COVERING CYBER

Media Coverage of Cyber Issues: *2020-2023 Update*

Sean Aday, Ph.D.

Institute for Public Diplomacy and Global Communication

George Washington University

COVERING CYBER

MEDIA COVERAGE OF CYBER ISSUES SINCE 2014

ABOUT THE REPORT

This report updates the 2021 study, “Media Coverage of Cyber Issues: 2019-2020 Update” with an analysis of coverage in mainstream media between 2020 and the first quarter of 2023.

This represents the final report in a series funded by the Hewlett Foundation as part of its cyber initiative. It finds evidence of several ongoing trends identified in earlier reports, showing how media have covered the evolution of and full integration of digital technologies into virtually every aspect of 21st Century life. Throughout the period of study, many aspects of media coverage have remained the same, especially in terms of the issues that dominate coverage and the privileged role political elites have in discussing them through the press. Who is to blame for issues and concerns related to cyber changes at the margins but still tends to reflect U.S. foreign policy priorities and citizens’ concerns about the potentially pernicious reach of technology into their lives. That said, this final report also updates the analysis beyond the last study’s tumultuous time period that included the COVID-19 pandemic, calls for racial justice following the murder of George Floyd, and various attempts to subvert democracy, overturn a presidential election, and attack American political institutions, including most notably the U.S. Capitol. The period studied here includes the aftermath of those events and thus represents a kind of return to normalcy in American life, though a precarious one where the previous threats still lurk on the horizon.

COVERING CYBER

About the Author:

Sean Aday is an associate professor of media and public affairs and international affairs at George Washington University.

About IPDGC:

The Institute for Public Diplomacy and Global Communication at George Washington University is a leading organization in the field of public diplomacy and global communication issues. It is jointly administered by the Columbian College of Arts and Sciences and the Elliott School of International Affairs.

www.ipdgc.gwu.edu

TABLE OF CONTENTS

EXECUTIVE SUMMARY

This study analyzed coverage of cyber-related issues in the *New York Times, Washington Post, Wall Street Journal,* CBS Evening News, and early evening news shows on CNN and FOX News Channel. It covered the period from July 2020 through the end of March 2023. The major findings from this analysis are:

- **Overall trend:** The previous three reports showed a steady increase in coverage of cyber issues beginning in 2015, with a spike in coverage in 2019. In the latest period, overall coverage of these topics returned to similar levels and trends as before 2019 though at a slightly higher level than before that and with another surge in 2022.

- **Cyber is still often a hacking and cybersecurity story, but crypto and cyber warfare became more prominent topics in 2020-2023:** Looking at "main subject," these were among the most commonly covered aspects of cyber in mainstream news. Overall, though, we see a remarkable amount of consistency in the topics that have dominated coverage since 2014.

- **Newspapers continued to focus on the technology industry during this period, though slightly less than in the previous period studied.** Stories about the business side of the tech industry, issues related to user privacy, and reporting on technological innovations represented about a third of overall print stories about cyber issues, slightly less than the nearly 4 out of 10 in the 2019-2020 period, but still a dramatic increase over the share of stories about these topics in the 2014-2019 era.

- **Most stories about cyber issues continued to be covered substantively and more in depth from 2020-2023, continuing a pattern seen since 2017.** The majority of stories about cyber issues were framed *thematically* or *substantively* (e.g., what this means and what can be done about it), as opposed to *episodically* (i.e., more event-driven and superficial). Stories during this period were slightly less likely to be substantively framed in this period than they were in 2019-2020, but still far more than in 2014-2017.

- **Cyber continued to be a largely U.S.-centric story, though slightly less so than in the 2019-2020 period.** Since 2014, with the exception of the 2017-2018 period, at least three-quarters of cyber-related stories in U.S. mainstream media were focused on America, and even in those outlier years about 65 percent were. From mid-2020 through the first quarter of 2023 about 70 percent of cyber stories were U.S.-centric, about ten percent less than we found in the 2019-2020 years.

- **Tech companies remained the most common "villain" in cyber stories.** As in the previous report, cyber stories that had a negative angle tended to focus on technology companies in some way as the antagonist, often because the stories were about privacy issues. In previous reports, the "villains" in negative stories were usually America's strategic rivals, especially Russia and China, or hackers. The U.S. government itself also showed up as one of the most common bad actors, reflecting the dominance of stories about government surveillance.

