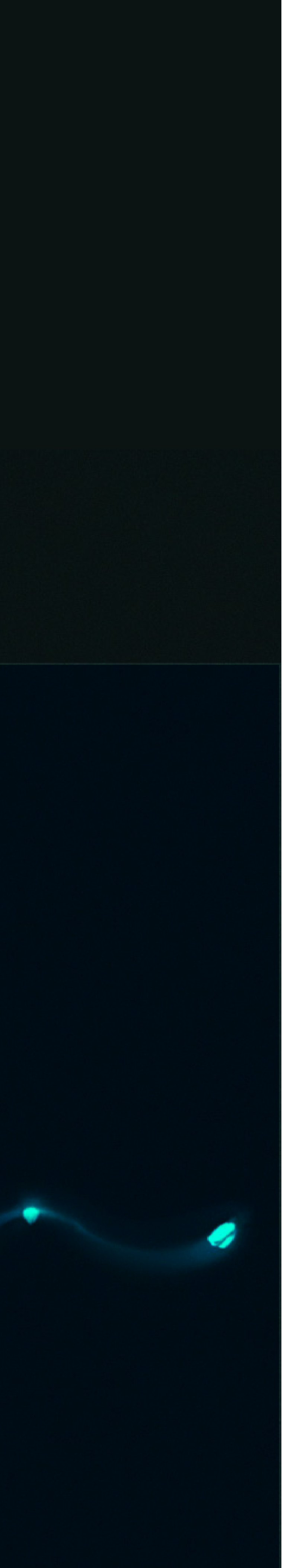
CYBER STATECRAFT INITIATIVE

DFRLab

DRAGON TAILS: Preserving International Cybersecurity Research

Stewart Scott, Sara Ann Bracket, Yumi Gambrill, Emmeline Nettles, and Trey Herr



CYBER STATECRAFT
INITIATIVE

DFRLab

The Cyber Statecraft Initiative works at the nexus of geopolitics and cybersecurity to craft strategies to help shape the conduct of statecraft and to better inform and secure users of technology. This work extends through the competition of state and non-state actors, the security of the internet and computing systems, the safety of operational technology and physical systems, and the communities of cyberspace. The Initiative convenes a diverse network of passionate and knowledgeable contributors, bridging the gap among technical, policy, and user communities.

The mission of the **Digital Forensic Research Lab (DFRLab)** is to identify, expose, and explain disinformation where and when it occurs using open-source research; to promote objective truth as a foundation of government for and by people; to protect democratic institutions and norms from those who would seek to undermine them in the digital engagement space; to create a new model of expertise adapted for impact and real-world results; and to forge digital resilience at a time when humans are more interconnected than at any point in history, by building the world's leading hub of digital forensic analysts tracking events in governance, technology, and security.

This report is written and published in accordance with the Atlantic Council Policy on Intellectual Independence. The author is solely responsible for its analysis and recommendations. The Atlantic Council and its donors do not determine, nor do they necessarily endorse or advocate for, any of this report's conclusions.

ISBN-13: 978-1-61977-247-2

Atlantic Council
1030 15th Street NW, 12th Floor
Washington, DC 20005

For more information, please visit
www.AtlanticCouncil.org.

Cover image licensing language: CSI produced this report's cover image using in part OpenAI's DALL-E program, an AI image-generating application. Upon generating the draft image-prompt language, the authors reviewed, edited, and revised the language to their own liking and take ultimate responsibility for the content of this publication.

CYBER STATECRAFT INITIATIVE

DFRLab

DRAGON TAILS:
Preserving International Cybersecurity Research

Stewart Scott, Sara Ann Bracket, Yumi Gambrill,
Emmeline Nettles, and Trey Herr

EXECUTIVE SUMMARY

Cybersecurity, writ large, benefits enormously from an international community of researchers, hackers, and bug hunters. They find and disclose critical vulnerabilities, often responsibly, while working outside affected vendors or codebases. Yet, the policy debates that shape the legal environment around vulnerability disclosure often fail to consider cybersecurity as a function of both the supply of vulnerability research and the health of those research communities. This paper analyzes a series of Chinese regulatory changes altering vulnerability disclosure practices to assess their impact on the supply of research from China's significantly productive community. The paper examines disclosure data from a mix of proprietary and open-source codebases, looking across vendor and software types with a simple time-series analysis to look for the impact of recent Chinese regulations. The study of this data revealed that while national regulations do indeed affect the supply of vulnerability research under some circumstances, the effect is not as large, consistent, or discernible as might first be expected. The prospect of copycat regulations, however, motivates concluding policy recommendations focused on strengthening the health of the global vulnerability-research community and lowering barriers-to-entry for both research and disclosure.

ACKNOWLEDGMENTS

The authors of this report would like to thank Winnona DeSombre, Art Manion, Allen Householder, Nick Reese, Dakota Cary, John Speed Meyers, Chris Rohlf, Jarek Stanley, Sasha Romanosky, Jantje Silomon, Mischa Hansel, and Matthew Tompkins for their feedback and insight during the development of this report. Thank you to Nancy Messiah and Andrea Raitu for data visualization and web design and to Donald Partyka for graphic and document design.

TABLE OF CONTENTS

For more on this project and the datasets behind it, visit us on the web **here**.

INTRODUCTION

One complicated reality of cybersecurity is the sheer volume of vulnerability disclosure to technology vendors and open-source projects that originates outside these organizations. Indeed, the notion originally articulated by Eric Raymond and credited as Linus' Law, that "given enough eyeballs, all bugs are shallow," is a central part of the open-source ecosystem's security model.[1] What often goes underappreciated is that these "eyes" may belong to the same person or people frequently examining the same or related codebases—the global distribution of eyes is uneven. Bug-bounty programs often show disproportionate contributions from a small number of people and countries, as some are home to comparatively more active researcher communities.[2]

One of the most prolific of these communities is that in China. For at least a decade, Chinese corporate research teams and individual researchers have dominated marquee hacking competitions and corporate bounty programs, scouring everything from browsers and mobile operating systems to networking gear. Their dominance in hacking competitions halted abruptly in 2018, when China blocked its researchers from participating in such events abroad.[3] Soon after, the Regulations on the Management of Network Product Security Vulnerabilities, or RMSV for short, took effect in September 2021. The law requires Chinese network product providers to notify the country's Ministry of Industry and Information Technology (MIIT) about vulnerabilities found in "network products"[4] within a few days of reporting them to the appropriate vendor.[5] As 2021 wound to a close, the legal environment for Chinese vulnerability research appeared fraught with the potential for a chilling effect caused by the ambiguities and requirements within the RMSV.

Enter Log4j. At the end of 2021, a bug in the popular logging library Log4j came into the public view as vendors raced to patch millions of vulnerable devices and applications—by some estimates, 10 percent of digital systems, including servers, web applications, Internet-of-Things (IoT) devices and more, were vulnerable.[6] Amid the ensuing tumult—White House summits,[7] Congressional testimony,[8] national directives,[9] and desperate calls for patching—a somewhat surprising strand in the saga went largely undiscussed. In late November 2021, a researcher at Chinese technology giant Alibaba a severe vulnerability in Log4j and disclosed it privately to the Apache Software Foundation (ASF) team maintaining the library. A month later, Alibaba found itself on the receiving end of government sanction. China's Ministry of Industry and Information Technology suspended subsidiary Alibaba Cloud from a cyber threat- and information-sharing

[1] Eric S. Raymond, *The Cathedral & the Bazaar: Musings on Linux and Open Source by an Accidental Revolutionary* (O'Reilly Media, Inc., 2001).

[2] *China's Cyber Capabilities: Warfare, Espionage, and Implications for the United States, Before the US-China Economic and Security Review Commission*, 117th Cong. (2022) (statement of Dakota Cary, research analyst, Center for Security and Emerging Technology), https://www.uscc.gov/sites/default/files/2022-02/Dakota_Cary_Testimony.pdf.

[3] Chris Bing, "China's Government Is Keeping Its Security Researchers from Attending Conferences," CyberScoop, March 8, 2018, https://www.cyberscoop.com/pwn2own-chinese-researchers-360-technologies-trend-micro/.

[4] Cyberspace Administration of China (CAC), "Notice of the Ministry of Industry and Information Technology and the State Internet Information Office of the Ministry of Public Security on Issuing the Regulations on the Management of Security Vulnerabilities of Network Products-Office of the Central Committee of the Communist Party of China," Pub. L. No. No. 66 (2021), http://www.cac.gov.cn/2021-07/13/c_1627761607640342.htm.

[5] To the reader, because there are several translations of the title, one might also find sources calling the RMSV "Regulations on the Management of Network Product Security Vulnerability," "the vulnerability disclosure provisions of the Data Security Law," "Provisions on Security Loopholes of Network Products," or any other number of synonyms.

[6] Amit Yoran, "One in 10 Assets Assessed Are Vulnerable to Log4Shell," Tenable (blog), December 22, 2021, https://www.tenable.com/blog/one-in-10-assets-assessed-are-vulnerable-to-log4shell?utm_source=charge&utm_medium=social&utm_campaign=internal-comms.

[7] "Readout of White House Meeting on Software Security," The White House, January 13, 2022, https://www.whitehouse.gov/briefing-room/statements-releases/2022/01/13/readout-of-white-house-meeting-on-software-security/.

[8] "Responding to and Learning from the Log4Shell Vulnerability" (Washington, DC, February 8, 2022), https://www.hsgac.senate.gov/hearings/responding-to-and-learning-from-the-log4shell-vulnerability.

[9] Cybersecurity and Infrastructure Security Agency (CISA), "Emergency Directive 22-02 Mitigate Apache Log4J Vulnerability," ED 22-02 (2022), https://www.cisa.gov/emergency-directive-22-02.

partnership for six months, apparently for failing to report the Log4j vulnerability, also known as Log4Shell, directly and promptly to the MIIT.[10], [11]

The precise enforcement mechanism behind Alibaba's suspension remains unclear in the sparse reporting on the incident. The MIIT may have cited a clause in the company's contract for the government-facing information-sharing platform, or it may have relied on the aforementioned RMSV, published in July 2021.[12] Legal mechanisms aside, and disregarding the concurrent rifts between the Chinese government and Alibaba, which has been on the losing end of massive antitrust fines recently,[13] an uncomfortable and under-addressed fact remains: the MIIT appears to have punished Alibaba, a titanic cybersecurity entity, for following what were by all accounts best practices, or at least something close to them. This augurs poorly for the supply of vulnerability research originating in China, and thus the security of software including open source and its "many eyes." The law has the potential to either funnel vulnerability information to the MIIT well ahead of industry-standard timelines or to create "a chilling effect on future coordinated disclosure" [14] in one of the world's largest information technology (IT) hubs.

Community Impact, Not National Intent

Chen Zhaojun, a researcher with Alibaba Cloud's security team, reported Log4Shell to ASF privately via email on November 24, 2021. Just weeks later—by December 9—he followed up with an alert that discussion of the bug was percolating through cybersecurity fora.[15] Coordinated vulnerability disclosure (CVD) refers to the process in which discoverers pass vulnerability information to various vendors, affected entities, and eventually the public. Given the many overlapping stakeholders in any software ecosystem, CVD is messy, and as in the case of Log4Shell, does not end after a single communication. As Carnegie Mellon University's CERT Coordination Center (CERT CC) puts it, "there is no single 'right' way to do this."[16] Certainly though, it is difficult to consider Alibaba's approach to Log4Shell "wrong" in any sense pertinent to current CVD norms. Alibaba's researcher disclosed Log4Shell, a vulnerability easily exploitable through many vectors including chat messages on Minecraft servers, to those best suited to remediate it—the ASF team maintaining the library. Alibaba kept the information close for a relatively short time, well within the thirty-day window allowed by, say, Google's Project Zero, and it communicated important developments regarding public knowledge of the vulnerability.[17]

[10] Sophie Yu and Eduardo Baptista, "China Regulator Suspends Cyber Security Deal with Alibaba Cloud," ed. Gerry Doyle, *Reuters*, December 22, 2021, https://www.reuters.com/world/china/china-regulator-suspends-cyber-security-deal-with-alibaba-cloud-2021-12-22/.

[11] Southern Finance and Economics, "Exclusive | Alibaba Cloud Is Suspended from the Ministry of Industry and Information Technology's Network Security Threat Information Sharing Platform Cooperation Unit – 21 Finance," December 22, 2021, https://m.21jingji.com/timestream/html/%7BU9Pjf0FaKEU=%7D.

[12] To the reader, an anonymous source familiar with the matter indicated the former possibility was more likely, which was reiterated by reporting from the *Wall Street Journal*, though the text of the RMSV law, found in Appendix III of this paper, seems equally applicable. See David Uberti and Liza Lin, "Alibaba Employee First Spotted Log4j Software Flaw but Now the Company Is in Hot Water With Beijing," *Wall Street Journal*, December 22, 2021, https://www.wsj.com/articles/china-halts-alibaba-cybersecurity-cooperation-for-slow-reporting-of-threat-state-media-says-11640184511. Other reporting refers to enforcement of the RMSV rather than contract clauses—see Phil Muncaster, "Alibaba Suffers Government Crackdown Over Log4j," *Infosecurity Magazine*, December 23, 2021, https://www.infosecurity-magazine.com/news/alibaba-suffers-government/. Regardless of the precise legal lever used, the source of the apparent sanction was Alibaba's failure to share the vulnerability with the MIIT more promptly, per the company's own statement, cited in Xinmei Shen's article, "Apache Log4j Bug: Alibaba Cloud Vows to Boost Compliance after Chinese Ministry Pulls Support for Not First Reporting Security Issue to Government," *South China Morning Post*, December 23, 2021, https://www.scmp.com/tech/big-tech/article/3160854/apache-log4j-bug-alibaba-cloud-vows-boost-compliance-after-chinese.

[13] Raymond Zhong, "China Fines Alibaba $2.8 Billion in Landmark Antitrust Case," *New York Times*, April 9, 2021, https://www.nytimes.com/2021/04/09/technology/china-alibaba-monopoly-fine.html.

[14] Cyber Safety Review Board, "Review of the December 2021 Log4j Event" (Arlington, VA: Department of Homeland Security, Cybersecurity and Infrastructure Security Agency, July 11, 2022), https://www.cisa.gov/sites/default/files/publications/CSRB-Report-on-Log4-July-11-2022_508.pdf.

[15] Uberti and Lin, "Alibaba Employee First Spotted Log4j Software Flaw but Now the Company Is in Hot Water with Beijing."

[16] Allen D Householder et al., "The CERT Guide to Coordinated Vulnerability Disclosure" (Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University, August 2017), 4, https://resources.sei.cmu.edu/asset_files/specialreport/2017_003_001_503340.pdf.

[17] Elizabeth Montalbano, "Google Project Zero Cuts Bug Disclosure Timeline to a 30-Day Grace Period," *Threatpost*, April 16, 2021, https://threatpost.com/google-project-zero-cuts-bug-disclosure-timeline-to-a-30-day-grace-period/165432/.

Deep, legitimate concerns exist about the intent of requirements to provide advanced notice of vulnerabilities to government agencies. This is especially true where those government agencies are implicated in harvesting vulnerabilities for offensive use from national databases and hacking competitions, [18], [19] all under a framework conceiving of vulnerabilities as a national resource.[20] Concerns over state access to vulnerabilities and influence on disclosure practices are not limited to China.[21], [22] However, this paper considers these regulations through a different lens: their impact on the supply of vulnerability disclosures worldwide.

CVD—The Big Picture

Researchers ranging from hobbyists to enterprise lab technicians hunt for vulnerabilities in products, open-source libraries, and embedded software. They have a variety of motivations: profit, prestige, ethical principles, and even entertainment.[23] Testaments to the importance of this thriving, distributed, community are widespread: bug bounty programs and platforms like HackerOne or EU-FOSSA 2, tomes of acknowledgments for external researchers in common vulnerabilities and exposures (CVE) records, and even the remarkable innovation of the open-source ecosystem itself, premised on the open and free flow of contributions from researchers and developers to projects and their maintainers.

If many eyes can better find vulnerabilities, then the global supply of security research—the product of these "eyes"—is essential to managing the level of risk posed by software to users. Regulations that might constrict this supply or limit its global reach are thus concerning. While much previous work has focused on the intricacies of vulnerability disclosure in a specific, transactional frame,[24] this paper takes an aggregate approach, concerned less with edge cases than the net effect of new laws on total vulnerability supply. The focus here is on the effect of the RMSV on research. Because Chinese researchers are such a significant proportion of the supply of vulnerability disclosures, and because the law offers a clear set of exogenous intervention dates, the possible effects of the RMSV are a critical case study for policymakers—if they exist, they should be relatively easy to detect and correlate to underlying events.

This paper seeks to answer whether the RMSV had any measurable effects on the supply of either global or Chinese vulnerability research.[25] The analysis measures whether such effects are detectable in publicly available vulnerability-reporting and crediting data from a selection of proprietary vendors and open-source libraries. First, the paper offers a brief, international history of policies and laws impacting vulnerability disclosure before diving into the RMSV. The second section examines statistical findings on the effect of the RMSV and discusses data gathering and analytic methodology. Finally, the paper provides recommendations for the US government and its allies to consider as they update policies impacting vulnerability disclosure in the context of the current administration's significant efforts to improve the security of software and IT supply chains.[26], [27] The report does not seek to indict any one country's approach to cybersecurity. Rather, it attempts to detect fragility in the global supply of vulnerability disclosures through accessible disclosure and acknowledgment data to highlight the subject law, its effects, and the need for policies to better encourage vulnerability disclosure outside of any single, national legal context by bolstering the wider research community's health and vitality.

[18] Priscilla Moriuchi and Bill Ladd, "China Altered Public Vulnerability Data to Conceal MSS Influence," *Recorded Future*, March 9, 2018, https://go.recordedfuture.com/hubfs/reports/cta-2018-0309.pdf.

[19] Patrick Howell O'Neill, "How China Turned a Prize-Winning IPhone Hack against the Uyghurs," *MIT Technology Review*, May 6, 2021, https://www.technologyreview.com/2021/05/06/1024621/china-apple-spy-uyghur-hacker-tianfu/.

