی باشد. شما در حال حاضر در کشوری بسر می برید که مشمول محدودیت بوده و اجازه AVG صفحه درخواست شده به دلیل محدودیت های قانونی و نظارتی شامل حال
.را ندارید AVG دسترسی به وب سایت

از کشوری هستید که مورد تحریم واقع نشده (کشورهایی به جز کوبا، ایران، کره شمالی، سوریه یا سودان) و فقط موقتا در یک کشور تحریم شده حضور AVG اگر شما یکی از کاربران
.ایمیل ارسال کنید restrictions@avg.com دارید، می توانید از یک روش ارتباطی جایگزین برای تماس با ما استفاده کنید. لطفا برای این منظور به

الصفحة المطلوبة غير متاحة

.AVG لن يتم تجميل الصفحة المطلوبة. أنت الآن موجود في دولة محظورة، ويحظر الوصول إلى ويب AVG، بسبب القيود القانونية والتنظيمية التي تسري على

من دولة غير محظورة (أي دولة بخلاف كوبا أو إيران أو كوريا الشمالية أو سوريا أو السودان) وتتواجد بشكل مؤقت في دولة محظورة، فيمكنك استخدام مسار اتصالات AVG إذا كنت مستخدم
restrictions@avg.com بديل للاتصال بنا. الرجاء إرسال رسالة بريد إلكتروني إلى

Figure 2. Screenshot of AVG's "Product not available" webpage.[3]

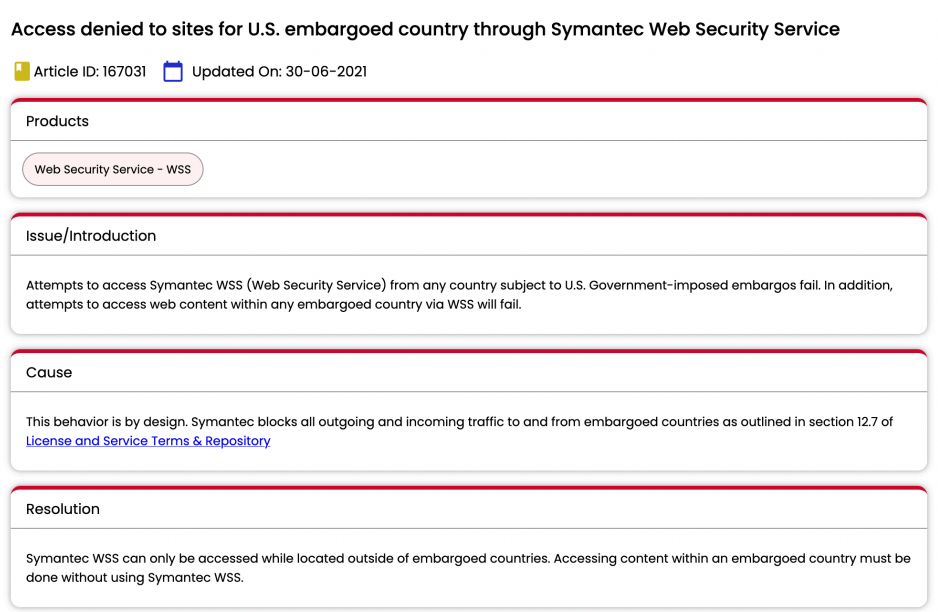
When it is seen directly within consumer software or online, the US embargo most often appears as an error message at the level of the interface, triggered by a blocked port at the level of network infrastructure. Consider the example shown above. In 2012, while studying in Havana, I realized it had been a month or two since I had updated my antivirus software. I clicked

"Update," and my web browser opened to a page like the one above. This notification gives more information than most used by similar companies, and is even translated into relevant languages: Spanish, Korean, Farsi, Arabic. The message reads, "Due to legal and regulatory restrictions applicable to AVG, the requested page will not load. You are presently located in a restricted country and are prohibited access."[4]

As a US company, AVG must comply with US trade law. In the Cuban context, this includes the Trading with the Enemy Act of 1917, the Cuban Democracy Act of 1992, the Helms-Burton Act of 1996, and a number of other statutes listed by the US Department of the Treasury's Office of Foreign Asset Control (OFAC) which collectively constitute the embargo's legal corpus.[5] Though it is frequently discussed as a singular legal apparatus, the embargo is in fact far from a monolithic object; assembled from myriad complementary pieces of legislature and enforcement mechanisms, the embargo is akin to a juridical Frankenstein.[6] Taken together, however, these elements constitute a remarkably totalizing work of law. As Joy Gordon notes, US sanctions against Cuba "are deliberately overbroad in every aspect [. . . they] are as thoroughgoing and indiscriminate as it is possible to be."[7]

The transposition of this legal apparatus into the digital sphere entails new problems of interpretation: does serving HTML to a machine with a Cuban IP address count as trading with the enemy? What about allowing a free software application to be downloaded by someone on the island? Rather than risk incurring heavy fines associated with breaking US trade law, many companies have designed policies of proactive denial-of-service: a tendency towards preemptive and indiscriminate port blocking that mirrors the heavy-handed and overbroad character of the sanctions themselves.