- **Experts and corporate officials still control the Cyber Megaphone.** As in previous reports, cyber experts and advocates were the most likely to be quoted, though in this period citizens had more of a voice and Members of Congress had less say than in the previous study.

Covering Cyber

INTRODUCTION

This report represents the fourth and final in a series dating back to 2014 analyzing mainstream American media coverage of cyber-related issues. It covers the period from July 1, 2020 through March 31, 2023. As with the previous reports, there are consistencies in coverage over this now nearly decade of research, but also important differences in how the press confronted myriad cyber topics in the current period. It is clear from this study and the ones that preceded it that cyber has increasingly become a central part of public life, public policy, and national security, and there is virtually no area of news that isn't touched by it in some way. Media have responded to this evolution by covering the issue more substantively in recent years than in the first few years examined as part of this project. The overall story, then, is a positive one regarding press coverage even as the story of cyber's influence and reach has increasingly become more worrisome in many ways.

This report analyzed coverage in the *New York Times, Washington Post,* and *Wall Street Journal* on the print side, and on the broadcast side, the CBS Evening News and CNN and Fox News Channel's early evening news programs. Decades of research has shown that the three network newscasts (i.e., ABC, CBS, and NBC) do not differ significantly in their news agendas or framing, so choosing one of the three was seen as sufficient. CNN and FNC have well-established differences in their approach to news and represent different audience constituencies. Finally, we chose the early evening newscasts on CNN and FNC, which looked at the major news of that day, because they were the closest in terms of mission and time of day to network evening newscasts.

Like the earlier studies, this report analyzed critical variables such as: the main topics covered, their frames, what sources were quoted, and, where relevant, who the "villains" were in cyber stories. These tell us not only what aspects of the broad topic of "cyber" made the mainstream news agenda, but at least as importantly the way in which they were discussed and who had access to that framing. At the same time, this report, like the two that preceded it, tell us the story of cyber by showing us what *isn't* covered and who *doesn't* get to tell the cyber story in the news.

This period of review began during the Covid pandemic, the end of one of the most tumultuous presidencies in U.S. history, and the Capitol insurrection on January 6, 2021. It ended with Covid contained but still present, a potential rematch of the 2020 election, continued threats to the democratic process from conspiracy theorists in and out of electoral politics, and concerns about AI's potentially pernicious influence on society looming on the horizon. In between, new social media platforms have become dominant and controversial (TikTok), while "older" ones have become even more controversial shells of their former selves (Twitter). Some governments still engage in online misinformation and disinformation campaigns (e.g., Russia), while others struggle to balance combatting these cyber threats with protecting individual rights to privacy (e.g., the U.S.). Cryptocurrency had a spectacular rise and seeming fall during this period, first as part of a 21st Century Gold Rush and now a story mostly of disgraced and indicted former captains of industry and tainted celebrity spokespeople. The story of cyber is still evolving and being written, and this report chronicles the way mainstream American news organizations have told it.

FINDINGS

Cyber-related issues remained an important focus of news stories in the 2020-2023 period studied for this report. Overall, the print and broadcast news organizations analyzed here spent even more time on these topics than they did in the first few years of this project, with a spike in coverage during 2022 that didn't quite match that of 2019 but still showed the ways in which technology stories occupy a central role in 21st Century century affairs (Figure 1).

In many ways the story here is the same as it's been since 2014: As technology permeates every aspect of society, policy, and business, it simultaneously bleeds into all areas of reporting beyond just specialized beats and one-off general assignment stories. In the previous report, for instance, Facebook itself and its often-controversial founder and CEO Mark Zuckerberg became stories themselves, often involving questions about inappropriate data collection, monopolistic business practices, and the platform's role in spreading mis- and disinformation about politics and the pandemic, among other things. This cycle, in the period from mid-2020 through the first quarter of 2023, this kind of story persisted, albeit with Elon Musk and his companies, especially his fraught purchase of Twitter, replacing Zuckerberg and what is now known as Meta. Although the central character may have changed, the nature of the stories about him and his companies remain similar in nature to those that have dominated cyber coverage since 2014. Reporters, audiences, and policymakers are still interested in the implications for protecting individual privacy, promoting fair business practices, protecting democracy and the free flow of ideas, and how to protect society from the ills of misinformation and cyber-attacks.