[20] Dakota Cary (@DakotaInDC), "Today Is My Last Day at @CSETGeorgetown...," Twitter, April 22, 2022, 11:05 a.m., https://twitter.com/DakotaInDC/status/1517519983718256640.

[21] Will Loomis and Stewart Scott, "A Role for the Vulnerabilities Equities Process in Securing Software Supply Chains," Lawfare Institute, January 11, 2021, https://www.lawfareblog.com/role-vulnerabilities-equities-process-securing-software-supply-chains.

[22] Mandiant, "Advanced Persistent Threats (APTs) | Threat Actors & Groups," Mandiant, accessed August 2, 2022, https://www.mandiant.com/resources/insights/apt-groups.

[23] Erik Silfversten et al., *The Economics of Vulnerability Disclosure* (Athens, Greece: ENISA, 2018), 28, https://www.enisa.europa.eu/news/enisa-news/the-economics-of-vulnerability-disclosure.

[24] Silfversten et al., *The Economics of Vulnerability Disclosure*.

[25] To the reader, with such effects, the paper also works to understand what, if any, characteristics of these effects varied with respect to vendors, product types, codebases, and contributions rates.

[26] President Joseph Biden, Executive Order, "Improving the Nation's Cybersecurity, Executive Order 14028 of May 12, 2021," *Federal Register*, 86, no. 93 (May 17,2021): 26633–47, https://www.govinfo.gov/content/pkg/FR-2021-05-17/pdf/2021-10460.pdf.

[27] Shalanda Young and Chris Inglis, "M-22-16 | Memorandum for the Heads of Executive Departments and Agencies: Administration Cybersecurity Priorities for the FY 2024 Budget," July 22, 2022, https://www.whitehouse.gov/wp-content/uploads/2022/07/M-22-16.pdf.

MAKING LAW FOR VULNERABILITY DISCLOSURE

The development of CVD processes stretches back to the 1990s, iterating through periods of tension and begrudging consensus.[28] Roles have evolved, and even some of today's champions of coordinated disclosure and public bounty programs were at best reticent about—and at worst overtly hostile toward—external vulnerability disclosure in the not-too-recent past.[29] In its "Guide to Coordinated Vulnerability Disclosure," the CERT CC, affiliated with Carnegie Mellon's Software Engineering Institute, describes CVD as the information management process of moving from initial discovery of a vulnerability to the deployment of remediation measures—patches, most commonly. A good CVD policy strives to establish rules that guide stakeholders through that process along an optimal route—somewhere between "disclose everything you know about a vulnerability to everyone as soon as you know it" and "never disclose anything you know about a vulnerability to anyone."[30] Differences in organizational preference, bug severity and publicity, patching timelines, maintenance resources, and much more cause great variation in the execution of CVD. Nonetheless, CERT CC's guide lays out several key principles along the path to patching: reducing harm, presuming researcher benevolence, avoiding surprise, incentivizing desired behavior, making ethical considerations, improving process, and considering CVD as "a wicked problem."[31]

In practice, there are many implementations of these and other guiding principles. For example, when Google researchers discover an external bug, they disclose it to vendors and provide a ninety-day period before going public with the vulnerability in the absence of a patch, with some wiggle room for slightly delayed patches and adoption, as well as a much more aggressive seven-day deadline for zero-day vulnerabilities under active exploitation.[32] Bug-bounty reporting platforms like HackerOne and BugCrowd run a variety of programs as aggregation and coordination platforms, each with their own guidelines—HackerOne's platform maintains a 180-day final deadline for disclosure in its public programs, for instance,[33] and both run a variety of private programs subject to CVD processes customized by participating organizations.[34]

Governments also maintain CVD policies for responsibly disclosing bugs found in their systems. For the US government, the US Cybersecurity and Infrastructure Agency (CISA) published the Binding Operational Directive (BOD) 20-01 on September 2, 2020, which required all federal agencies to implement their own vulnerability disclosure programs (VDPs) by March 2022.[35], [36] In April 2022, the European Union Agency for Cybersecurity (ENISA) published a report on CVD policies in the European Union (EU), providing useful overview of processes in its twenty-seven member-state.[37] Only four member-states—the Netherlands, France, Belgium, and Lithuania—had adopted a national CVD policy at the time of publication. Nine EU members had not begun

[28] Haroon Meer and Thu T. Pham, "History of Vulnerability Disclosure," Duo Security, August 3, 2015, https://duo.com/labs/research/history-of-vulnerability-disclosure.

[29] Ars Technica Staff, "When Google Squares off with Microsoft on Bug Disclosure, Only Users Lose," *Ars Technica*, January 12, 2015, https://arstechnica.com/information-technology/2015/01/google-sees-a-bug-before-patch-tuesday-but-windows-users-remain-vulnerable/.

[30] Householder et al., "The CERT Guide to Coordinated Vulnerability Disclosure," 6.

[31] Householder et al., "The CERT Guide to Coordinated Vulnerability Disclosure," 8.

[32] "How Google Handles Security Vulnerabilities," Google, accessed August 2, 2022, https://about.google/appsecurity/.

[33] "Vulnerability Disclosure Guidelines," HackerOne, accessed August 2, 2022, https://www.hackerone.com/disclosure-guidelines.

[34] To the reader, for example, BugCrowd's program list can be found at https://BugCrowd.com/programs, and hackerone's at https://hackerone.com/directory/programs.

[35] To the reader, in addition to outlining timelines and reporting requirements, VDPs often also define what types of research are permitted—for example, some VDPs prohibit testing denial-of-service attacks that would disrupt networks and data. They may also be referred to as Responsible Disclosure Programs, or RDPs.

[36] Cybersecurity and Infrastructure Security Agency (CISA), "Binding Operational Directive 20-01 – Develop and Publish a Vulnerability Disclosure Policy," BOD 20-01, (2020), https://www.cisa.gov/binding-operational-directive-20-01.

[37] Debora di Giacomo et al., *Coordinated Vulnerability Disclosure Policies in the EU*, ed. Evangelos Kantas and Marnix Dekker (Athens, Greece: ENISA, 2022), https://www.enisa.europa.eu/publications/coordinated-vulnerability-disclosure-policies-in-the-eu.

the process of implementing a national CVD policy at all, and the rest were at some stage of development.[38] The United Nations maintains a working group that has written on considerations for encouraging responsible disclosure.[39] Meanwhile, the International Organization for Standardization (ISO) with the International Electrotechnical Commission (IEC) outline responsible vendor practices for handling external vulnerability disclosure in the ISO/IEC:29147:2018 standard.[40]

Because governments also control the legal environments that might delineate between security research and prosecutable crime, clear national CVD policies foster a healthy research community, while their absence often disincentivizes or even punishes researchers. For example, reporting by Just Security on the Log4j incident and the RMSV describes the investigation of a German security researcher who found vulnerabilities in a polling application for a political campaign. The authors—Fabiola Schwarz, Jantje Silomon, and Misha Hansel—emphasize that a lack of clear guidance and protections imposes legal concerns on researchers, impeding their ability to contribute research findings.[41] Somewhat similarly, in the United States, Missouri threatened legal action against a reporter who found that thousands of social security numbers were publicly accessible on the internet through Missouri's Department of Education website.[42] Fortunately, governments have begun closing these loopholes to some degree. In addition to the CISA BOD 20-01, the US Department of Justice recently announced that it will choose not to charge security researchers acting in what it defines as good faith under the Computer Fraud and Abuse Act,[43] which has long been criticized for practical overreach with regards to benevolent research.[44]

Importantly, where security vulnerabilities are concerned, governments do more than create legal environments and act on researcher findings to patch their systems—many have offensive organizations with an interest in obtaining some of these vulnerabilities for eventual use, adding a third dimension to their CVD interactions. In the United States, the Vulnerability Equities Process (VEP) governs the management of vulnerabilities found by government agencies, reviewing the most severe on a case-by-case basis to decide whether to retain them for offensive use or disclose them to the vendor or maintainer.[45] Other countries have made some portion of their equities processes public too, including the United Kingdom, Australia, and Canada.[46] While these policies are only tangential to most CVD processes, some US agencies are explicitly required to submit findings to the VEP even when working with open-source code,[47] and the handling of vulnerabilities that the US government learns of in information sharing fora is not well understood from public documentation.[48]

[38] To the reader, ENISA notes that there is a lack of standardization among member-state CVD policies stemming from differing legal and economic resources. The report also highlights the Network and Information Security Directive 2 (NIS2), which emphasizes the importance of each country creating its own computer emergency response team (CERT) and recommends the establishment of national vulnerability databases.

[39] Mar Negreiro, "The NIS2 Directive: A High Common Level of Cybersecurity in the EU," *European Parliamentary Research Service* PE 689.333 (June 2022), 13, https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/689333/EPRS_BRI(2021)689333_EN.pdf.

[40] 14:00-17:00, "ISO/IEC 29147:2018," ISO, accessed June 30, 2022, https://www.iso.org/cms/render/live/en/sites/isoorg/contents/data/standard/07/23/72311.html. To the reader, this standard is currently behind a paywall, though arguments from security researchers Katie Moussouris and Art Manion swayed the ISO to make it freely available for a time. For more on this, read the following: Juha Saarinen, "ISO Vulnerability Disclosure Standard Now Free," *iTnews*, April 18, 2016, https://www.itnews.com.au/news/iso-vulnerability-disclosure-standard-now-free-418253, and Katie Moussouris, "Vulnerability Disclosure Deja Vu: Prosecute Crime Not Research," *Dark Reading*, May 12, 2015, https://www.darkreading.com/vulnerabilities-threats/vulnerability-disclosure-deja-vu-prosecute-crime-not-research.

[41] Fabiola Schwarz, Jantje Silomon, and Micha Hansel, "Empowering Security Researchers Will Improve Global Cybersecurity," Just Security, May 6, 2022, https://www.justsecurity.org/81293/empowering-security-researchers-will-improve-global-cybersecurity/.

[42] Lucas Ropek, "Missouri Governor Accuses Journalist of Hacking for Warning That State Left Teachers' Data Exposed," Gizmodo, October 14, 2021, https://gizmodo.com/missouri-governor-wants-to-prosecute-journalist-for-war-1847866414.

[43] US Department of Justice, *Justice Manual, Title 9: Criminal 9-48.000 – Computer Fraud and Abuse Act*, [updated May 19, 2022], accessed August 2, 2022, https://www.justice.gov/opa/press-release/file/1507126/download.

[44] Adi Robertson, "Justice Department Pledges Not to Charge Security Researchers with Hacking Crimes," *The Verge*, May 19, 2022, https://www.theverge.com/2022/5/19/23130910/justice-department-cfaa-hacking-law-guideline-limits-security-research.

[45] "Vulnerabilities Equities Policy and Process for the United States Government," November 15, 2017, https://trumpwhitehouse.archives.gov/sites/whitehouse.gov/files/images/External%20-%20Unclassified%20VEP%20Charter%20FINAL.PDF.

[46] Schwarz, Silomon, and Hansel, "Empowering Security Researchers Will Improve Global Cybersecurity."

[47] John Sherman, "Memorandum for Senior Pentagon Leadership, Commandant of the Coast Guard, Commanders of the Combatant Commands, Defense Agency and DoD Field Activity Directors | Subject: Software Development and Open Source Software," January 24, 2022, https://dodcio.defense.gov/portals/0/documents/library/softwaredev-opensource.pdf.

[48] To the reader, these regulations are notably different from incident-reporting requirements, which have become more common. Incident-reporting requirements, such as nascent legislation covering critical infrastructure incidents in the United States, or India's recent, more expansive regulations are premised on the fact that attackers have already made forays against (usually) non-government entities, by abusing either known vulnerabilities, unknown ones, or both. Because they are already able to compromise a target, which does not necessarily even know the exploits involved, there is less, if any, risk that reporting will reveal information about a vulnerability that others will exploit, especially when governments responsibly control what portion of the report is made public.

The RMSV

In July 2021, the Cyberspace Administration of China (CAC) published a draft version of the RMSV. The following articles of the RMSV—in effect since September 2021—are the focus of this work:

- "**Article 4**: No organization or individual may…illegally collect, sell, or publish information on network product security loopholes…"

- "**Article 7**: Network product providers shall perform the following…:

  i. After discovering or learning that there are security vulnerabilities in the provided network products…it shall immediately notify the relevant product provider…

  ii. The relevant vulnerability information shall be submitted to the Network Security Threat and Vulnerability Information Sharing Platforms of the Ministry of Industry and Information Technology within 2 days…"

- "**Article 9**: Organizations or individuals engaged in the discovery and collection of network product security vulnerabilities shall release information on network product security vulnerabilities to the public through network platforms, media, conferences, competitions, etc. principles and abide by the following provisions:

  iii. Vulnerability information shall not be released before network product providers provide network product security vulnerability repair measures…

  iv. Not to publish the details of the security loopholes in the networks, information systems and equipment used by network operators…

  v. …

  vi. Not to publish or provide programs and tools specially used to exploit the security loopholes…in activities that endanger network security."

The RMSV creates a few specific concerns including the potential for the law to create a chilling effect on the disclosure of vulnerabilities from China's research community and thereby impact the supply of vulnerability disclosures more widely. Because of the difficulty of disclosing the required information within the given two-day timeline, the ambiguity of what is considered a "network product provider," and the fuzzy borders between provider, individual, and individuals funded by a provider, researchers might hesitate to disclose a vulnerability to the vendor entirely, turning them over to the government only, if at all, or waiting for further legal clarity before continuing their work. The ambiguity about which entities the RMSV covers and the scope of the mandated notice to government also holds the prospect of legal penalties over individual researchers.

The RMSV is of particular interest in the context of studying the impact of CVD regulation for several reasons. First, it is unambiguous in requiring that some subsets of vulnerabilities be reported from private enterprise to the Chinese government prior to patching, even if there are ambiguities in what entities and which vulnerabilities it regulates. If anything, wider quantitative analysis might reveal the Chinese government's current views of those gaps. Second, the RMSV provides a well-delineated timeline to examine—a 'before' and 'after' for when its reporting requirements were either publicly known or enforceable. Third, the portion of the global security research that it regulates is enormous—Chinese researchers, until recently, were prolific contributors at international hacking competitions,[49] and the nation's information and communications technology (ICT) sector is one of the largest globally.[50], [51], [52] Any chilling effect would therefore be more likely to emerge in publicly available data, and its impact on global security would be nontrivial, particularly given the fact that the only known, documented instance of potential enforcement was Alibaba's handling Log4j.

Strategic Context

The RMSV is noteworthy in its strategic ambiguity. It is not made explicit how the law applies to multinational companies with offices in China, what kind of entity is considered a network product provider, or what degree of affiliation an individual can maintain with a network product provider without being subject to the law. In addition, it is unclear what level of severity a vulnerability must have to require reporting (and the law provides for no rating or review process), what level of early disclosure to affected entities outside of a product maintainer it allows,

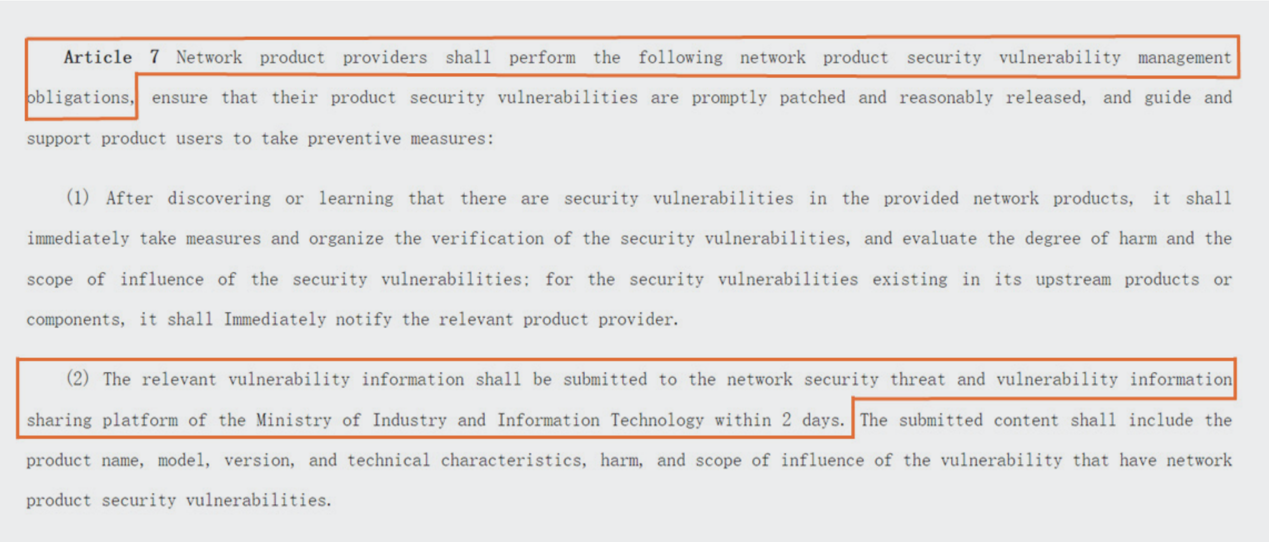
[49] Bing, "China's Government Is Keeping Its Security Researchers from Attending Conferences."

[50] Justina Alexandra Sava, "Global ICT Market Share 2013 - 2022, By Selected Country," Statista, March 3, 2022, https://www.statista.com/statistics/263801/global-market-share-held-by-selected-countries-in-the-ict-market/.

[51] "IT Industry Outlook 2022," CompTIA, accessed August 2, 2022, http://connect.comptia.org/content/research/it-industry-trends-analysis.

[52] To the reader, a similar study of the impact of better legal protections for researchers in the EU, for example, might struggle with its sample size given the patchwork of legal environments across the EU's many member-states, whereas the Chinese model is conveniently (for the purposes of this study) monolithic.

Highlighted RMSV



Article 7 Network product providers shall perform the following network product security vulnerability management obligations, ensure that their product security vulnerabilities are promptly patched and reasonably released, and guide and support product users to take preventive measures:

(1) After discovering or learning that there are security vulnerabilities in the provided network products, it shall immediately take measures and organize the verification of the security vulnerabilities, and evaluate the degree of harm and the scope of influence of the security vulnerabilities; for the security vulnerabilities existing in its upstream products or components, it shall Immediately notify the relevant product provider.