In Cuba, of course, the embargo is far from abstract, profoundly restricting the daily availability of food, medicine, and information. Cristina Venegas argues that the embargo contributes to an entire "embargo culture," noting that "life under sanctions has colored the experience of many generations."[8] Like a dark cloud on the horizon, the embargo is obliquely omnipresent, persistently felt and endured. The Internet merely adds another dimension to how the embargo is encountered in everyday life.



Access denied to sites for U.S. embargoed country through Symantec Web Security Service

Article ID: 167031 Updated On: 30-06-2021

Products

Web Security Service - WSS

Issue/Introduction

Attempts to access Symantec WSS (Web Security Service) from any country subject to U.S. Government-imposed embargos fail. In addition, attempts to access web content within any embargoed country via WSS will fail.

Cause

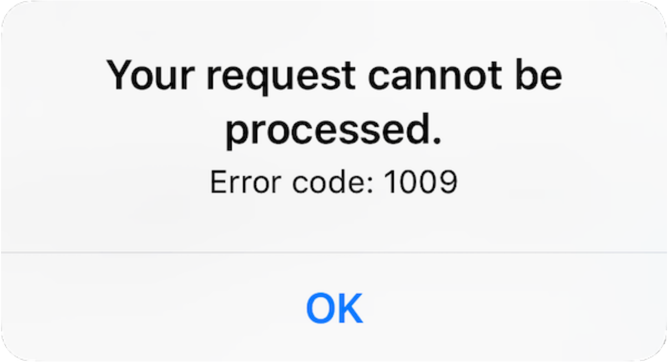
This behavior is by design. Symantec blocks all outgoing and incoming traffic to and from embargoed countries as outlined in section 12.7 of License and Service Terms & Repository

Resolution

Symantec WSS can only be accessed while located outside of embargoed countries. Accessing content within an embargoed country must be done without using Symantec WSS.

Figure 3. Screenshot from Broadcom's support site.[9]

Symantec, another US antivirus product, likewise forbids anyone in sanctioned countries from using their software, regardless of how and where it was originally procured or whether any money changed hands. Broadcom, Symantec's parent company, hosts an article about sanctions on its support website complete with an ID number, internalizing the embargo itself into its technical issue filing system as though geopolitical struggles were reducible to a series of compatibility or localization issues. The failure of the software, meanwhile, is quite explicitly "by design."[10]



Your request cannot be processed.

Error code: 1009

Figure 4. Screenshot of Apple's 1009 error message.

One final example from Apple's App Store should drive home just how abnormal of a condition the embargo is within the world of software, as both a productive externality and a disabling condition. If an attempt is made from Cuba to use an unmodified iPhone to download or update an app, even a free one, the user will be met with the message above: no explanation, simply the generic fact that the request could not be processed along with an opaque error code. The user is left with no choice but to acknowledge their wretched position: "OK."

In all of these examples, well-established paradigms for port blocking and error handling in software development are appropriated by companies to address the geopolitical condition of sanctions. Like Broadcom and AVG, Apple pursues something akin to infrastructural self-sabotage as a matter of policy, adapting the modular technique of port blocking to resolve a contradiction: that between a desire to sell software to anyone, anywhere, and a legal regime which explicitly forbids it. In such cases, the appearance of an error message is itself somewhat misleading: the software is functioning exactly as designed so as to protect companies from legal liability, even if, from a user's perspective, the software is unusable.