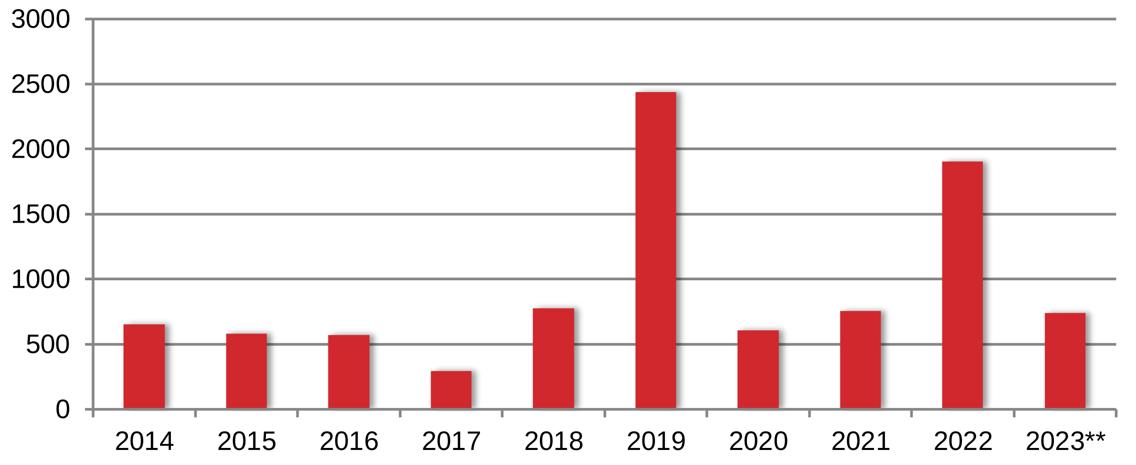
This has led policymakers to continue to become more central to the cyber story. Questions about how to balance a free market with a healthy marketplace of ideas, and what role government, industry, and citizens themselves play in that dynamic, are increasingly the focus of Congress and the White House, as well as advocates of all stripes.

In addition, cyber continues to become an increasingly important area of geostrategic policy and even warfare. When this project began a decade ago, Edward Snowden and Wikileaks were central storylines about whether the U.S. government was exceeding its authority in trying to combat international terrorism and nation-state conflict. Russia and China were often portrayed as using cyber to meddle in American affairs and spread misinformation. All these issues remain, but more so. Russian meddling in the 2016 and 2020 U.S. elections mirrors its pernicious activities globally, and one of the most covered stories in this latest period was the spy balloon China sent over U.S. soil.

No discussion of the most recent period of coverage would be complete if it ignored concerns about AI. In many ways these stories only began to permeate coverage toward the end of our analysis period, but it's clear to even the most casual observer that this is the topic *du jour* across many domains going into the rest of the 2020s and perhaps beyond. Questions from the relatively mundane – how can teachers stop students from using ChatGPT to write their papers and what impact will the technology have on learning? – to the existential – will AI literally be the end of mankind? – are the latest wave of techno deterministic philosophizing and hand-wringing that have accompanied the invention of every new technology in at least the last 150 years. We are still in the infancy of these concerns, and news coverage of them during the mid-2020 to early 2023 period only started to reflect that.

In our last report, in 2021, we wrote, "Clearly (or at least, hopefully), 2020 will be an outlier, and the world will return to 'normal' in coming years. Should this happen, we would expect to see a return to the earlier trend of cyber stories occupying an increasingly central place on the mainstream news agenda." In many ways, that is exactly what this report finds, albeit with a trend line in overall coverage sloping upward as news organizations continued their pattern of integrating cyber stories more and more into their coverage.

Figure 1: Total Cyber-Related Stories Coded By Year, Print & Broadcast News*



* Figure 1 shows coverage at the most prominent news organizations that have been included in these reports since 2014.