(2) The relevant vulnerability information shall be submitted to the network security threat and vulnerability information sharing platform of the Ministry of Industry and Information Technology within 2 days. The submitted content shall include the product name, model, version, and technical characteristics, harm, and scope of influence of the vulnerability that have network product security vulnerabilities.

if any, what its designs for multi-party products are, or how it intends to regulate vulnerabilities in critical open-source software. Some bugs might be reported to vendors by researchers who do not even realize the presence of significant security impacts. In some ways, all this vagueness might be the point, allowing enforcement at the convenience of the government and creating a Damocles sword of legal liability for researching entities. Even the MIIT's ability to cope with the significant volume of vulnerability research the RMSV seems to demand is doubtful.

Strategic ambiguity is a recurring trend in Chinese cybersecurity policy and law. In China, cybersecurity is part of broader information security—the goal is full control of the information space within China to ensure social stability and regime continuity—including against myriad threats from and through digital technology.[53] As a unitary government, and with recent reforms to recentralize the government following devolution to the local level during earlier phases of reform and opening up,[54] China exercises a top-down imposition of government policy. Information security has seen a greater national-level consolidation in oversight because of its strategic nature. Moreover, many of China's key enforcement mechanisms relevant to information security are the direct responsibility of state entities such as the MIIT, Ministry of State Security (MSS), and the CAC.

As China innovates in digital technologies, it has sought to preempt regulatory challenges through a top-down approach common across sectors (China conducts nearly all its development planning at the national level as well). Many of the country's major technology firms—Ant Group, Baidu, Tencent, etc.—are private companies that nevertheless must function inside this policy environment. Recent fines for monopolistic behavior and blocks against international initial public offerings (IPOs) demonstrate the government's tightening grip on its IT industry scions,[55], [56] alongside a drive towards stricter regulations and localization of data centers.[57]

The RMSV emerges from an approach to information management that focuses on applying regulation with purposeful ambiguity at the source of what is considered a resource, all to create wider and more flexible effects on firms and maybe even individuals. It is precisely this framework that threatens to undermine the supply of vulnerability disclosures abroad.

[53] Dean Cheng, *Cyber Dragon: Inside China's Information Warfare and Cyber Operations* (Santa Barbara, California: Praeger, 2017).

[54] Cheng, *Cyber Dragon*.

[55] Zhong, "China Fines Alibaba $2.8 Billion in Landmark Antitrust Case."

[56] "China Blocks Didi From App Stores Days After Mega U.S. IPO," *Bloomberg News*, July 4, 2021, https://www.bloomberg.com/news/articles/2021-07-04/china-regulator-orders-didi-to-be-removed-from-app-stores.

[57] Yan Luo, Zhijing Yu, and Vicky Liu, "The Future of Data Localization and Cross-Border Transfer in China: A Unified Framework or a Patchwork of Requirements?," International Association of Privacy Professionals (IAPP), June 22, 2021, https://iapp.org/news/a/the-future-of-data-localization-and-cross-border-transfer-in-china-a-unified-framework-or-a-patchwork-of-requirements/.

EFFECTS OF THE RMSV

With these considerations in mind, this paper looks at a large dataset of publicly reported vulnerability acknowledgments to detect a significant change in contributions from Chinese researchers—from individuals to large companies—over the lifetime of the RMSV at three key points:

- Public release of Data Security Law draft: July 2020.[58], [59]
- Publication: July 2021.
- Enactment: September 2021.

Specifically, this paper proposes that any of those three dates may see either a significant decline in the proportion of vulnerabilities attributed to Chinese researchers or firms or a significant decline in the total reporting of vulnerabilities in the case that most reports were initially unattributed or anonymously made.

Methodology

To look for these effects, the team gathered a variety of publicly available vulnerability data from both proprietary vendors and open-source product managers. These entities included Microsoft, Apple, VMware, F5, and Red Hat, which provides data about a wide variety of open-source packages it is involved with. Specific data organization and entries varied among these entities. Microsoft provides the ability to download a spreadsheet of CVEs reported to the company, which includes external acknowledgments, dates, and affected products.[60] Apple maintains records of its security updates, which include information on CVEs and external reporters scraped from its website, as with VMware and F5.[61], [62], [63] Red Hat maintains several datasets relevant to the task, including the Extensive Markup Language (XML) files of CVEs reported to its open-source projects, CVE acknowledgments, dates, and affected projects.[64] The team selected data sources for their ability to represent significant subsections of the technology ecosystem—multi-platform providers (Microsoft), significant infrastructure providers (VMware and F5), companies with massive consumer-facing product lines (Apple), and well-established open-source software (OSS) stakeholders (Red Hat). Other entities considered for study but not included due to processing challenges are Google (specifically its Chrome stable releases) and the Open Source Vulnerability (OSV) schema.[65]

The publication date of security advisories is not necessarily the same as the corresponding vulnerability's disclosure, and the lag time between these two dates might vary within and among vendors based on a host of factors. These advisories are a useful source of time-stamped data and possibly make visible the effects of policy interventions. Random distribution or no consistent patterns of change are thus useful findings as well. In addition, the decision to publicly credit a researcher (as opposed to labeling them "anonymous" or crediting no entity or individual at all) despite the law also would also

[58] Catalin Cimpanu, "Chinese Government Lays out New Vulnerability Disclosure Rules," *The Record by Recorded Future* (blog), July 14, 2021, https://therecord.media/chinese-government-lays-out-new-vulnerability-disclosure-rules/. To the reader, the precise timeline, however, of the specific vulnerability reporting requirements is difficult to track through the flurry of recent cybersecurity regulations in China. This best estimate derives from Bill Goodwin's reporting at *ComputerWeekly* and Catalin Cimpanu's at *The Record*, indicating that the first draft of the law that included the reporting mandate was published by the Standing Committee of the National People's Congress of China on July 2, 2020, alongside the draft Data Security Law. See also: Bill Goodwin, "Chinese Law May Require Companies to Disclose Cyber-Security Preparations Outside China," *Computer Weekly*, July 3, 2020, https://www.computerweekly.com/news/252485674/Chinese-law-may-require-companies-to-disclose-cyber-security-preparations-outside-China. The key quote citing Goodwin's reporting is: "The provision that product vendors might need to share vulnerability details with Chinese state agencies has been known and in the public domain since at least 2020."

[59] To the reader, this date also collides with significant US sanctions activity and other cyber legislation initiatives in China, making it both the most likely to show an effect and the least conclusive in the case that it does.

[60] Microsoft Security Response Center (MSRC), "Security Update Guide – Vulnerabilities," Microsoft, [updated August 9, 2022], https://msrc.microsoft.com/update-guide/vulnerability.

[61] "Apple Security Updates," Apple Support, https://support.apple.com/en-us/HT201222.

[62] "VMware Security Advisories," VMware, Inc., https://www.vmware.com/security/advisories.html.

[63] AskF5, "Security Knowledge Centers," F5, https://support.f5.com/csp/knowledge-center/security.

[64] Red Hat Customer Portal, "Security Data," Red Hat, https://access.redhat.com/security/data.

[65] "A Distributed Vulnerability Database for Open Source," OSV, https://osv.dev/.

reveal something about the respective organization's thinking.[66]

These datasets were compiled (separately) into a log of CVEs, originating webpages, acknowledged entities (differentiated into individuals and organizations where possible), best-estimated publication date, and affected products.[67] From there, the team associated credited companies with a best-estimate country of legal provenance, while identifying credits to open-source projects and multinational organizations as such. Some organizations operated only in two countries and were split to reflect such. While the paper does not identify the legal environments where individuals operated, some geolocation information volunteered either through Twitter, GitHub, or email addresses is available and has been used in other studies.[68] This provided the necessary material for analyzing, roughly, by country contribution over time. Each entry received a month-year tag for batching, especially convenient as two of the three significant dates were on the first and second days of a month (July 2, 2020, and September 1, 2021—the draft RMSV released on July 13, 2021). Each step presented various opportunities for cleaning the datasets, and this paper describes the steps taken for further analysis.

The data collected by this methodology was unavoidably noisy.[69] Many entries were created by hand at the source, leading to an enormous quantity of typos and spelling variations (e.g., Qihoo 360, QIHU360, Qihoo360, or just 360 represent the same company), and different formats and encoding protocols mangled accents and non-English characters. There is also considerable overlap between datasets, where vulnerabilities in a common codebase affected multiple products or where CVEs were retroactively revealed to discuss the same vulnerability. There is no standard process for acknowledgment either—some uncredited CVEs may have been reported anonymously or discovered by researchers internal to the company providing the data. Meanwhile, F5 didn't always list CVEs, relying on its own numbering system throughout.

Dating entries is similarly imprecise, reflecting many possible significant dates: original confidential report to a company, discovery of a known CVE's impact on a product not previously known to be affected, public publishing, addition to another dataset like the US National Vulnerability Database (NVD), and so on. Not all Red Hat's CVEs were updated with accurate reporting dates on one of their datasets, so this analysis used their searchable database to fill in dates for approximately one-third of the entries, supplementing with publication dates from MITRE and Tenable as needed.[70] In addition, not all companies batched their data in the same manner. Microsoft seemed to organize reports by CVE mainly, while Apple and F5 focused on reporting CVEs within relevant software updates, leading to double reporting and time-shifts. These discrepancies alongside other unknown differences in internal policy and the variances in sample size prevent comparisons between datasets. Overall, while this data is by no means fully representative of the security research ecosystem, it does present best estimates of small slices of that community and its contributions to various product and project environments.

[66] To the reader, this is not to say that the law prohibits crediting, but rather that, if a researching entity fails to comply with the law, public acknowledgment of their disclosure provides an easy source of enforcement information to the MIIT.

[67] To the reader, scripts used for scraping and processing for acknowledgments are found through https://www.atlanticcouncil.org/in-depth-research-reports/report/preserving-international-cybersecurity-research/. Data cleaning not reflected in these scripts occurred in Excel.

[68] Johannes Wachs et al., "The Geography of Open Source Software: Evidence from GitHub," *Technological Forecasting and Social Change* 176, no. 121478 (March 2022), https://doi.org/10.1016/j.techfore.2022.121478.

[69] To the reader, more discussion of data challenges can be found in the Appendix.

[70] "CVEs," Tenable, accessed August 2, 2022, https://www.tenable.com/cve.

On the Data

The datasets utilized for this study had samples sizes of 14,740 (Apple), 4,355 (Microsoft), 3,307 (Red Hat), 1,363 (VMware), and 335 (F5). In addition to providing data on potential impacts of the RMSV, this data helps illustrates trends in vulnerability disclosure across a portion of the technology ecosystem. Overall, country attribution acknowledgment ratios give a useful sketch of the largest, most active research communities as well as the differences among them.

The following charts detail the total number of records for each dataset and the number and percentage of those where an acknowledgment links back to organizations operating out of the United States, China, an EU member state, or other countries. Each also details the number and percent of entries with acknowledgments not linked to country-tagged organizations (where organizations were not able to be tagged to a specific country). Because acknowledgments can credit multiple organizations and thus tag multiple countries, the rows do not add up to 100 percent of entries.

Tables 1 – 5: Dataset contribution counts and ratios by country, aggregated for each company

F5	#	%
Total	334	
US	227	68%
China	0	0%
EU	33	10%
Other Countries	33	10%
No Country	43	13%

Microsoft	#	%
Total	4,354	
US	1,813	42%
China	1,081	25%
EU	313	7%
Other Countries	319	7%
No Country	1,136	26%

Red Hat	#	%
Total	3,306	
US	1,061	32%
China	274	8%
EU	213	6%
Other Countries	889	27%
No Country	904	27%

VMware	#	%
Total	1,363	
US	184	13%
China	52	4%
EU	50	4%
Other Countries	160	12%
No Country	940	69%

Apple	#	%
Total	14,739	
US	6,821	46%
China	1,903	13%
EU	695	5%
Other Countries	763	5%
No Country	5,010	34%

These charts help highlight differences in vulnerability disclosure patterns across the datasets included here, but they also underline the variability in disclosure record-keeping practices. For example, all Red Hat and Microsoft entries contained some form of acknowledgment, and most entries in the Apple and F5 datasets did too, yet most VMware entries did not. Similarly, rates of Chinese contribution varied between datasets, from no identifiable contributing organizations in the F5 data to a quarter of entries in the Microsoft dataset crediting an organization based in China, among others. Somewhat surprisingly, the portion of acknowledgments crediting only individual researchers (rather than organizations either affiliated with the researcher or contributing independently) was consistent among the three largest datasets at around one quarter of entries, while much lower for F5 and VMware entries.

Benchmarking these aggregate measurements against other datasets is useful. An anonymous bug-bounty platform provided Dakota Cary in his February 2022 Congressional testimony with data on the portion of bounty payments paid to researchers in different countries by US firms in 2021 through the platform.[71] This paper reproduces that data below in a similar format as the above data.

Notably, these data show less of a gap between the United States and China or the European Union, and greater representation of the European Union overall. Part of this gap originates from the narrower timeframe of the bug-bounty platform data. The datasets gathered by this paper from vendors show, consistently, US dominance of contributions in earlier years, followed by increasing representation of other countries—particularly China—as their IT sectors develop and the disclosure pipelines become more accessible to non-US researchers. Filtering this paper's datasets for just 2021 reflects that shift, bringing parity to the United States and China points similar to that in the bug-bounty platform numbers, though the EU still lags. This might reflect selection bias in the countries with which the bug-bounty platform has developed strong relationships. Figure 1 shows the contributions tagged to the United States and China over time in the Apple dataset, illustrating the changes in composition over time.

Table 6: Anonymized bug bounty funding data for 2021

Country	Funds Paid	Percent of Total Payments
United States	$6,718,923	15%
EU	$6,601,114	15%
China	$4,220,302	10%

[71] Cary, *China's Cyber Capabilities: Warfare, Espionage, and Implications*.

Findings on the RMSV

The majority of the analysis in this paper looks for an impact timed with one of the three key dates identified regarding the RMSV. First, it examines both the raw counts and proportional contributions by country, focusing on China while using the US as a baseline. It discusses these results below. F5 contained no acknowledgments tagged to Chinese companies, thus producing no finding. Data from Apple and VMware showed no significant impact correlated with the RMSV, though the paper includes basic charts of their raw contribution datasets in the appendices. Data from Red Hat and Microsoft produced more notable results and are considered and analyzed in greater detail below.

MICROSOFT

Between June and July of 2020, CVE contributions credited to Chinese organizations plummeted from 59 to 11, where they hover each month since (see figure 2). Even more surprisingly, this decline occurred as overall contributions increased and broke a trend of a steadily increasing proportion of Chinese contributions (see figure 3).