It may be instructive here to further classify the errors encountered by users which result from geopolitically motivated port blocking. Olga Goriunova and Alexei Shulgin distinguish three general error structures in software: "syntax errors (grammatical errors in a program), logic errors (errors in an algorithm), and exception errors (arising from unexpected conditions and events)."[11] Syntax errors might emerge from typos, for example, while logic errors occur when the program has resolved correctly in a semantic and syntactic sense but has yielded an output different from that intended by the programmer. For instance, a program might divide rather than multiply, or sort a list but do so backward. Last, exception errors are understood as happening during program execution or runtime. Matthew Fuller and Andrew Goffey elaborate on the software exception: "In the technical sense, exceptions arise when a piece of code—perhaps a class in an object-oriented programming language—encounters an *abnormal condition* that it cannot handle, when an event occurs that lies outside the expected range of possibilities that code is expected to cope with."[12] Exception errors thus designate abnormalities or deviances from prevailing norms, pointing to software's possibilities for juridical enforcement as well as to the problem of software's "outside," an outside which remains unruly. Much software pulls resources from elsewhere, such as the Internet or user input. If counted-on resources are not properly formatted or unavailable, then the situation is termed exceptional.

Port blocking often induces exception errors in software by blocking access to required connections or resources. They are symptoms of a contradiction between the opportunistic and aspirational universalism of consumer software and an antagonistic political and legal regime that forbids exchange with entities labeled enemies (exchange of goods but also, functionally, of information). In principle, much software is designed to work everywhere—these are the imagined conditions of borderless scalability and total market saturation where everyone is a potential user and the global network sparkles with untapped value. In this ideal world, all locations and all IP addresses are equally valid: Castro never expropriated US oil refineries, and Kennedy never invaded the Bay of Pigs. According to the rubrics of capitalist cyberspace, sanctions are exceptional anomalies, and a means of retroactively breaking the software—of ensuring that the company is not held liable for violating the embargo—must be introduced without undermining the coherence of the application itself. When a request is judged as originating from a sanctioned locale, the connection is severed by blocking a piece of critical infrastructure: the port. Port blocking thus functions as a readymade political sieve or filter introduced at a chokepoint: a modular technical procedure appropriated as a means of legal compliance, satisfying the whims of the prevailing legal regime while maintaining the software's aspirational universality.

In the case of the embargo, port blocking performs an active geopolitical role: a technical solution to a problem posed by politics and codified by law. The embargo is something "outside" that must nonetheless be accounted for. The strategic deployment of error-inducing blocked ports protects the company from liability while simultaneously upholding the aggressive political mandate of the United States. Like a gunship stationed offshore that never actually fires a shot, the purpose is to exclude and excise, maintaining rule by isolating the offending entity, cutting it off from the rest of the network.

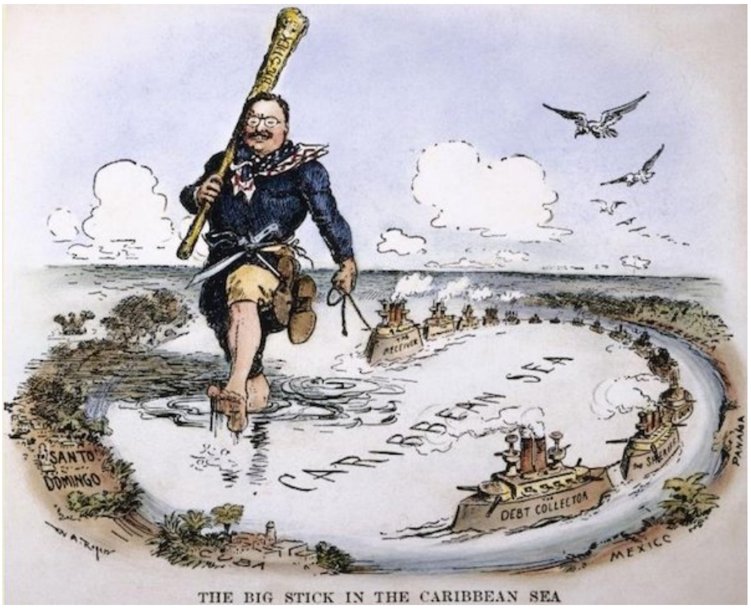


Figure 5. 1904 political cartoon by William Allen Rogers satirizing US naval power in the Caribbean under Theodore Roosevelt.[13]

Port blocking remains an emblematic tool of economic warfare and imperial ambition today, as it was, in a different sense, in nineteenth and twentieth-century gunboat diplomacy. In the Caribbean and elsewhere, naval blockades have long been used to enforce the interests of foreign powers by cutting supply lines and impeding the flow of goods and information. The concept and terminology of the port were first adopted metaphorically and logically by engineers in the 1970s to organize inbound and outbound network traffic. With network port blocking and related techniques of monitoring and management, the port's prominence as a site of geopolitical intervention has hardly diminished. Functioning much like Gilles Deleuze's sieve in his essay on control societies, port blocking dynamically modulates access depending on whether various criteria are met: a tool of surgical economic warfare proper to an era of "smart sanctions" and distributed regimes of algorithmic governance.[14]

In the context of US-Cuban relations today, port blocking constitutes an intentionally designed modular technique in the digital infrastructure of the embargo, as well as a mechanism for the protection of opportunistic US corporations for whom everyone is, by default, a potential customer, user, or data point. On its own, the fact of blocked ports both communicates something—it symbolizes the presence of the embargo in software—and simultaneously materializes, in practice, that which the embargo *is* and *does*.