**2023 totals are a projection for the year based on the trend of stories coded in the first quarter of the year.

Cyber stories also continued to be overwhelmingly U.S.-centric, as we've found in earlier reports. About 70 percent of these stories from mid-2020 through the first quarter of 2023 were centered largely or entirely around the United States, down about 10 points from the high in the

2019- mid-2020 period, but roughly in line with earlier years when no more than 35 percent of stories were mostly concerned with other countries or regions. This is interesting given that cyber issues and topics are in many ways borderless. It also neglects the fact that virtually every country, as well as international bodies and alliances such as the European Union and the G7, is wrestling with cyber issues. This is yet another example of the well-established ethnocentric bias of American news media, as numerous studies have demonstrated over the decades.

What Gets Covered?

We also see some consistency in the topics of cyber stories most covered in the news in the latest period, although like earlier reports, we also see new areas of focus rise to the fore. Tables 1-4 show the most common topics covered in cyber stories since 2014. Hacking and cyber security, especially related to the U.S. government's efforts to protect itself from cyber-attacks, have been mainstays of major media cyber coverage during the last decade. In addition, many stories, especially in print news, focus on the technology industry itself, whether it's new products, platforms, and innovations, or questions about data mining, privacy, and policy responses to these and other related issues.

The news in 2020-2023, however, saw two stories that had been largely absent from coverage in past years gain prominence: cryptocurrency and cyberwarfare. In the case of the former, stories mostly revolved around either the rise and fall of these currencies across trading marketplaces and the fortunes won and lost in the process; or they involved the scandals surrounding nefarious crypto schemes and entrepreneurs such as Sam Bankman-Fried. Studies of news have long shown that mainstream media tend to gravitate toward stories about scandal and about individuals, and the crypto story during this period often involved both.

Cyberwarfare stories also saw prominence in this period, many about the spy blimp China sent over U.S. airspace, which the Biden Administration soon had shot down. In part this story got a lot of traction because it played into a familiar partisan battle, as Republicans used the blimp as a cudgel with which to attack the White House as being both soft on military preparedness generally and on China specifically. News has always been attracted to these partisan political stories, devoted as it is to a norm of "he said-she said" two-sided reporting frames, but also because of its Fourth Estate responsibility to reflect political debates back to audiences. In the end, it's not clear that the balloon represented much of a threat, and certainly not a new one (reporting showed examples of similar espionage efforts during the Trump administration, for example), but stories about it spilled over into several different news beats and lasted for a few weeks.

In many ways, cyberwarfare has always been present as a topic of concern in media coverage – and policy interest – in the last decade. After all, government surveillance and many hacking stories revolve around various efforts by nation states and terrorist organizations to use technology to attack adversaries, or countries to protect themselves against these attacks. Indeed, the U.S. and other governments have created new agencies and institutional apparatuses to address cyber threats, such as the U.S. Cyber Command, one of the eleven unified combatant commands of the U.S. Department of Defense, created in 2010. It is likely that these stories will only grow in prominence in the coming years.

An interesting development in the current period under study was the relative decline in the proportion of cyber stories about law, policy, and legislation. Whereas in the last report, covering 2019 and the first half of 2020, these stories were the fifth most common type of cyber-related story in newspapers, between mid-2020 and early 2023 they were only the tenth most covered, dropping to about 5 percent of cyber stories from about 10.5 percent in the earlier period. This is interesting given how much more cyber issues have created an opening for, or one might think a demand for, legislative attention. The explanation for this decline is not, it seems, because Congress (and other legislatures or similar international bodies) have not been attentive to cyber issues. Rather, it is probably a function of the increasing diversity of cyber stories and their centrality to myriad issue domains. In other words, there are simply more stories about cyber in some form or another (see Figure 1). It also may be a function of high-profile stories that involved Congress, especially, in the past period, from Facebook whistleblower testimony to mis- and disinformation and cyber conspiracy theories being significant storylines in the unprecedented two impeachments of former President Trump. Although some of these stories overlap with the current period of study, as mentioned earlier this era represents a kind of return to normal in cyber coverage. Still, that normal does, it should be emphasized, include a greater attention to law, legislation, and policy than we saw in the pre-2019 coverage.