Figure 1: Contribution counts by country per month, Apple

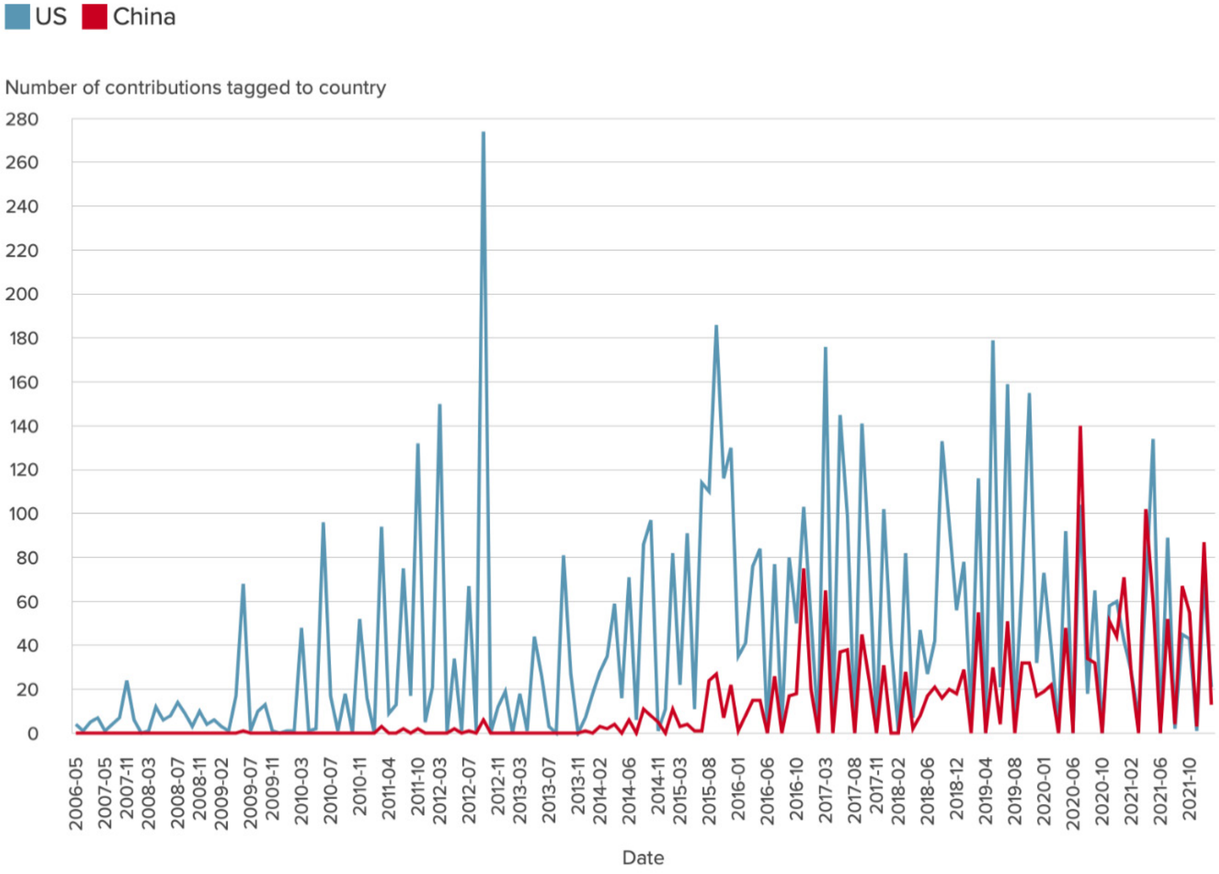


Figure 2: Contribution counts by country per month, Microsoft

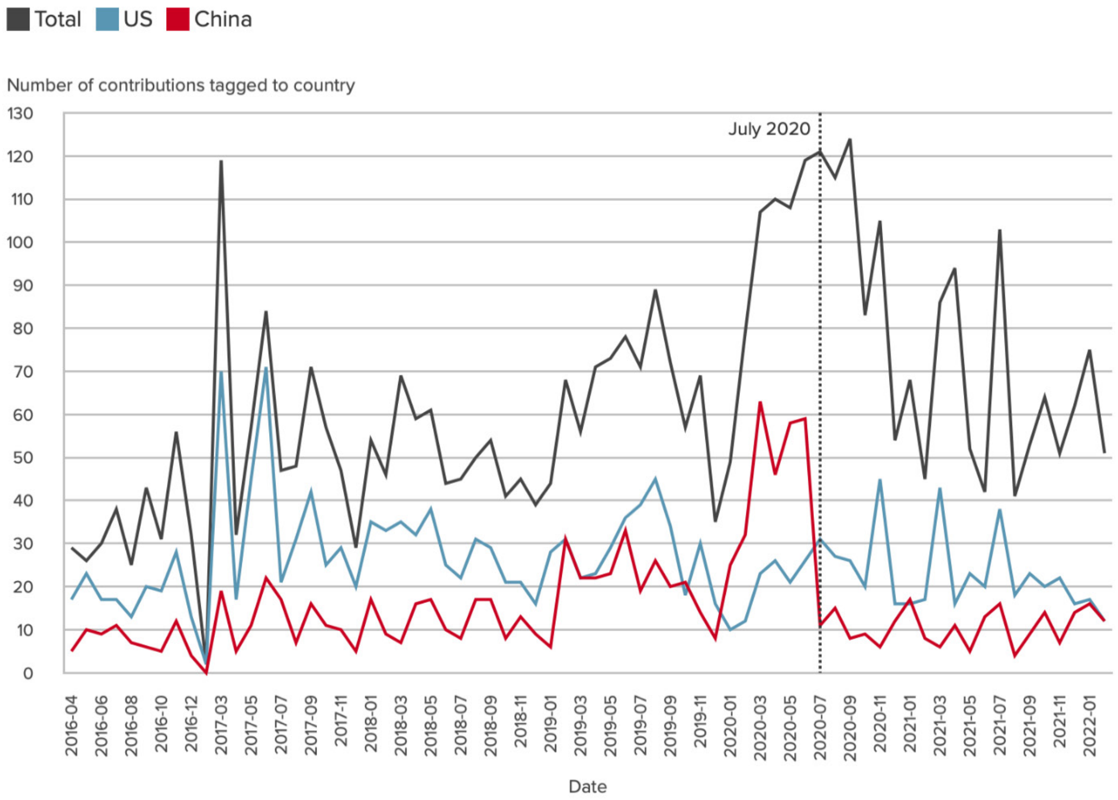
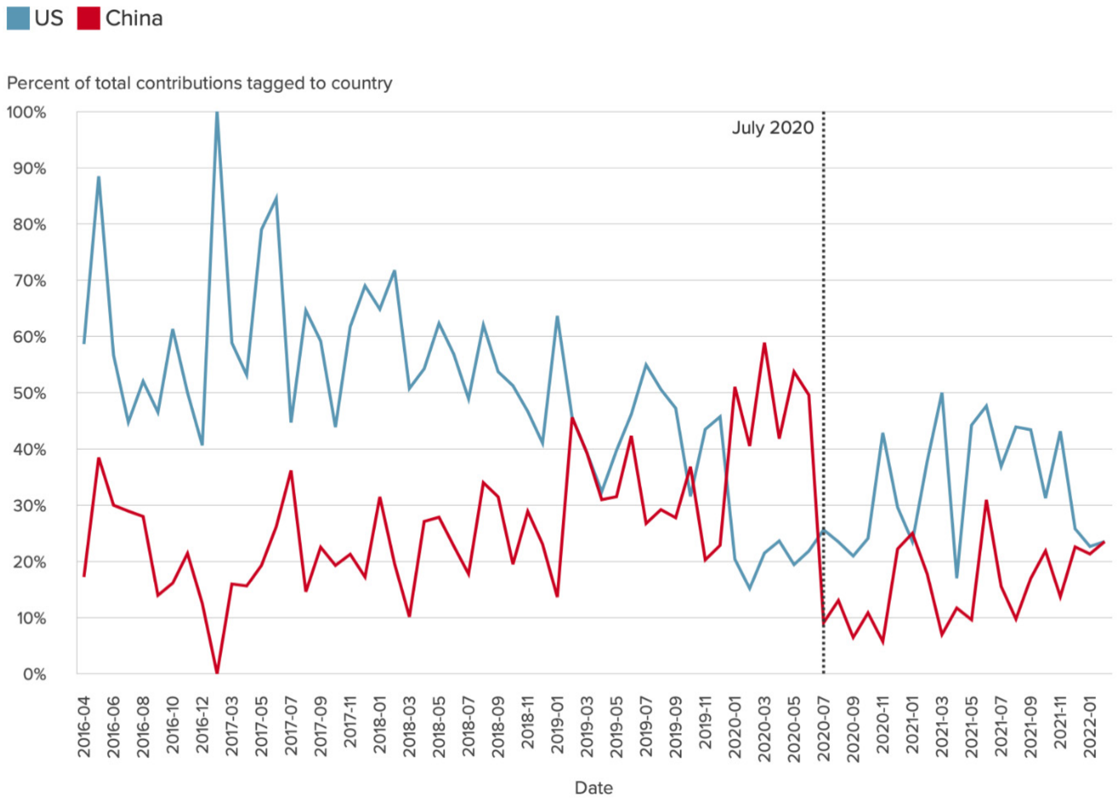


Figure 3: Contribution portions by country per month, Microsoft



To better analyze this result, this paper uses Google's CausalImpact analysis package for R.[72] To do so, it considers the July 2020 data as an intervention treatment for China-tagged contributions, predicting a post-treatment trendline based on pre-treatment China-tagged contributions and using non-China contributions as a covariate to help predict China-tagged contributions based on data-points unaffected by the RMSV. This modelling has the advantage of capturing, with considerable nuance, the relationship between China-tagged contributions and overall contributions each month—few overall contributions predicts a low number of China-tagged contributions, while a large number of contributions makes a large number of China-tagged contributions more likely. Last, this post-treatment forecast is measured against the actual post-treatment data and tested for statistical significance. The results of this analysis are shown in table, graph, and text form—provided by the CausalImpact package itself—below.

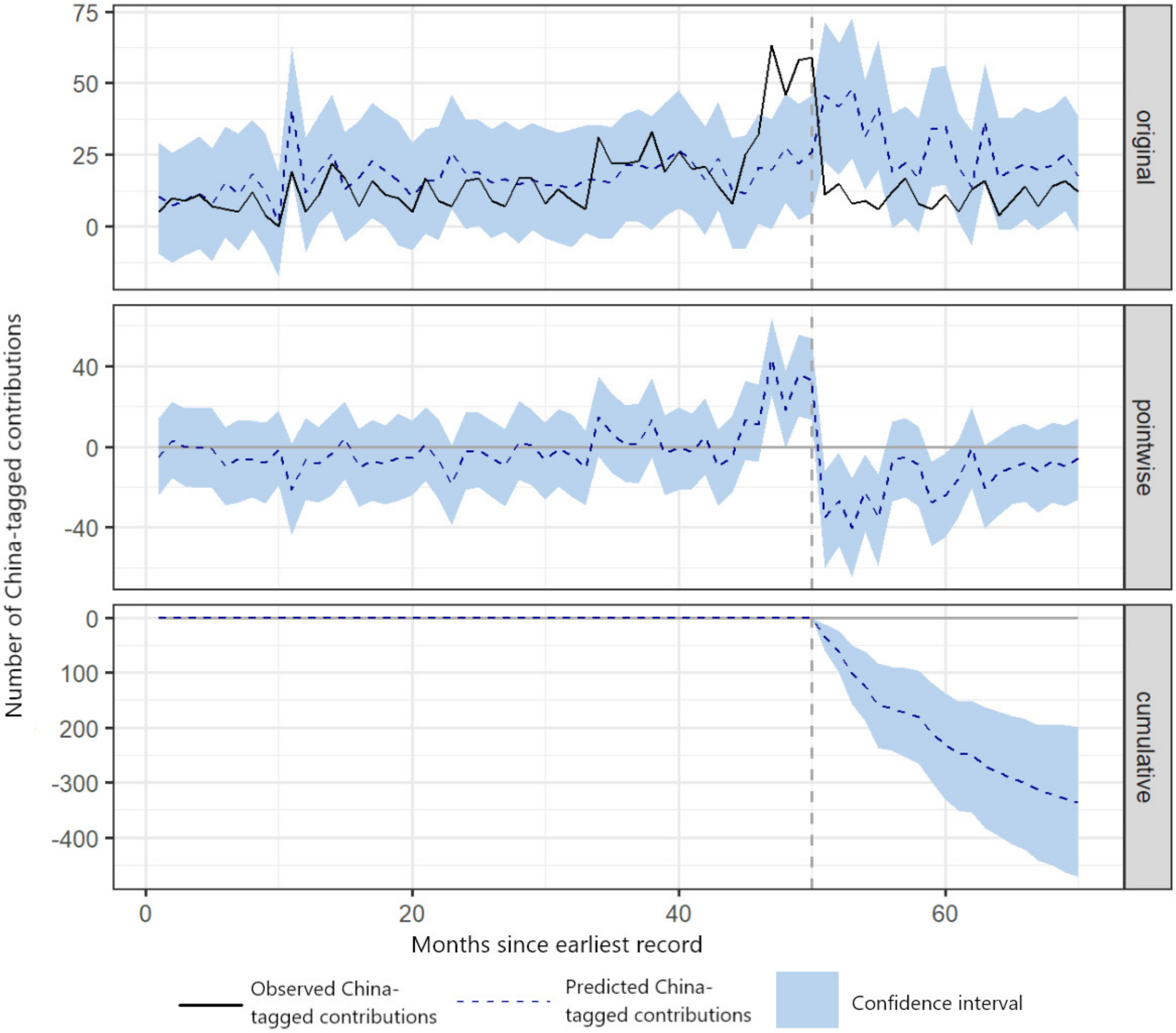
As a downside, the use of only one predictor variable is not optimal—the CausalImpact developers recommend somewhere between five and twenty where possible. Others to be considered include total CVEs made public each month and IT-sector size per month among other predictors of general vulnerability disclosure, though their addition is beyond the scope of this paper, which serves mainly as a proof-of-concept analysis. As such, while this is not rigorous statistical evidence of a significant impact from the RMSV, it is moderately convincing and provides clear direction for future analysis.

Table 7: Significance Check

Posterior inference (CausalImpact)	Average	Cumulative
Actual	11	213
Prediction (sd)	27 (3.5)	549 (69.4)
95 percent CI	[21, 34]	[418, 686]
Absolute effect (sd)	-17 (3.5)	-336 (69.4)
95 percent CI	[-24, -10]	[-473, -205]
Relative effect (sd)	-61% (13%)	-61% (13%)
95 percent CI	[-86%, -37%]	[86%, -37%]
Posterior tail-area probability p:	0.00102	
Posterior probability of a causal effect:	99.89827%	

[72] "An R Package for Causal Inference Using Bayesian Structural Time-Series Models," CausalImpact, https://cran.r-project.org/web/packages/CausalImpact/vignettes/CausalImpact.html.

Figure 4: Original and projected China-tagged contributions, pointwise difference, and cumulative difference, Microsoft



The x-axis of the above graphs shows the number of time-steps from the earliest data entry, while the y-axis shows the number of contributions. The top graph shows as a black line the number of China-tagged contributions over time, on top of the predicted number of China-tagged contributions derived from covariate and pre-treatment modelling as a dotted blue line, with confidence intervals shaded in light-blue and the treatment date shown as a vertical dotted gray line. The second graph shows the difference between prediction and observed data, called pointwise causal effects, which the third panel sums up to show the cumulative deviation from the predictive model. The significant drop-off in China-tagged contributions, especially in the context of no corresponding drop-off in contributions from other countries, is statistically significant and described in technical detail below.

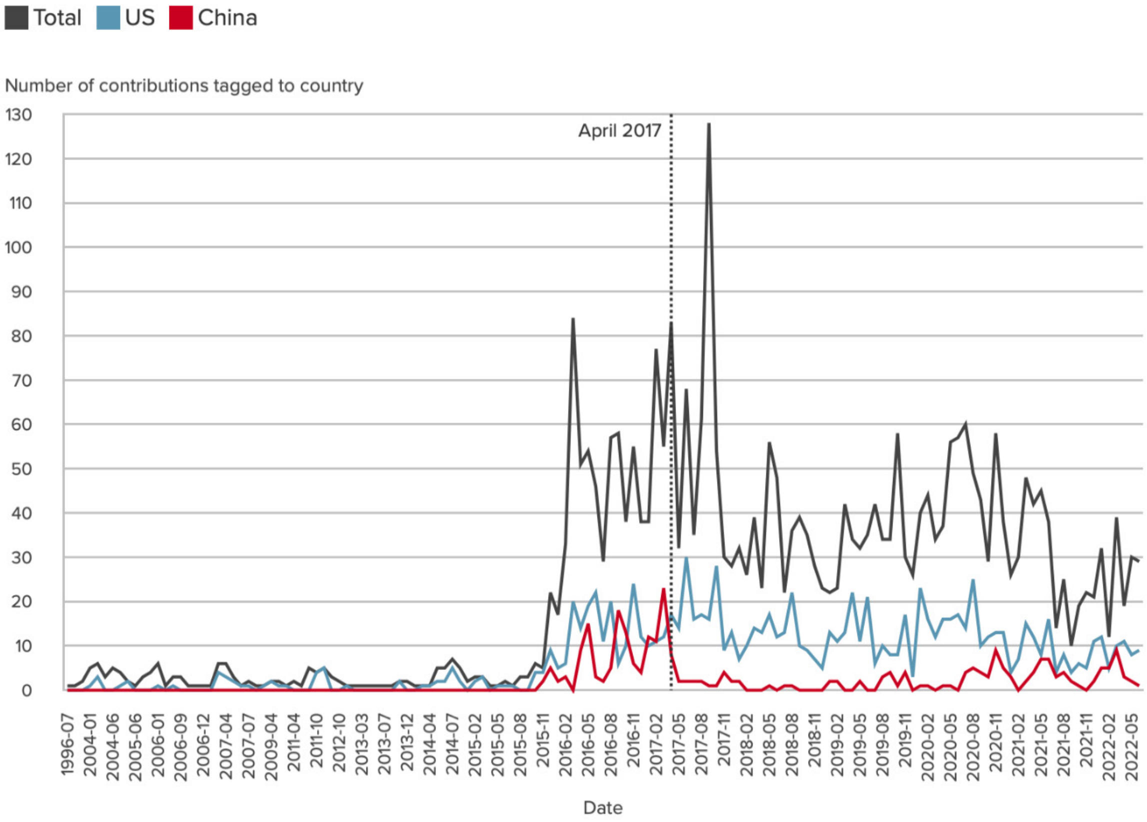
During the post-intervention period, the response variable had an average value of approximately 10.65. By contrast, in the absence of an intervention, we would have expected an average response of 27.45. The 95 percent interval of this counterfactual prediction is [20.89, 34.32]. Subtracting this prediction from the observed response yields an estimate of the causal effect the intervention had on the response variable. This effect is -16.80 with a 95 percent interval of [-23.67, -10.24]. For a discussion of the significance of this effect, see below. Summing up the individual data points during the post-intervention period (which can only sometimes be meaningfully interpreted), the response variable had an overall value of 213.00. By contrast, had the intervention not taken place, we would have expected a sum of 548.91. The 95 percent interval of this prediction is [417.75, 686.49]. The above results are given in terms of absolute numbers. In relative terms, the response variable showed a decrease of -61 percent. The 95 percent interval of this percentage is [-86 percent, -37 percent]. This means that the negative effect observed during the intervention period is statistically significant. The probability of obtaining this effect by chance is very small (Bayesian one-sided tail-area probability p = 0.001). This means the causal effect can be considered statistically significant.[73]

Interestingly, the drop in China-tagged contributions coincides with an increase of similar size and significance in contributions tagged either to individuals, companies with no known country tag, or no acknowledgement at all.[74] This might suggest that in response to the RMSV, researching entities and disclosure recipients opted to refrain from explicit, public acknowledgments rather than from disclosure all together.

RED HAT

While no significant change in contributions from Chinese entities occurred in the Red Hat data at any of the three key dates identified above, a significant decline in contributions did occur in April 2017 and has been largely sustained since, even amid a general increase in the overall number of contributions, though those declined from a high of 128 in September 2017 to a lower mean since (see figure 4). The proportional data reflects that initial drop while also showing an upward-trending resurgence of Chinese contributions beginning in August 2020 (see figure 5). As in the Microsoft, VMware, and Apple data, the trend of US predominance of contributions early on, followed by increased participation from China and other countries persists. If the April 2017 drop resulted from an external intervention, analysis similar to that performed on the Microsoft dataset and included in the appendix also indicates statistical significance, but no clear exogenous event is apparent, indicating that the movement reflects either internal policy changes, statistical noise, or a more complex interaction among contributors and stakeholders.