What does an embargo do but erect a systematic process of denial and isolation? As a well-established technical practice in software development, port blocking is easily conscripted by engineers to carry out the geopolitical boundary work that governments require. It can be seen simultaneously as both a continuation and a rupture, a transposition of the US's sixty-year policy of denying Cuban sovereignty onto the distributed context of the digital network.

In a more general sense, port blocking can be thought of as a technique for interrupting circulation at a targeted point or interface, useful in any situation organized according to a networked logic of links, flows, and nodes. Since it is targeted, port blocking is contingent upon the presence of chokepoints (the ports themselves), emblematic features of what Elizabeth Cullen Dunn has termed vascular geopolitics—"a geopolitics based on the control of circulation rather than on the control of territory."[15] Among the simplest possible means of impeding inbound or outbound traffic to a given network node, port blocking can be exploited for a wide variety of political ends: to strategically deny the transmission of information to or from a target device, network, or region, or—in post-Fordist contexts in which the transmission of information is also frequently the transmission of value—to double as a means of enforcing economic compliance and hegemony via the strategic exclusions of entities deemed abnormal.

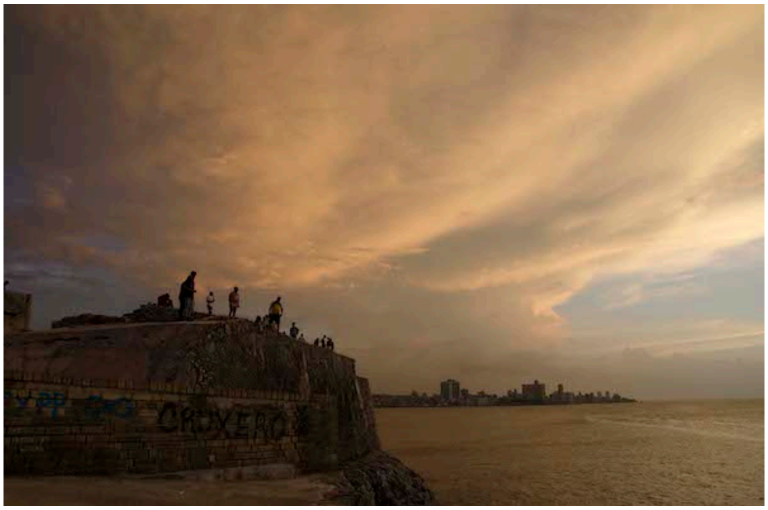


Figure 6. Looking across the mouth of Havana harbor from the *Morro*, a Spanish fort built to protect the city's port. Photo by author, 2017.

However, as with any technique of power, port blocking is not insurmountable, and for Cubans, the digital embargo can often be overcome more easily than the embargo on traditional commodities. VPNs, proxies, aftermarket modifications, and parallel networks are all used to reroute, disguise, or obviate the need for traffic, dampening the embargo's digital effects. In networked geopolitical struggles targeting the control of flows, blocked connections tend to induce the search for new ones.[16] The "tangled ball of yarn" that Fidel Castro once dubbed US-Cuba relations thus seems far from being unraveled, and the architecture of the embargo appears more coiled than ever in the Internet age.[17] If the distributed network is indeed the reigning political diagram of our age—a diagram in which interconnection is both telos and valorized condition—then port blocking may be thought of as a modular, surgical technique operating on its vascular tangles of circulation and distribution: an algorithmic excision, and a unilateral political severing, of an antagonistic relation.[18]

Acknowledgements

Thanks to the editors of *Media Fields*, to two anonymous reviewers, and to Alejandra Bronfman, Jeanne Etelain, Nicole Starosielski, and my colleagues in MCC's Fall 2020 doctoral seminar for their generous comments on drafts of this essay. Thanks to my excellent co-panelists at SIGCIS 2019—Ginevra Sanvitale, Rory Solomon, Sarah Myers West, and Gili Vidan—where an early version of this work was presented. I am also grateful for a Tinker Field Research Grant which helped fund my research in Cuba in 2017, and for a Doctoral Travel Grant from NYU which allowed me to attend SIGCIS in 2019.