Table 1: Most Common Main Subject in Cyber Stories, Print and Broadcast News, 2020-2023

Newspaper Main Topics	**Broadcaster Main Topics**
Cryptocurrency (18.3%)	Cyber Attack/Hacking (15.6%)
Business (14.6%)	Govt. Cyber Security (11.8%)
Cyber Attack/Hacking (11.1%)	Cyber Warfare (7%)
Technology (9.2%)	Business (7%)
Govt. Cyber Security (8.2%)	Technology (6.2%)
Surveillance (7.1%)	Internet Governance (4.3%)
Business Cyber Security (6.2%)	Business Cyber Security (3.4%)
Cyber Warfare (5.7%)	Cryptocurrency (2.6%)
Privacy Issues vs. Tech (5.2%)	Surveillance (2.6%)
Legislation/Policy (5.1%)	Misinformation/Disinformation (2.6%)

Table 2: Most Common Main Subject in Cyber Stories, Print and Broadcast News, 2019-2020

Newspaper Main Topics	Broadcaster Main Topics
Business (14.9%)	Cyber Attack/Hacking (22.6%)
Technology (12.8%)	Surveillance (19.4%)
Privacy Issues vs. Tech (12.5%)	Privacy Issues vs. Tech (14.5%)
Cyber Attack/Hacking (10.8%)	Govt. Cyber Security (11.3%)
Legislation/Policy (10.6%)	Cyberwarfare (11.3%)

Table 3: Most Common Main Subject in Cyber Stories, Print and Broadcast News, 2017-2018

Newspaper Main Topics	Broadcaster Main Topics
Cyber Attack/Hacking (23%)	Cyber Attack/Hacking (33%)
Government Cyber Security (19%)	Government Cyber Security (16%)
Consumer/Citizen Cyber Security (9%)	Consumer/Citizen Cyber Security (9%)
Government Surveillance (7%)	Tech Industry Cyber Security (8%)
Tech Industry Cyber Security (7%)	Politics/Campaign (6%)

Table 4: Most Common Main Subject in Cyber Stories, Print and Broadcast News, 2014-2017

Newspaper Main Topics	Broadcaster Main Topics
Cyber Attack/Hacking	Cyber Attack/Hacking
Government Surveillance	Government Cyber Security
Tech Industry Cyber Security	Politics/Campaign
Government Cyber Security	Tech Industry Cyber Security
Consumer/Citizen Cyber Security	Consumer/Citizen Cyber Security/ Government Surveillance

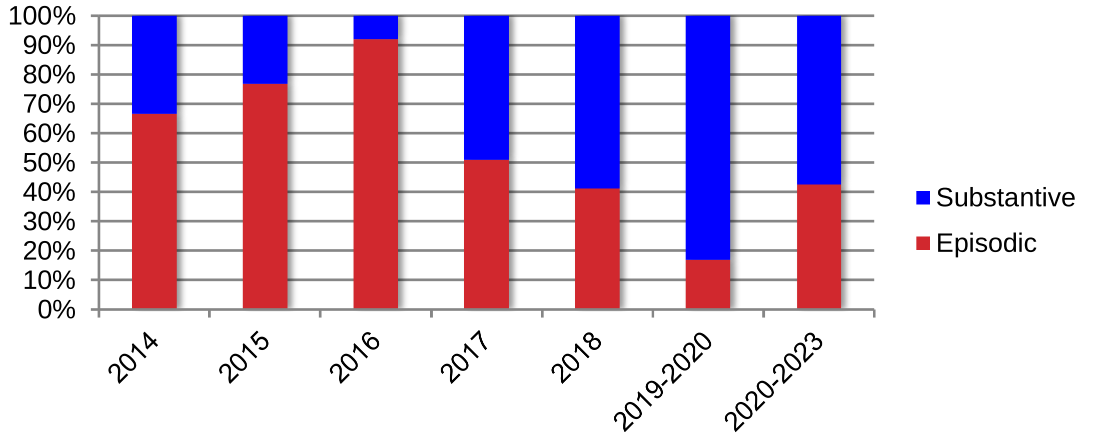
More Substantive Coverage of Cyber

Another way in which media coverage of cyber issues changed dramatically beginning around 2017 involved the level of attention news organizations gave these stories. In the earlier years studied, coverage tended to be more superficial and episodic, describing rather than explaining or otherwise going more in depth. This is consistent with how research has shown news media tend to cover most issues, where being "the first draft of history" tends to create a bias toward event-driven news – e.g., "A hack occurred," "The White House announced….," "Apple reported…." – than what academics refer to as "thematic" news, which looks more at an issue's complexities, ramifications, and root causes and possible solutions.