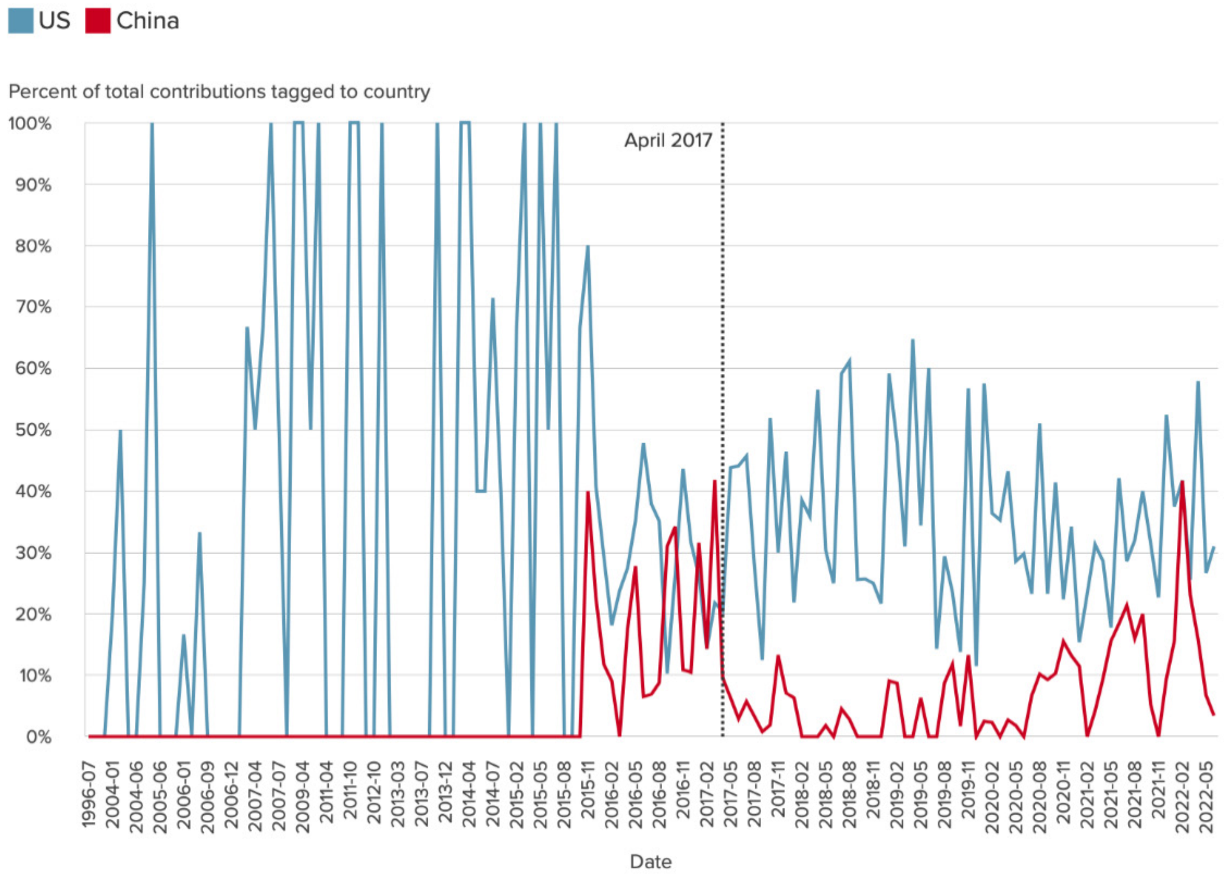
Figure 5: Contribution counts by country per month, Red Hat



[73] To the reader, text produced by the summary method of the CausalImpact package.

[74] To the reader, statistical analysis of this effect is in the appendix for brevity, though it is essentially a positive version of the negative RMSV-correlated impact on China-tagged contribution.

Figure 6: Contribution portions by country per month, Red Hat



Product Type Breakdown

This paper also looked at product-type breakdowns within each dataset, pulling out information for hypervisor products in VMware and Microsoft, internet browsers in Apple and Microsoft, and examining iOS and macOS updates in Apple. While no significant impact from any of the three RMSV dates arose in these subsets, further analysis of the datasets may reveal interesting areas of research focus. The analysis strove to compare Microsoft and Apple operating system trends, but a lack of clear labelling conventions frustrated attempts at identifying contributions to Microsoft operating systems. These non-findings may indicate that, while researchers necessarily specialize in specific product types and systems, the combination of large datasets and smaller numbers of true experts as well as the difficulties in pulling out information on vulnerability severity even with CVSS scores[75] drown out any discernable trends in specialization.

[75] Jacques Chester, “A Closer Look at CVSS Scores,” Theory of Predictable Software, June 19, 2022, https://theoryof.predictable.software/articles/a-closer-look-at-cvss-scores/.

By-Company Breakdown: Microsoft

To help clarify the specific cause of the July 2020 decline in China-based contributions in the Microsoft dataset, this paper analyzed the data's China-tagged companies more closely. In addition to the first public knowledge of the RMSV, the July 2020 date coincided roughly with several rounds of US sanction activity against Chinese companies as well as significant cyber legislation in China.[76] While determining precisely which regulations might have caused the decline is beyond the scope of the paper, it is possible to measure some impact of company-specific sanction activity with this paper's dataset.

Tracking the contributions of large, China-tagged companies over time was straightforward. This dataset already has disclosures tracked over time, linking them to companies and tagging those companies to the best-approximated country of operation. In practice, though, poor data quality complicates the process by providing multiple spellings of the same companies and inconsistently referencing subsidiary companies, subdivisions, and research labs. For each of these variations, we created—and then tracked over time—an alias tag, providing a common identity for typos, spelling variations, and subsidiaries. For example, QIHU360 (misspelling), 360 SkyEye Labs (subsidiary), and Vulcan Team (also called Qihoo 360 Vulcan Team) all received the same alias—Qihoo 360.

Sums of pre- and post-July 2020 contributions for each company (both by their original entry names and by their aliases) provide a preliminary analysis. Altogether, Chinese companies contributed 1,090 disclosures in the Microsoft dataset before July 2020, and 230 after. An impressive 691 of the pre-RMSV contributions from China-tagged companies came from Qihoo 360 affiliated groups, followed by 190 from Tencent, thirty from Baidu, and twenty-five from Alibaba (and several other companies contributed similarly or less prior to the RMSV—see the following table for more).

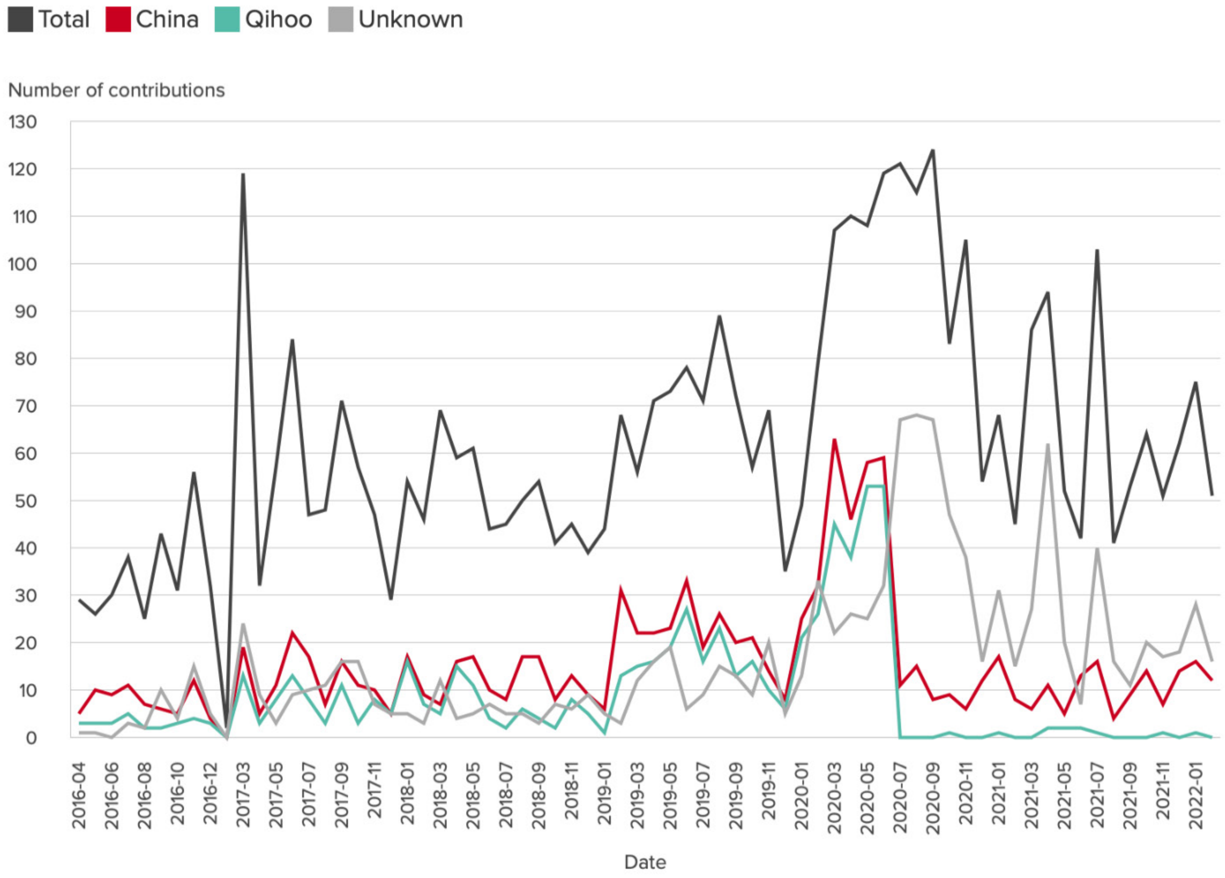
After July 2020, the data initially tells a different story. While some companies increased their disclosures—for example, DBAPP and Venustech more than doubled their contributions—the largest pre-RMSV contributors fell off precipitously with no other entities filling the gap to the same magnitude. Because Qihoo 360 contributed more than 60 percent of the total pre-RMSV, this paper tracks Qihoo's year-month contributions to confirm that it was the driving force behind the China-tagged contribution drop-off in July 2020 (see figure #).

Table 8 – By Company Microsoft Contributions

Microsoft Aliases	Pre-RMSV	Post-RMSV	Decrease
Qihoo 360	691	11	680
Tencent	190	11	179
Baidu	30	3	27
Alibaba	25	5	20

[76] US Department of Defense, "DOD Releases List of Additional Companies, in Accordance with Section 1237 of FY99 NDAA," news release, August 28, 2022, https://www.defense.gov/News/Releases/Release/Article/2328894/dod-releases-list-of-additional-companies-in-accordance-with-section-1237-of-fy/.

Figure 7: Contribution counts within Microsoft by month



Indeed, before July 2020, most month-to-month contributions from China-tagged entities came from Qihoo 360 and its affiliated labs and teams. The decline in Qihoo's contributions accounts for nearly the entire drop in China-tagged contributions in the Microsoft dataset after July 2020, as well as the increase running up to it.

Crucially, the US Department of Commerce added Qihoo 360 to the Entity List—a list of foreign entities to which the Department applies moderate trade restrictions—on June 5, 2020, as well as Qihoo's UK offices and twenty-three other companies in China and Hong Kong.[77] This would suggest that the decline in China-tagged contributions is primarily a result of Qihoo's shifting legal status combined with their contribution preeminence, perhaps augmented by the inclusion of its UK branches, rather than the public circulation of the RMSV's reporting mandates.

Qihoo 360 is a China-based internet software and security company founded in 2005 by the former head of Yahoo's China operations, Zhou Hongyi. The company has enjoyed a litigious, dynamic history, from lawsuits against Yahoo China, Baidu, Tencent, and others to going private in 2016 as it delisted from the New York Stock Exchange and reshored to China.[78], [79] It also has close ties to the Chinese government, from executives working with the Cybersecurity Association of China[80]—which helped pass the RMSV—to its role in finger-pointing disputes

[77] Bureau of Industry and Security Department of Commerce, "Addition of Entities to the Entity List, Revision of Certain Entries on the Entity List," *Federal Register*, June 5, 2020, https://www.federalregister.gov/documents/2020/06/05/2020-10869/addition-of-entities-to-the-entity-list-revision-of-certain-entries-on-the-entity-list.

[78] Paul Mozur, "Qihoo 360's Zhou Hongyi: Taking Aim at China's Internet," *Wall Street Journal*, November 30, 2012, http://online.wsj.com/article/SB10001424052970204707104578094460340552442.html.

[79] Qihoo 360 Technology Co Ltd, "Qihoo 360 Announces Completion of Merger," *Cision PR Newswire*, July 15, 2016, https://www.prnewswire.com/news-releases/qihoo-360-announces-completion-of-merger-300299435.html.

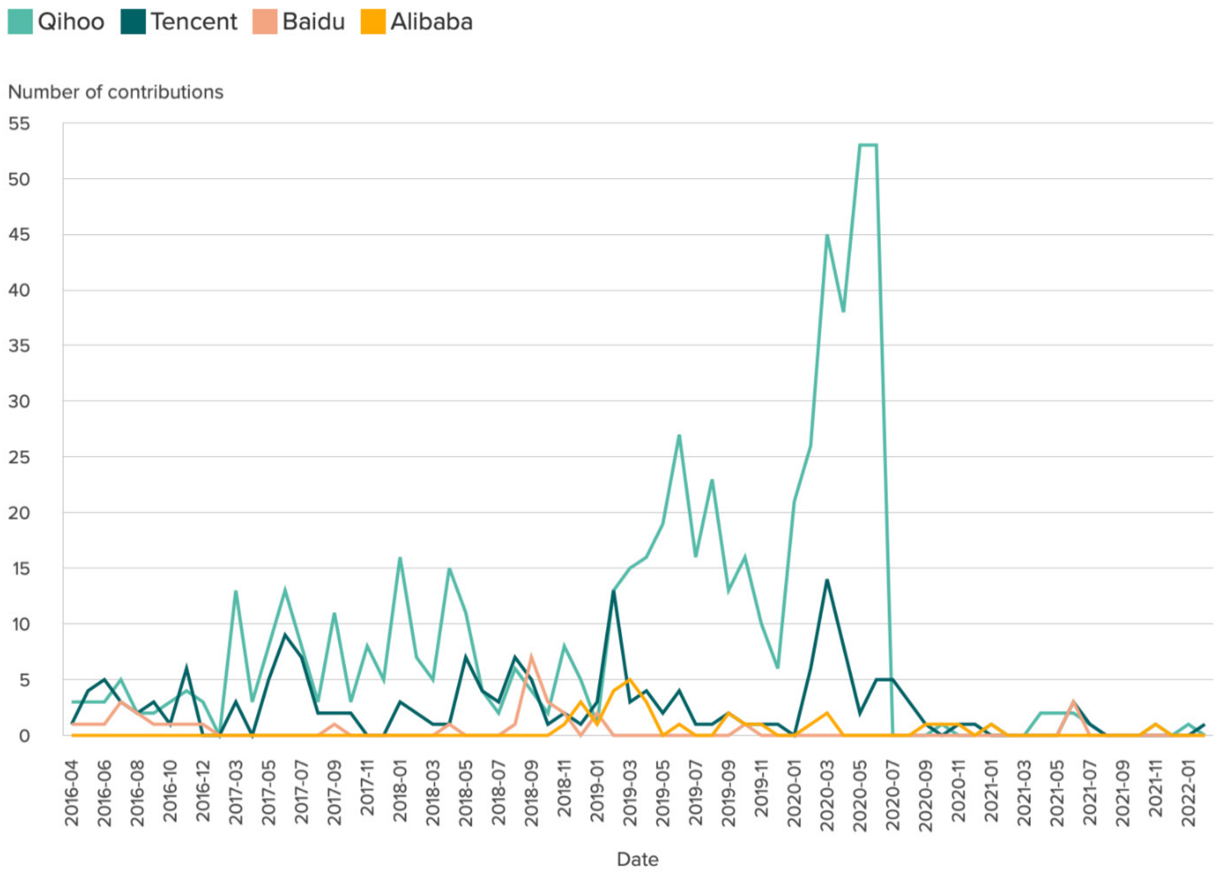
[80] Viola Rothschild and Hongshen Zhu, "A Crack in the Wall? Not So Fast.," Council on Foreign Relations (blog), October 15, 2020, https://www.cfr.org/blog/crack-wall-not-so-fast.

with the United States and China's overall cybersecurity posture.[81] Qihoo's researchers have long dominated hacking competitions like Pwn2Own and the Tianfu Cup as well as Microsoft's security researcher leaderboards.[82] Interestingly, the most recent tweet from one of Qihoo's subsidiary accounts, 360BugCloud, was made on August 6, 2020, right after the decline in Microsoft contributions from the company—and, of course, the tweet bragged about the company's preeminence in that research space.[83] Despite the company's decline in contributions to the Microsoft and Red Hat ecosystems, its researchers still seem active elsewhere—for instance, most recently, Steven Seeley discovered CVE-2022-31664 in early August of 2022, which allows for privilege escalation in VMware products.[84]

Notably, the other large China-tagged entities that demonstrate a similar decline in contribution do not conform to the same time frame. Tencent, for example, contributes through the July 2020 date for a few months before falling off, while Baidu and Alibaba contributions dry up earlier, around early 2019. This suggests that the majority of the chilling effect seen in the MSFT data arises from the Qihoo 360 entity listing—moreover, that the larger reticence of large China-tagged corporations to contribute is part reversion to mean, part generalized hesitance.

The focus on Qihoo 360 might also help provide some context for the uptick in unattributed reports that follows the July 2020 date. Given the reasonably expected

Figure 8: Contribution counts by company by month, Microsoft



[81] John Feng, "China Accuses CIA of Hacking Beijing for over a Decade," *Newsweek*, July 20, 2021, https://www.newsweek.com/china-accuses-cia-hacking-beijing-over-decade-1611321.

[82] 360BugCloud (@360bugcloud), Twitter, August 6, 2020, https://twitter.com/360bugcloud.

[83] 360BugCloud (@360bugcloud), "Qihoo 360 swept the top three ...," Twitter, August 6, 2020, https://twitter.com/360bugcloud/status/1291583230332686339/photo/1.

[84] Jonathan Grieg, "CISA Urges Defenders to Update after VMware Patches Vulnerabilities in Multiple Products," *The Record by Recorded Future* (blog), August 4, 2022, https://therecord.media/cisa-urges-defenders-to-update-after-vmware-patches-vulnerabilities-in-multiple-products/.

delay between receipt of a disclosure and remediating and reporting it, Microsoft likely found itself with a significant number of vulnerabilities from Qihoo 360 disclosed before the entity listing complicated the two companies' relationship. The value continuity between pre-entity-listing Qihoo 360 contributions and post-entity-listing unattributed contributions might imply the company chose not to disclose the source of those discoveries. The fact that disclosure for the elevated levels of unattributed reports was for some five months might hint at the size of the backlog and the time it took to clear. Notably, the decline in unattributed disclosures following the post-July 2020 uptick coincides with a decline in overall contributions to Microsoft, which could imply that the chilling effect caused by the entity listing did impact the entire ecosystem due to the noteworthy productivity of the entity-listed company.