Notes

1 To quote Vint Cerf and Robert Khan, who first appropriated the term while developing the TCP protocol, "We introduce the notion of *ports* in order to permit a process to distinguish between multiple message streams. The port is simply a designator of one such message stream associated with a process." Further on: "A pair of ports will exchange one or more messages over a period of time. We could view the sequence of messages produced by one port as if it were embedded in an infinitely long stream of bytes." Vinton G. Cerf and Robert E. Kahn, "A Protocol for Packet Network Intercommunication," *IEEE Transactions on Communications* 22, no. 5 (1974): 637–48. See also: Network Working Group, "Specification of Internet Transmission Control Program," Internet Engineering Task Force Request for Comments, December 1974.

2 Much past scholarship, including my own, has approached the Cuban digital media landscape from the perspective of everyday users or independent journalists, emphasizing the Cuban capacity to *inventar* and *resolver*—to overcome difficulties and circumvent obstacles. This paper instead attempts to theorize port blocking as a modular technique deployed by powerful entities like states and corporations as

engendering a need for such tactics of circumvention in the first place. Anglophone readers interested in the Cuban context are encouraged to begin with Cristina Venegas, *Digital Dilemmas: The State, the Individual, and Digital Media in Cuba* (New Brunswick: Rutgers University Press, 2010); Ted A. Henken and Sara Garcia Santamaria, *Cuba's Digital Revolution: Citizen Innovation and State Policy* (Gainesville: University of Florida Press, 2021); and the special dossier on *el paquete* edited by Jennifer Cearns in *Cuban Studies* 50 (2021).

3 AVG, "Requested Page Not Available," AVG, static.avg.com/restricted-not-available (accessed February 2022).

4 Ibid.

5 United States Department of the Treasury, "Cuba Sanctions," United States Department of the Treasury, home.treasury.gov/policy-issues/financial-sanctions/sanctions-programs-and-country-information/cuba-sanctions (accessed February 2022).

6 William M. LeoGrande, "A Policy Long Past Its Expiration Date: US Economic Sanctions Against Cuba," *Social Research: An International Quarterly* 82, no. 4 (2015), 939–66.

7 Joy Gordon, "The Invisibility of Human Harm: How Smart Sanctions Consumed All the Oxygen in the Room," *Social Research: An International Quarterly* 82, no. 4 (2015), 863.

8 Venegas, *Digital Dilemmas*, 24.

9 Broadcom, "Access Denied to Sites for U.S. Embargoed Country through Symantec Web Security Service," Broadcom, 30 June 2021, knowledge.broadcom.com/external/article?legacyId=tech242821.

10 Ibid.

11 Olga Goriunova and Alexei Shulgin, "Glitch," in *Software Studies: A Lexicon*, ed. Matthew Fuller (Cambridge, MA: The MIT Press, 2008), 111.

12 Matthew Fuller and Andrew Goffey, *Evil Media* (Cambridge, MA: The MIT Press, 2012), 118.

13 William Allen Rogers, "Theodore Roosevelt and His Big Stick in the Caribbean" (1904); "The Price of Freedom: Americans at War," National Museum of American History, americanhistory.si.edu/price-of-freedom/spanish-american-war/defeating-spain-philippines (accessed February 2022).

14 "Enclosures are *molds*, distinct castings, but controls are a *modulation*, like a self-deforming cast that will continuously change from one moment to the other, or like a sieve whose mesh will transmute from point to point." Gilles Deleuze, "Postscript on the Societies of Control," *October* 59 (1992), 5.

15 Elizabeth Cullen Dunn, "Warfare and Warfarin: Chokepoints, Clotting and Vascular Geopolitics," *Ethnos* (2020), 2.

16 See note 2.

17 William M. LeoGrande and Peter Kornbluh, *Back Channel to Cuba: The Hidden History of Negotiations between Washington and Havana* (Chapel Hill, NC: University of North Carolina Press, 2014), 203.

18 On the distributed network as a political diagram, see: Alexander R. Galloway, *Protocol: How Control Exists after Decentralization* (Cambridge, MA: The MIT Press, 2004), 3.

Sam P. Kellogg is a writer, researcher, editor, teacher, and trekking guide. He is a PhD candidate in the department of Media, Culture, and Communication at New York University. When not on a mountain, he lives in Rockaway Beach, New York City. His website is samkellogg.com.