As Figure 2 shows, beginning in 2017 coverage for the first time became balanced between episodic and substantive coverage. In 2018, when we also see the beginning of the trend toward more overall coverage of cyber issues that has continued to this day (Figure 1), most cyber stories were thematic in nature. This has continued to be the case each year since, and although the peak during the current project occurred in the 2019-2020 period, from mid-2020 through early 2023 nearly 6 out of 10 cyber stories were substantively covered.

Some of this might be because the kinds of cyber stories that are dominating coverage the past few years have been complex and nuanced. It's difficult to imagine a story about the trade-offs between government surveillance and personal privacy, or one exploring the range of Russian efforts to spread misinformation online and their potential impact, that is superficial. Another explanation may be that many of these stories fall into established prestigious news beats, such as the national security beat, or specialized beats, such as technology. These beats tend to be staffed by more seasoned reporters, and those reporters tend to develop an expertise in the topics that allow them to explore issues in depth. Many cyber stories don't lend themselves to being assigned to general assignment reporters, who research shows are typically less expert on a given topic and who tend to write more episodic and event-driven stories.

Figure 2: Episodic vs. Substantive Coverage, Print and Broadcast News



This matters. Academic studies show that when audiences see a steady diet of episodic stories, they tend to think problems and solutions lie with individuals, and are less likely to see the broader societal implications and responsibilities in dealing with issues and problems. When they see more thematic, substantive stories about an issue, however, they are more likely to understand the role of society and institutions in general, especially government, in thinking about causes and solutions. Put another way, more substantive coverage is likely to help news audiences understand what an issue is, what it means, and why it matters. This can also have profound implications for government accountability, as citizens can be empowered by what they learn in the media to question policies and demand official action. At a minimum, it should lead to a more informed audience than an overwhelming bias toward superficial stories would create.

Who Speaks about Cyber?

Past reports in this series have found that, for the most part, the sources journalists seek out to tell the cyber story are the same kinds people decades of research have shown reporters favor in virtually all types of coverage: elites, especially government officials, credentialed experts, and advocates for special causes and interest groups. Sociological studies find that journalists, with deadlines always looming, try and find the most efficient ways to report the news and this typically leads them to return repeatedly to a steady “Rolodex” of established, and establishment, sources.

This pattern didn’t really change much from mid-2020 to early 2023. Government and technology company officials joined subject experts and issue advocates in the top tier of quoted sources in cyber stories, just as they have every year since we began studying the topic in 2014 (Table 5). As with the 2019-mid-2020 period, though, citizens cracked the top five of quoted sources, coming in third ahead of executive branch sources. A qualitative review of stories with citizen quotes reveals that while many of them came in stories about technology itself (e.g., reactions to new products), reporters also seemed to be seeking out citizen opinions on issues that became more salient in the last few years, especially cryptocurrency and conspiracy theories/misinformation. Meanwhile, Members of Congress dropped to fifth at just over 6 percent of total quotes, and, as we found in the last report, the President himself was largely silent in cyber-related stories.

Table 5: Most Frequently Quoted Sources, All Stories 2020-2023

Source	Percentage of Total Quotes
Expert/Advocate	28%
Corporate Official	26.7%
Citizen	10.3%
Executive Agency Official	9.3%
Member of Congress	6%

Cyber Villains

Reporters rely on sources to tell news stories, and those stories also often have character-driven narratives. In part because of a well-established negativity bias in news, one of the more common characters in news narratives is the “villain.” Cyber stories are no different, especially when one considers the kinds of stories that dominate this coverage, such as hacking, surveillance and privacy issues, and scandals ranging from crypto scams to government-sponsored disinformation campaigns.

Past reports in this series have found that the villains in cyber stories tend to not only reflect these dominant storylines, but also in many ways U.S. policy and strategic interests. Russia and China have been among the most common bad actors in cyber stories in every year analyzed, reflecting their various attempts at online mis- and disinformation, cyber-attacks, and espionage. The U.S. government itself has also been a common antagonist in cyber stories, mostly in those where questions are being raised about the propriety of its surveillance of American citizens. In the last report, covering 2019 through mid-2020, technology companies themselves became one of the most common villains in cyber stories, reflecting concerns about the industry's invasive data collection tactics, product issues, and the controversial actions and attitudes of some of its most notable officials.