Given that this July 2020 trend existed only in the Microsoft ecosystem, checking for possible causal events within that company's specific context was also necessary. Two possible explanations specific to Microsoft are changes to its bug bounty reward incentive programs both in April and July 2020,[85] when the company reduced or eliminated prizes for certain classes of vulnerabilities that had surged in reporting. In theory, the removal of financial incentives from a specific type of vulnerability research might explain a drop in supply if Qihoo 360 alone focused on the work. There are a few problems with this explanation, however. First, the later bounty change occurred on July 24, 2020, after the reporting date that saw the massive Qihoo 360 drop off—July 14, 2020. Second, the fact that much of the significance in the Qihoo 360 decline derives from the absence of any other similar drop off from other companies or countries frustrates the narrative of removed incentives: total reports would likely also fall off if they had surged around a handful of vulnerability types that no longer paid out.

The data specifying what vulnerabilities Qihoo was reporting before July 2020 and what vulnerabilities were reported after the date by other contributors can help address the argument that Qihoo 360 alone was affected by the reporting changes. 75 percent of the company's findings focused on privilege escalation in the months leading up to July 2020. The April 2020 updates make no mention explicitly of privilege escalation, though technical synonyms are certainly possible, and following the July 2020 collapse, other companies continued to report privilege escalation vulnerabilities. Privilege escalation remains the second highest compensated security impact in fact, only following remote code execution. In simpler terms, the explanation that Qihoo 360 focused on a specific type of bug and stopped contributing at all when it was no longer lucrative doesn't hold insofar as this paper's researchers can determine with limited technical fluency. Other entities continued to the vulnerabilities Qihoo 360 had focused on long after the bounty rule changes. Moreover, Qihoo 360 should in theory have kept reporting 25 percent of their original contributions if the changes did indeed drive a research-type specific decline—instead, the company effectively collapsed to no reporting at all. In truth, the starkness of Qihoo's drop and the complete absence of any other country or company behaving similarly at the same time suggests that something unique to China or Qihoo 360 was at play, and the timing of entity listing provides a more compelling explanation. Finally, it's unclear what portion of the MSRC vulnerability dataset is connected to bounty payouts to begin with—doubtless, some are uncompensated.

Regarding the broader concept of preserving supplies of security information, this finding within the Microsoft data only emphasizes the point: while the RMSV may not have been the causal factor, reliance on a singular legal context, or even one company within a singular legal context, creates a security bottleneck. Changes in law, trade regulation, or even a company's financial status can have an outsized impact on security if those changes affect vulnerability research and disclosure at a particularly productive node, as shown in the data on Qihoo 360. Diversifying sources of research across national lines, market verticals, revenue sources, and other areas all increase the research community's resilience and productivity, avoiding single points of failure.

By-Company Breakdown: Red Hat

The Red Hat data saw a similarly significant decline in China-tagged contributions in 2017 from February to April. This decline did not coincide with any of the critical dates highlighted in analyzing the RMSV—in fact it predates them all. Accordingly, this paper sought to explain that decline with the research first looking for potential causal mechanisms around the 2017 window in general news about Red Hat and Chinese technology firms. For example, in April of 2017, Red Hat and Huawei signed a collaboration agreement for delivering enterprise Linux.[86]

[85] Microsoft, "Microsoft Windows Insider Preview: Bounty Program," microsoft.com, https://www.microsoft.com/en-us/msrc/bounty-windows-insider-preview.

[86] Huawei, "Huawei Signs Server OEM Agreement with Red Hat Enterprise Linux – Huawei Press Center," press release, April 26, 2017, https://www.huawei.com/en/news/2017/4/huawei-oem-agreement-redhat.

Table 9 – By company Red Hat contributions

Red Hat Aliases	Pre April 2017 Sum	Post April 2017 Sum	Delta
Qihoo 360	115	22	93
Zhejiang University	0	21	-21
VenusTech	0	19	-19
Tencent	3	16	-13
NSFOCUS	0	12	-12
Ant Group	0	11	-11
SQLab NCTU	0	11	-11
Huawei	15	10	5
Qianxin Group	0	10	-10
Kunlun Lab	0	6	-6
UHK	0	6	-6
Tsinghua University	0	5	-5

Earlier in the same month, then-President Trump met with Xi Jinping at a general-purpose US-China summit.[87] However, the summit concluded on good terms, and the mechanism by which it or a Huawei-Red Hat deal would reduce China-tagged contributions are unclear.

For better insight, the team replicated the aliasing process used on the Microsoft dataset and discovered that, once again, Qihoo 360 was the driving force behind much of the China-tagged contributions in the Red Hat data, at least before April 2017. The company was tagged in almost 80 percent of Chinese contributions prior to April 2017 and a mere 12 percent afterward, and its work was the overwhelming source of trends in the total China-tagged contributions before the steep decline. Huawei, Tencent, Ant Group, NSFOCUS, VenusTech, and a handful of universities were also somewhat significant contributors to the Red Hat ecosystem, but by an order of magnitude less than Qihoo 360, and without noteworthy activity on either side of the key April 2017 date. If anything, their contributions grew years after the Qihoo decline.

The Red Hat data, unlike that from Microsoft, does not show an increase in unattributed contributions coincident with the April 2017 decline. Moreover, the team could find no clear exogenous event that might have caused Qihoo 360 to reduce its contributions to the ecosystem to near-zero. In theory, perceived future competition from Huawei researchers turning to Red Hat products as part of their corporate agreement may have incentivized Qihoo, a much smaller company, to shift its limited resources elsewhere, particularly as their concurrent privatization may have created an environment of financial uncertainty.[88] However, this is speculative at best. No other contributing entity was as prolific as Qihoo 360, and no entity took its place either. Most likely, this data captures a change in personnel or internal policy either at Red Hat, Qihoo 360, or both, and its implications for the fragility of the research community and the dangers of centralized dependence are unchanged.

[87] "Trump, Xi End Summit with 'Tremendous' Progress," *Aljazeera*, April 7, 2017, https://www.aljazeera.com/news/2017/4/7/trump-xi-end-summit-with-tremendous-progress.

[88] Henny Sender, "Cayman Lawsuits Challenge Valuations of Delisted Chinese Companies," *Financial Times*, February 28, 2017, https://www.ft.com/content/ed8768f4-fd1a-11e6-8d8e-a5e3738f9ae4.

DISCUSSION

These data suggest that the RMSV has not yet had a significant impact on the supply of vulnerability disclosures in most of these codebases, but with the possible and notable exception of Microsoft. However, that is not to suggest that the research community in China is immune to its legal context. First, the potential for a delayed effect outside of this study's timeframe remains, especially when acknowledging the considerable vagueness in CVE reporting and dating practices—depending on the duration of vulnerability retention, CVEs regulated by the RMSV may simply not have entered the public record in appreciable numbers yet. It is possible that the RMSV will more unambiguously impact vulnerability research in the future as enforcement practices come to light and undisclosed vulnerabilities reported prior to its enactment grow rarer over time. Second, two of the largest datasets utilized in this study do seem to some form of China-based supply shock, even if only one might be tied to the RMSV, and neither trickles clearly into global reporting numbers. For example, in the Microsoft dataset, that effect may be correlated with either the first public knowledge of the RMSV reporting requirements, US sanctioning of Chinese technology firms,[89] other Chinese cybersecurity legislation, or some combination of the three, and its impact continues to the present day. In the Red Hat dataset, the cause of the decline in reporting is unclear as it predates any reported knowledge of the RMSV, and contributions from China appear to have since recovered to earlier levels.

Open-Source Spotlight

This paper's findings are of particular importance to the open-source ecosystem. At an abstract level, vulnerability research and disclosure closely mirror the system of open-source contributions: developers, motivated by profit, prestige, personal interest, and other factors, contribute to open-source projects they do not necessarily maintain. Similarly, legal environments can indeed shape this supply of contributors. For example, various sanction regimes led to the blocking of GitHub developers in Iran, Syria, Crimea, and other geographies in 2019.[90] And similar to the vulnerability research ecosystem, China is well noted as a significant contributor to and user of open-source projects, where the

[89] US Department of Defense, "DOD Releases List of Additional Companies, in Accordance with Section 1237 of FY99 NDAA," news release, August 28, 2022, https://www.defense.gov/News/Releases/Release/Article/2328894/dod-releases-list-of-additional-companies-in-accordance-with-section-1237-of-fy/.

[90] Rita Liao and Manish Singh, "GitHub Confirms It Has Blocked Developers in Iran, Syria and Crimea," *TechCrunch*, July 29, 2019, https://social.techcrunch.com/2019/07/29/github-ban-sanctioned-countries/.

geographical distribution of developers resembles the distribution of vulnerability disclosures by country.[91], [92] In his writing on the shifting open-source ecosystem in China, Kevin Xu notes that this trend is likely to continue: “Why the central government would embrace open source is rather straightforward: it prefers to favor flexible technologies that aren’t tied to certain vendors, companies, or countries, so it can control and shape them at will. The thinking here is not that different from the rationale behind any large enterprise’s adoption of open source, in or outside China. ‘Self-reliance’ as a national theme and technological imperative will be front and center for China for many years to come.”[93]

This sustained interest and the general predominance of open-source software in codebases—both open and proprietary—makes the supply of open-source contributors as valuable as the supply of vulnerability research, and there is considerable overlap between the two. Potential threats to that supply are more varied in the open-source ecosystem as well—for example, China while on the one hand embracing GitHub has also worked to establish its own open-source ecosystem, Gitee.[94] While there is nothing inherently wrong with competing codebases, and even some security to be derived from that diversity,[95] fracturing open-source contributor bases might drain valuable developers from an already resource-strapped environment.

At the largest scale, these data illustrate a degree of fragility in external contribution ecosystems—the tireless work of security researchers cannot be taken for granted, and imprecise vulnerability-reporting laws do indeed have the potential to limit their contributions. The specifics of the mechanisms involved are less clear—say, whether laws regulating domestic researchers or limiting interactions with foreign entities providing research have more impact. Connecting these supply-side effects to security incidents downstream is almost impossible—one cannot know what vulnerabilities might have been discovered by researchers who would have otherwise been searching for them. Nonetheless, any reduction in the rate of vulnerability discovery or constraint on reporting those vulnerabilities to affected entities and codebase maintainers promises to reduce cybersecurity at large.

[91] Wachs et al., “The Geography of Open Source Software: Evidence from GitHub.”

[92] Silver Keskkula, “What Is This Github You Speak Of?” *Medium* (blog), September 7, 2016, https://medium.com/@keskkyla/https-medium-com-keskkyla-what-is-this-github-you-speak-of-dd457a29771.

[93] Kevin Xu, “Open Source in China: The Game,” Interconnected, May 10, 2020, https://interconnected.blog/open-source-in-china-the-game/.

[94] Meaghan Tobin, “China Wants to Build an Open Source Ecosystem to Rival GitHub,” Rest of World, January 19, 2021, https://restofworld.org/2021/china-gitee-to-rival-github/.

[95] Daniel Geer et al., “CyberInsecurity: The Cost of Monopoly,” Schneier on Security, September 24, 2003, https://www.schneier.com/essays/archives/2003/09/cyberinsecurity_the.html.

CONCLUSION & RECOMMENDATIONS

The passage of the RMSV and its coincidence with an increased US government attention on the security and sustainability of open-source software provide a significant opportunity for both government and industry. The risk to the cybersecurity of the technology ecosystem of laws like the RMSV is the potential isolation of significant subsets of the research community from the larger global supply of vulnerability disclosures. This kind of fear and fragmentation only adds risk to an already difficult to mitigate landscape.

The United States and allied governments can proactively address these kinds of supply-side security effects in coordination with industry by further expanding the supply of disclosure information rather than mimicking such laws to hoard vulnerability disclosures like a scarce resource. Key to this proactive approach is smoothing the journey from discovery to disclosure to patching across jurisdictions, providing better, more consistent tooling for vulnerability discovery, and working to better recognize and countercyclically invest against emerging gaps in global vulnerability disclosure. Three recommendations come to the fore:

1 Harmonize Vulnerability Disclosure across the United States and Allies

The United States, through the National Cyber Director in partnership with CISA's Computer Emergency Response Team (US-CERT) should seek to lower barriers to vulnerability disclosure in a group of like-minded allies, including Australia, New Zealand, the United Kingdom, Estonia, and the Netherlands. Such an activity should expand to include Japan and other NATO members in short order. Organized as an ad-hoc working group, staff-level engagement across these states should work to harmonize domestic vulnerability-disclosure laws so that cross-jurisdictional disclosure is less burdensome and uncertain for vulnerability researchers. Harmonization could focus on requirements for companies to publish and adhere to CVD policies and the removal of legal penalties for non-commercial reverse-engineering activities, among other avenues. The working group should not seek to determine a common definition of "good-faith" security research, but rather seek near-term wins to better knit these jurisdictions together into a common disclosure environment.

Properly realized, this harmonization would deepen the supply of vulnerability disclosures to firms and maintainers in the United States and allied states, promoting more effective function as a single disclosure environment. As a second stage, the working group should consider manners of establishing international processes and protections for receiving and validating anonymous vulnerabilities. These efforts should include members of civil society and industry on a limited basis, with Joint Cyber Defense Collaborative (JCDC) members as logical starting partners.

2 Improve the Quality and Consistency of Support of Vulnerability Discovery Tools

Should authorization of the Critical Technology Security Centers (CTSC) finally pass through the National Defense Authorization Act (NDAA) conference process, the director of CISA should include vulnerability-discovery tooling and long-term support for these tools as eligible areas of investment for the Open-Source Software CTSC. Where policy moves threaten to curtail the supply of vulnerability disclosure, wider access to more capable, better-supported vulnerability discovery tools can help counter that effect. Providing these tools as open source for free use by the community will directly benefit open-source software security too, and such an approach could well have similar effects on proprietary code. This would achieve the above state goals while furthering the administration's avowed interest in improving the security of software.[96] This would also serve as a good example of indirect investment from the public sector in the security of open-source software and follows recommendation thirteen of the recently released Cyber Safety Review Board report.[97]

[96] Biden, Executive Order 14028.

[97] Cyber Safety Review Board, "Review of the December 2021 Log4j Event."

3 Track Vulnerability Disclosure Patterns and Invest Against Gaps

The National Security Agency's (NSA) Cybersecurity Directorate should work to track patterns in vulnerability disclosures, collaborating with researcher and industry partners through the Cybersecurity Collaboration Center where possible. While the resulting trends analysis need not be public, it should remain unclassified for maximal usefulness as evidence to compel investment where gaps or the absence of disclosures appears. This monitoring effort attempts to understand the sourcing patterns of vulnerability disclosures and where disclosures of a similar style or against critical software cluster.[98] This tracking program should help identify where those disclosures significantly decline, perhaps as the result of laws impeding disclosure from other jurisdictions.

If such a gap emerges, the Directorate's leadership should collaborate with the National Cyber Director, leveraging the office's budgetary review authorities, as well as existing federal bug-bounty programs to offer added incentives, such as doubled payments, for vulnerabilities like those in the identified gap submitted to private bounty programs. This countercyclical investment could help incentivize further disclosure against critical software and offset the effects of policies that limit disclosures. This program would bring greater awareness of important trends in vulnerability disclosure regardless of the reason that such disclosure gaps emerged. This funding would be particularly useful to incentivizing the discovery of vulnerabilities in technologies with sufficient maturity to have driven vulnerability density towards sparseness—in other words, the discovery of vulnerabilities in well-scrutinized systems are more valuable from a security standpoint,[99] and incentives to find them can help economic rewards reflect that.

The supply of vulnerability disclosures is a significant driver of security outcomes in software. Threats to that supply will, over time, reduce the security of software and add risk for individual users and organizations. This is perhaps most important for open-source software, which thrives on disclosures and contributions more generally from outside of the original developer network. As the policy community continues to study the effects of the RMSV and other regulations, greater sensitivity of the potential diverging effects of these policies on open-source and proprietary code should help motivate wider support for public-sector investments in the health and sustainability of the open-source software ecosystem. For China watchers, the future of enforcement of the RMSV and related policies would benefit from better public study of how the laws apply under varying political conditions and to companies and individual researchers. A more concrete understanding of the law's practical implementation will help counter the seemingly purposeful ambiguity it has created.

The United States and its allies should see the disclosure of Log4Shell as a call to action to improve the scale and resilience of the global supply of vulnerability disclosure. Domestic legal changes to improve vulnerability research in single countries are useful, but they are insufficient to address the strategic ramifications of a potential supply shock. More can be done, to proactively limit the harm from such a moment and improve the state of software security along the way. As a closing note, it is particularly important to acknowledge the general goodwill of researchers in this space. In many ways, the Log4j case illustrates this emphatically—a corporate researcher found and responsibly disclosed a crippling vulnerability in an open-source library directly to its maintainers and kept them abreast of events directly relevant to their remediation timeline, all in spite of the RMSV and other legal contexts and with no apparent profit motive. That kind of relationship, writ large across the security ecosystem, is one well worth preserving.

[98] Biden, Executive Order 14028.

[99] Dan Geer, "For Good Measure: The Undiscovered," Usenix, *;Login:* 40, no. 2 (April 2015), 50–52, https://www.usenix.org/system/files/login/articles/login_apr15_12_geer.pdf.

APPENDIX I: DATA CHALLENGES

Gathering from organizational feeds rather than CVE datasets allows for more complex multi-vector acknowledgment, most prominently in instances where a researcher showed an existing vulnerability's impact on a previously unconnected product. It also allows focusing in on specific vendor and product types. For example, the VMware Security Advisory (VMSA) VMSA-2011-0004.3 responds to the following CVEs: CVE-2010-3613, CVE-2010-3614, CVE-2010-3762, CVE-2010-3316, CVE-2010-3435, CVE-2010-3853, CVE-2010-2059, and CVE-2010-3609. The VMWare security advisory credits Nicolas Gregoire and US CERT for reporting the issue that one of these CVEs created for their Service Location Protocol daemon regarding vulnerability to a denial of service attack. Most likely, they are referring specifically to CVE-2010-3609. However, a GitHub CVE list mentions Gregoire in none of those entries,[100], [101] though an exploit proof of concept on a common exploit database appears authored by Gregoire.[102]

That is not to say that the GitHub CVE data is "bad," but that—between the changing standards in its recorded fields and the primary focus of its records—it captures a different segment of the research community. Further analyses could gather valuable insight from scraping through both the exploit and GitHub database credits and authorship logs. These analyses will face constraints too, though—for example, using exploit-db.com filters out all researchers who didn't upload proof-of-concept code to that specific database, which likely biases against the inclusion of researchers outside of the English-speaking world. Accordingly, Google's Security Research Team has contributed over one-thousand entries to exploit-db.com compared to just one from Qihoo 360. In contrast, Apple's security advisories mention Qihoo 360 more than 300 times, versus 2000 mentions of Google that include multiple departments (Google Security Team, Google's TAG, Google Project Zero, etc.).

It's difficult to compare the 1:1,000 and 3:20 ratios directly, especially when credits might refer to CVE discovery, CVE application, or other nuanced forms of acknowledgment—some credits even imply that researchers played a role in developing patches. Nonetheless, working within a company's public-facing ecosystem will help reduce (but not eliminate) bias against international research and deal with concerns about filtering effects where exploit code must be publicly disclosed for inclusion in a dataset.

[100] CVE-Team (Auto-merge), "CVEProject / cvelist," GitHub, accessed August 2, 2022, https://github.com/CVEProject/cvelist

[101] CVE-Team (Synchronized Data), "CVEProject / cvelist," GitHub, accessed August 2, 2022, https://github.com/CVEProject/cvelist/blob/master/2010/3xxx/CVE-2010-3609.json

[102] Exploit Database, "OpenSLP 1.2.1 / < 1647 trunk - Denial of Service," August 5, 2011, https://www.exploit-db.com/exploits/17610.

APPENDIX II: THE FULL RMSV

Sourced from http://www.cac.gov.cn/2021-07/13/c_1627761607640342.htm, translation provided by Google Translate.

Notice of the Ministry of Industry and Information Technology and the State Internet Information Office of the Ministry of Public Security on Issuing the Provisions on the Management of Security Vulnerabilities of Network Products

July 13, 2021 17:11

Notice of the Ministry of Industry and Information Technology and the State Internet Information Office of the Ministry of Public Security on Issuing the Provisions on the Management of Security Vulnerabilities of Network Products

Ministry of Industry and Information Technology Network Security [2021] No. 66

All provinces, autonomous regions, municipalities directly under the Central Government and Xinjiang Production and Construction Corps industry and informatization departments, Internet Information Offices, and public security departments (bureaus), and communications administrations of all provinces, autonomous regions, and municipalities directly under the Central Government:

The "Regulations on the Management of Security Vulnerabilities of Network Products" are hereby issued and will come into force on September 1, 2021.

Ministry of Industry and Information Technology State Internet Information Office Ministry of Public Security

July 12, 2021

Provisions on the Management of Security Vulnerabilities of Network Products

Article 1 In order to regulate the discovery, reporting, patching, and release of network product security vulnerabilities, and prevent network security risks, these Provisions are formulated in accordance with the «Network Security Law of the People›s Republic of China».

Article 2 Providers and network operators of network products (including hardware and software) within the territory of the People›s Republic of China, as well as organizations or individuals engaged in activities such as the discovery, collection, and release of network product security vulnerabilities, shall abide by these Provisions.

Article 3 The Cyberspace Administration of China is responsible for coordinating and coordinating the management of network product security vulnerabilities. The Ministry of Industry and Information Technology is responsible for the comprehensive management of network product security vulnerabilities, and undertakes the supervision and management of network product security vulnerabilities in the telecommunications and Internet industries. The Ministry of Public Security is responsible for the supervision and management of network product security loopholes, and cracks down on illegal and criminal activities that take advantage of network product security loopholes in accordance with the law.

Relevant competent departments strengthen cross-departmental coordination, realize real-time sharing of network product security vulnerability information, and conduct joint assessment and disposal of major network product security vulnerability risks.

Article 4 No organization or individual may use network product security loopholes to engage in activities that endanger network security, and may not illegally collect, sell, or publish information on network product security loopholes; It provides technical support, advertising promotion, payment settlement and other assistance.

Article 5 Network product providers, network operators and network product security vulnerability collection platforms shall establish and improve network product security vulnerability information receiving channels and keep them unblocked, and keep network product security vulnerability information receiving logs for no less than 6 months.

Article 6 Relevant organizations and individuals are encouraged to notify network product providers of security vulnerabilities in their products.

Article 7 Network product providers shall perform the following network product security vulnerability management obligations, ensure that their product security vulnerabilities are promptly patched and reasonably released, and guide and support product users to take preventive measures:

(1) After discovering or learning that there are security vulnerabilities in the provided network products, it shall immediately take measures and organize the verification of the security vulnerabilities, and evaluate the degree of harm and the scope of influence of the security vulnerabilities; for the security vulnerabilities existing in its upstream products or components, it shall Immediately notify the relevant product provider.

(2) The relevant vulnerability information shall be submitted to the Network Security Threat and Vulnerability Information Sharing Platform of the Ministry of Industry and Information Technology within 2 days. The submitted content shall include the product name, model, version, and technical characteristics, harm, and scope of influence of the vulnerability that have network product security vulnerabilities.

(3) It should organize the repair of network product security vulnerabilities in a timely manner, and if it is necessary for product users (including downstream manufacturers) to take measures such as software and firmware upgrades, the network product security vulnerability risks and repair methods should be promptly notified to potentially affected product users, and provide necessary technical support.

The network security threat and vulnerability information sharing platform of the Ministry of Industry and Information Technology simultaneously reports relevant vulnerability information to the National Network and

Information Security Information Notification Center and the National Computer Network Emergency Technology Handling Coordination Center.

Network product providers are encouraged to establish a security vulnerability reward mechanism for the provided network products, and rewards are given to organizations or individuals who discover and report security vulnerabilities of the provided network products.

Article 8 After a network operator discovers or learns of a security loophole in its network, information system and equipment, it shall immediately take measures to verify and complete the repair of the security loophole in a timely manner.

Article 9 : Organizations or individuals engaged in the discovery and collection of network product security vulnerabilities shall release information on network product security vulnerabilities to the public through network platforms, media, conferences, competitions, etc. principles and abide by the following provisions:

(1) Vulnerability information shall not be released before network product providers provide network product security vulnerability repair measures; if it is deemed necessary to release in advance, it shall evaluate and negotiate with relevant network product providers, and report to the Ministry of Industry and Information Technology and the Ministry of Public Security , published by the Ministry of Industry and Information Technology and the Ministry of Public Security after evaluation.

(2) Not to publish the details of the security loopholes in the networks, information systems and equipment used by network operators.

(3) Do not deliberately exaggerate the harm and risk of network product security vulnerabilities, and do not use information on network product security vulnerabilities to conduct malicious speculation or conduct fraud, extortion and other illegal and criminal activities.

(4) Not to publish or provide programs and tools specially used to exploit the security loopholes of network products to engage in activities that endanger network security.

(5) When releasing network product security loopholes, it shall simultaneously release repairs or preventive measures.

(6) During the period of major national events, without the consent of the Ministry of Public Security, it is not allowed to release information on network product security vulnerabilities without authorization.

(7) Not to provide undisclosed network product security vulnerability information to overseas organizations or individuals other than network product providers.

(8) Other relevant provisions of laws and regulations.

Article 10 Any organization or individual establishing a network product security vulnerability collection platform shall file with the Ministry of Industry and Information Technology. The Ministry of Industry and Information Technology shall promptly notify the Ministry of Public Security and the Cyberspace Administration of China of relevant vulnerability collection platforms, and publish the vulnerability collection platforms that have passed the filing.

Organizations or individuals who find security vulnerabilities in network products are encouraged to report to the Ministry of Industry and Information Technology’s Network Security Threat and Vulnerability Information Sharing Platform, National Network and Information Security Information Notification Center Vulnerability Platform, National Computer Network Emergency Technology Handling Coordination Center Vulnerability Platform, China Information Security The evaluation center vulnerability database reports network product security vulnerability information.

Article 11 Organizations engaged in the discovery and collection of network product security vulnerabilities shall strengthen internal management and take measures to prevent information leakage and illegal release of network product security vulnerabilities.

Article 12 If a network product provider fails to take measures to remedy or report network product security vulnerabilities in accordance with these regulations, the Ministry of Industry and Information Technology and the Ministry of Public Security shall deal with it according to their respective responsibilities; If the circumstances stipulated in this article are met, punishment shall be imposed in accordance with the provisions.

Article 13 If a network operator fails to take network product security loophole repairs or preventive measures in accordance with these regulations, it shall be handled by the relevant competent departments according to law; if it constitutes a situation specified in Article 59 of the «People›s Republic of China Network Security Law», the regulations shall be followed. be punished.

Article 14 Violation of these regulations to collect and publish network product security vulnerability information shall be handled by the Ministry of Industry and Information Technology and the Ministry of Public Security in accordance with their respective responsibilities; punished in accordance with this provision.

Article 15 Those who use network product security loopholes to engage in activities that endanger network security, or provide technical support for others to use network product security loopholes to engage in activities endangering network security, shall be handled by the public security organs according to law; Those who fall under the circumstances stipulated in Article 63 shall be punished in accordance with the provisions; if a crime is constituted, criminal responsibility shall be investigated according to law.

Article 16 These regulations shall come into force on September 1, 2021.

APPENDIX III: NULL FINDING CHARTS

Figure 10: Contribution counts by country per month, Apple iOS

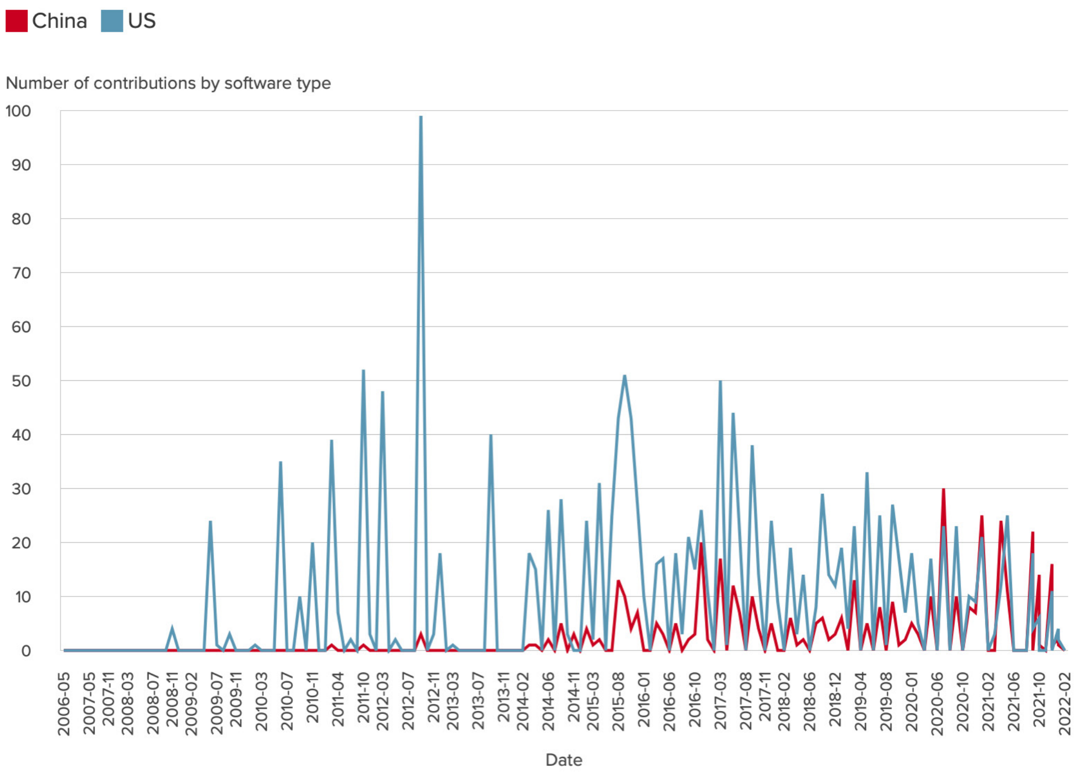


Figure 11: Contribution counts by country per month, VMware

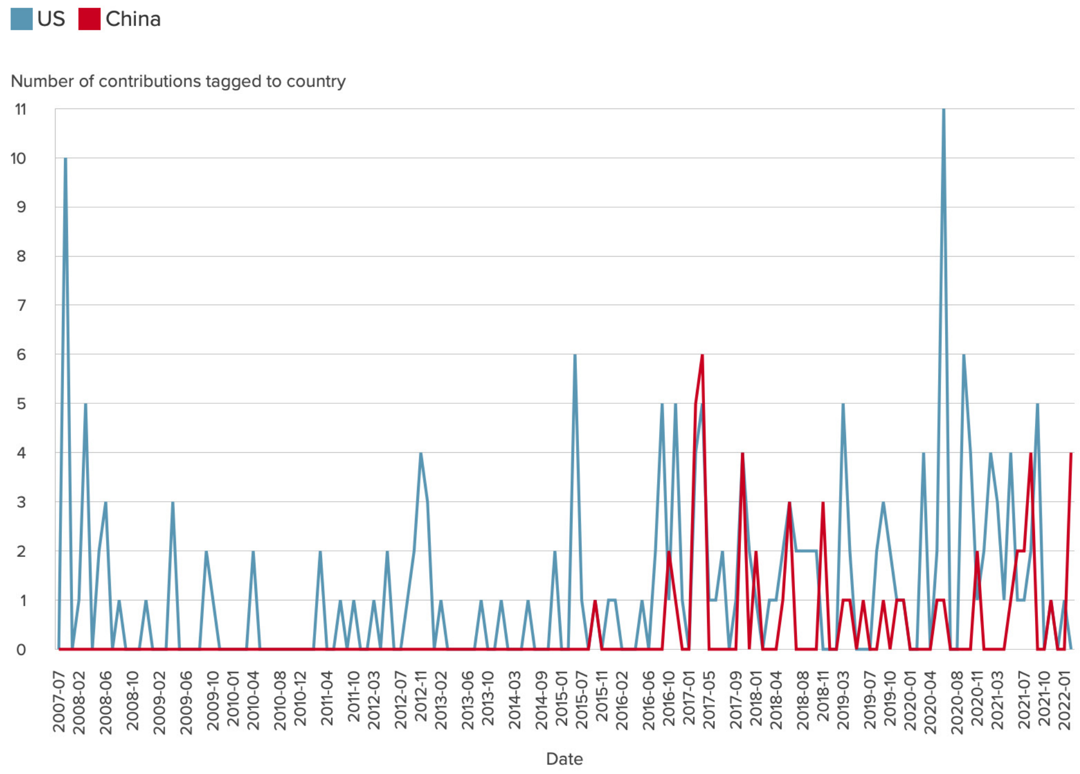


Figure 12: Contributions by country per month, Apple Safari (browsers)

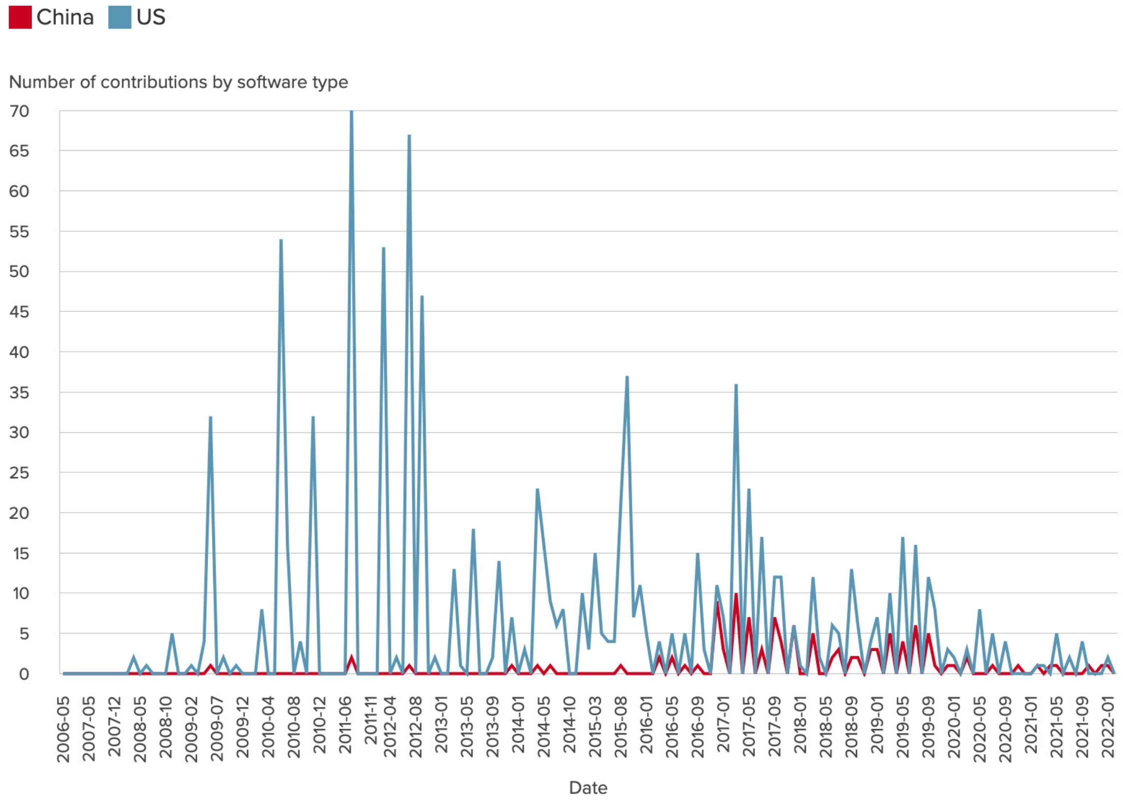


Figure 13: Contributions by country per month, Apple iOS (mobile operating systems)

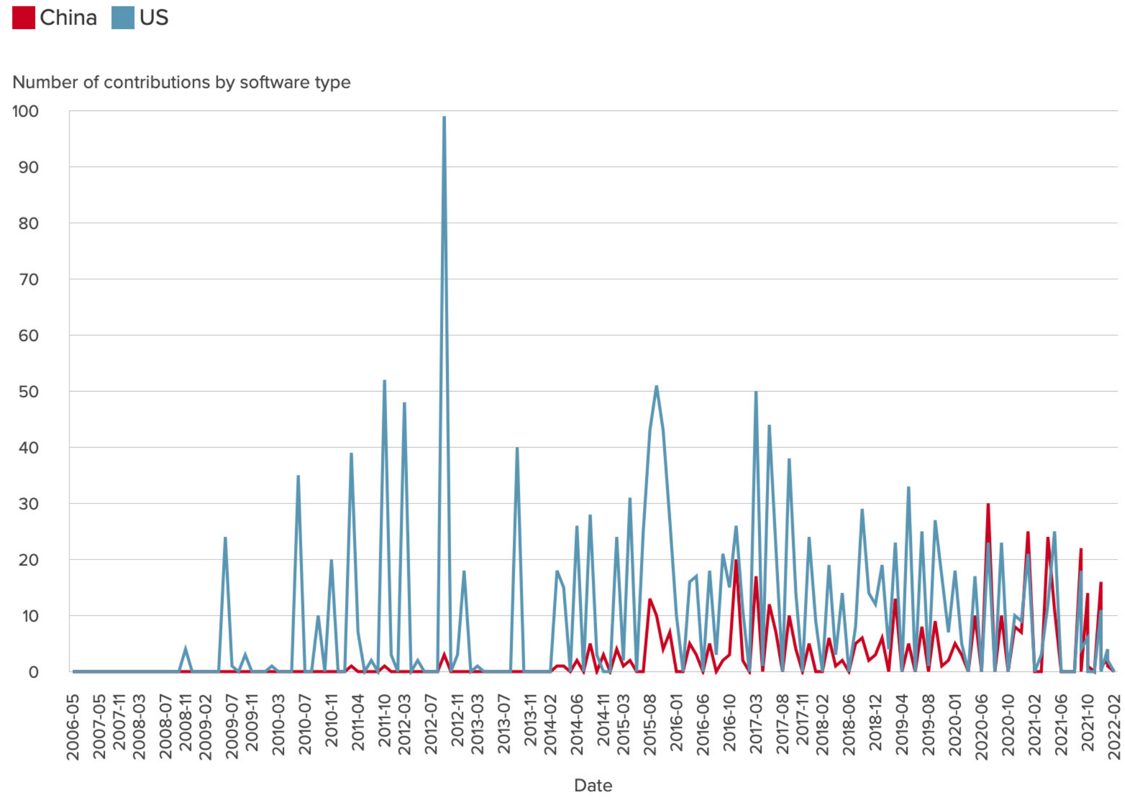


Figure 14: Contributions by country per month, Apple macOS (operating systems)

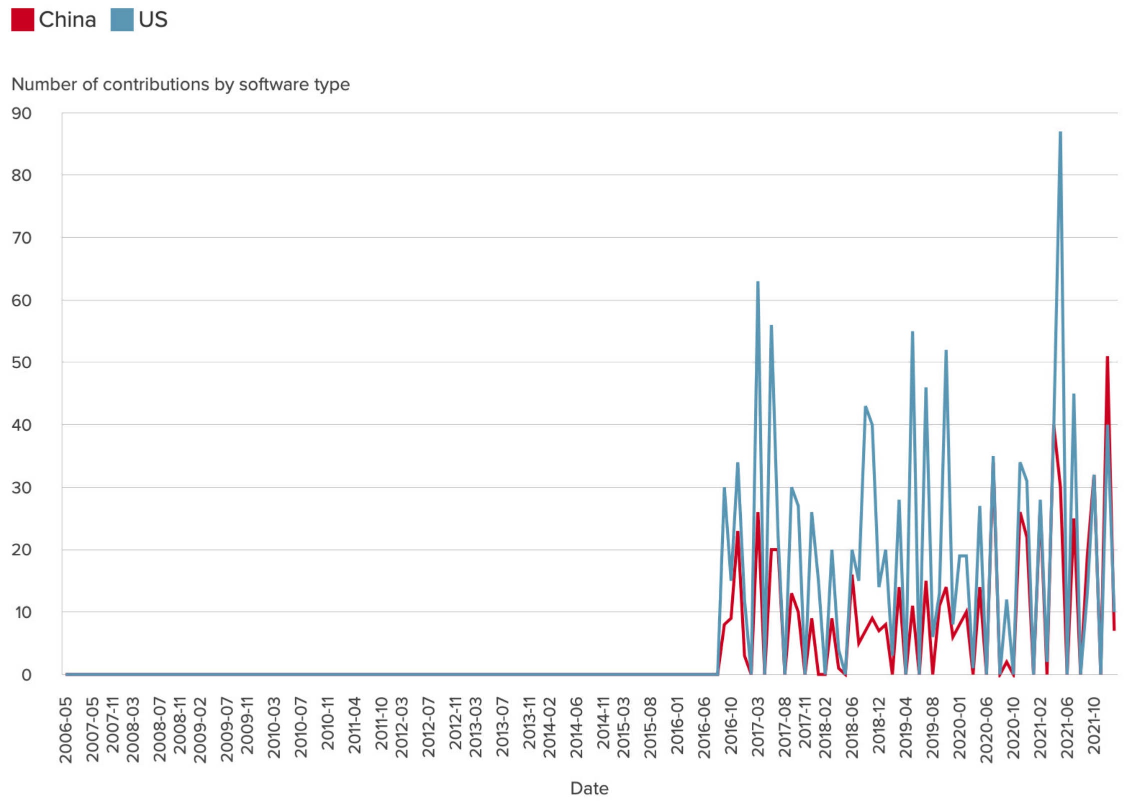


Figure 15: Contributions by country per month, Microsoft Edge and Internet Explorer (browsers)

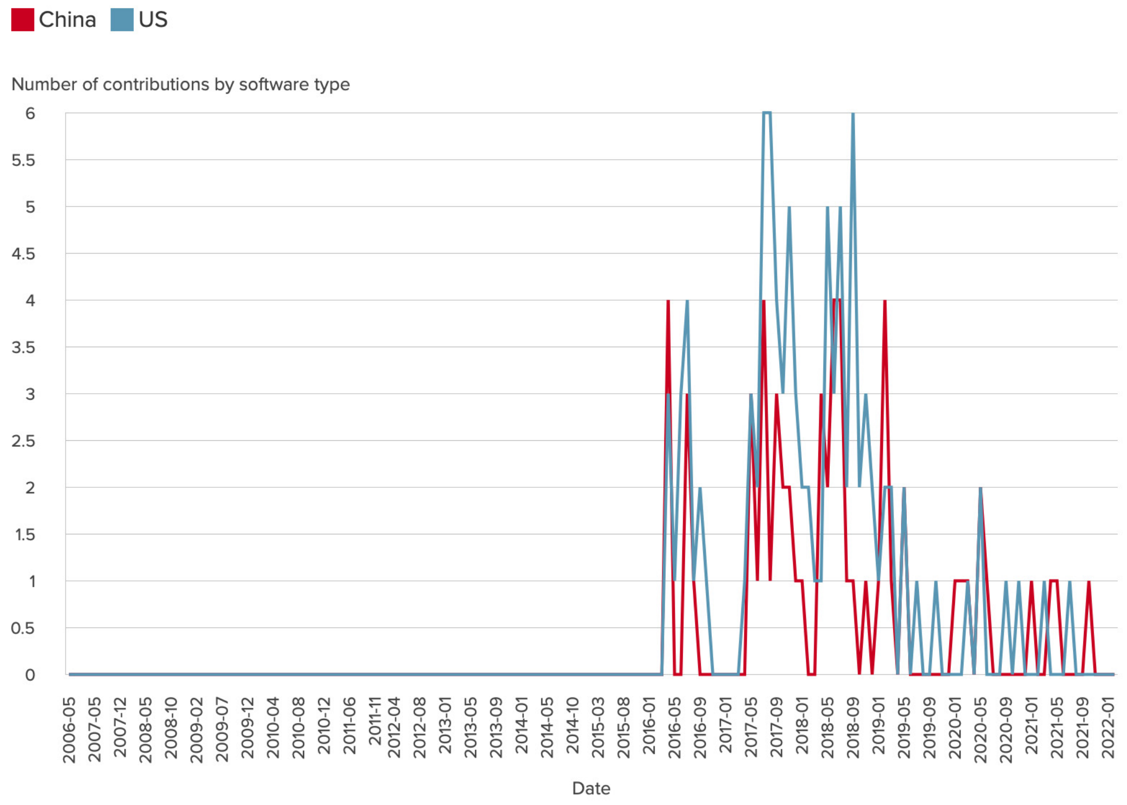


Figure 16: Contributions by country per month, Microsoft Hyper-V (hypervisors)

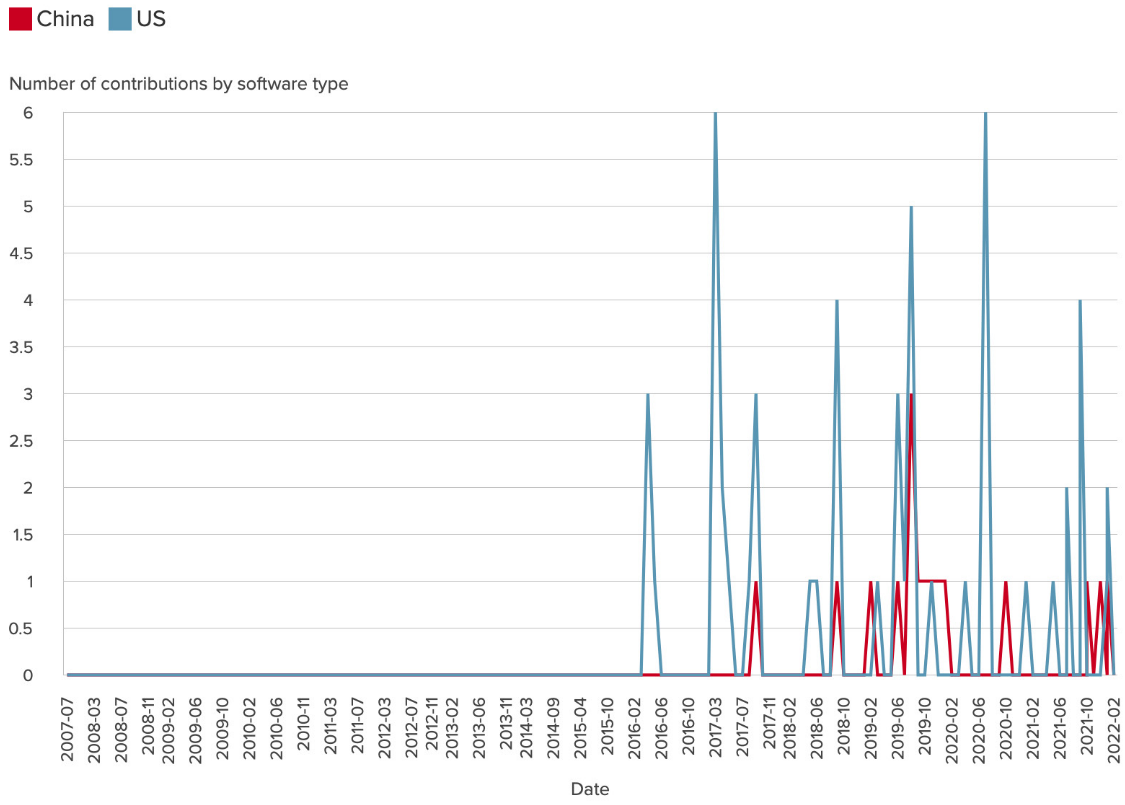
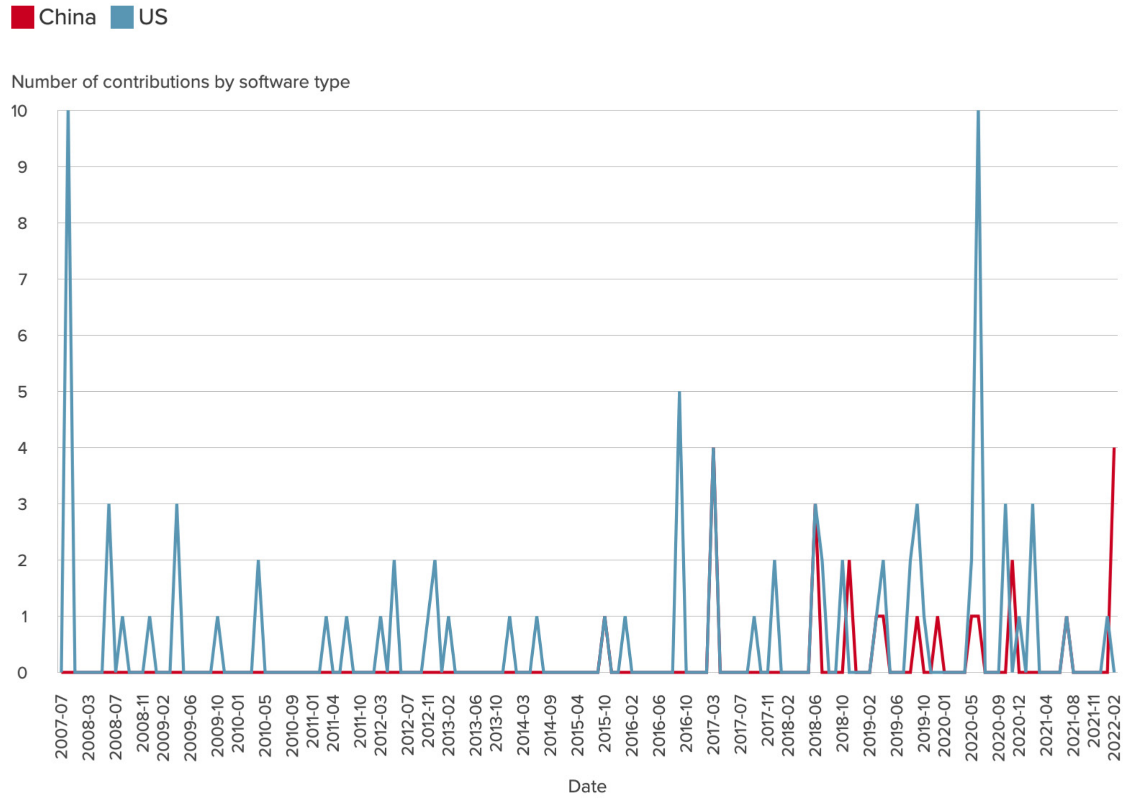


Figure 17: Contributions by country per month, VMware hypervisors



ABOUT THE AUTHORS

Stewart Scott is an assistant director with the Atlantic Council's Cyber Statecraft Initiative under the Digital Forensic Research Lab (DFRLab). He works on the Initiative's systems security portfolio, which focuses on software supply-chain risk management and open-source software security policy. Stewart earned his B.A. from Princeton University at the School of Public and International Affairs along with a minor in Computer Science. His course of study centered on misinformation, social media policy, online extremism, journalism, and American political and economic history. He joined the Atlantic Council after interning with its Cyber Statecraft Initiative.

Sara Ann Bracket is a research assistant at the Atlantic Council's Cyber Statecraft Initiative under the Digital Forensic Research Lab (DFRLab). She focuses her work on open-source software security, software bills of material, and software supply-chain risk management and is currently an undergraduate at Duke University.

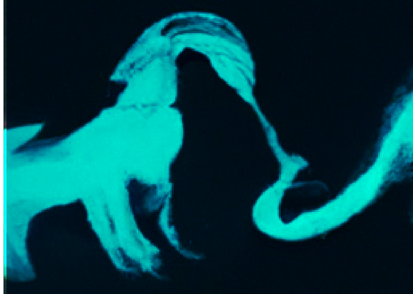
Yumi Gambrill is a master's candidate at Georgetown University's Security Studies Program. She recently moved back to the United States after nearly seven years in the United Arab Emirates, where she completed her BS in chemistry at New York University Abu Dhabi. After graduation, Yumi was a management consultant at Booz Allen Hamilton, focusing on defense and security strategy and public administration reform in the Middle East and North Africa region. Her professional interests include doctrine and norms development for cyber and hybrid conflict, US-East Asia policy, and public-sector organizational transformation. In her free time, she is an avid baker and maker of Japanese sweets, violinist, and scuba diver.

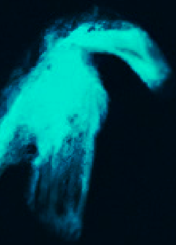
Emmeline Nettles is a research assistant studying international affairs with minors in Chinese and creative technology at the University of Colorado Boulder. Prior to joining the Atlantic Council, she was an undergraduate research assistant in the University of Colorado Boulder's political science research lab, STUDIO, where she conducted quantitative analysis on regional international organizations in Africa. Emmeline is interested in continuing to study cyber policy, particularly how the lack of norms in censorship of social media affects access to information as well as vulnerabilities found through open-source intelligence. She speaks some Chinese and German and has experience with a variety of programming languages. In her free time, she continues her Chinese studies and practices Muay Thai.

Trey Herr is the director of the Atlantic Council's Cyber Statecraft Initiative under the Digital Forensic Research Lab (DFRLab). His team works on cybersecurity and geopolitics including cloud computing, the security of the internet, supply chain policy, cyber effects on the battlefield, and growing a more capable cybersecurity policy workforce. Previously, he was a senior security strategist with Microsoft handling cloud computing and supply chain security policy as well as a fellow with the Belfer Cybersecurity Project at Harvard Kennedy School and a non-resident fellow with the Hoover Institution at Stanford University. He holds a PhD in Political Science and BS in Musical Theatre and Political Science.

Atlantic Council

Board of Directors





The Atlantic Council is a nonpartisan organization that promotes constructive US leadership and engagement in international affairs based on the central role of the Atlantic community in meeting today’s global challenges.

1030 15th Street, NW, 12th Floor,
Washington, DC 20005
(202) 778-4952
www.AtlanticCouncil.org