The latest period studied mostly showed continuity with the last report in terms of who got cast as cyber villains. Technology companies and their officials were the most common, at around 10 percent, followed by Russia, hackers, China, and the U.S. government. American media, probably reflecting the concerns of its audience members, appears to be beyond any cyber utopian phase that might have accompanied the early stages of the digital revolution, and are now adopting a much more skeptical stance toward the industry. Although AI only started to get covered with any momentum at the very end of this current analysis, concerns raised about it in the common discourse seem likely to continue this trend in coming years.

Table 6: "Villains," All Stories 2020-2023

Villain	Percentage of Total Villains
Corporations/Tech Companies	9.4%
Russia	7.4%
Hackers	6.6%
China	4.9%
USA	2.3%

CONCLUSIONS

When this project began nearly a decade ago, the internet as a mass medium was only about 20 years old. Cyber technology as a daily presence in people's lives was still relatively novel, even if in many ways it already seemed ubiquitous. The world in 2014 had recently witnessed revolutionary moments in the Arab world that seemed for a moment to confirm the most cyber utopian views of technology's power to be a force for democracy and freedom, and yet had also watched as those dreams were already being tempered by those same societies descending into civil wars and authoritarianism. Cyber had already been shown to be a dangerous tool for waging hot and cold wars, while the way governments responded to these threats had already been exposed as invading the privacy of citizens and forcing a national conversation about when the ends justify the means. Even the new digital toys and sources of unlimited information, our phones, were being seen simultaneously as both indispensable tools for productivity and enjoyment, as well as potentially dangerous distractions that risked accentuating alienation, abuse, and societal atrophy.

Since 2014, the reports produced in this series analyzing mainstream U.S. media coverage of cyber issues have revealed the many ways technology has evolved and become even more central to peoples' daily lives and the policy and strategic priorities of governments. Part of that story is in some ways how *little* has changed. Hacking, surveillance, privacy, and the tech industry itself have dominated coverage every year between 2014 and early 2023. Elites, especially government and industry officials, cyber experts, and digital activists of various stripes have remained the people reporters seek out to tell the cyber story. Those stories are often framed negatively or skeptically, as many news stories about most topics are, and when that happens governments themselves – especially the United States, Russia, and China, though for different reasons – have been among the most commonly cast villains. In many ways, then, the story about cyber told in these reports has been that the more things have changed, the more they have stayed the same.

Yet there have been important changes in how news about cyber has been covered that mirror the evolution of technology's role in society over this time. Most significantly, news went from being mostly episodic and event-driven in the first years of this project to being predominantly substantive since 2017. This means news audiences are more likely to get news that explains the complexity and nuance of cyber-related issues, reported by mainly beat reporters who themselves are quasi-experts on the topic. It is important to reiterate that this is atypical for news, which research shows covers most issues more superficially.

Since 2014, we've also seen an overall rise in the salience of cyber stories to news organizations, which are devoting progressively more coverage to these topics in the last few years. No doubt, this reflects both the importance of cyber issues to governments and the public, as well as the ever-growing diversity of subject areas touched by technology. Put simply, there are just more stories to cover about cyber in 2023 than there were in 2014.

Those stories are of critical importance, as well. Since this project began, America and other countries have seen the core pillar of democracy, fair and free elections, corrupted by online mis- and disinformation campaigns, conspiracy theories, and illegal attempts to subvert the vote. These nefarious efforts have been spearheaded by foreign governments (especially Russia), terrorist groups, domestic political parties and partisans, and others. Scholars and national security officials and experts have shown that the goal of many of these efforts is to break down the basic trust citizens have in not only their political and societal institutions, but the very notion of information and truth itself. This has been an era in which we've seen White House officials claim to reporters that there is such a thing as "alternative facts," and conspiracy theories have spawned hate and violence, including the January 6th Capitol insurrection in 2021.

Given the stakes raised by cyber stories, and the pervasiveness of technology in our lives, mainstream media's responsibility in covering these stories has never been more profound and is only likely to become more so in the coming years. So far, cyber is the rare topic in the United States that has mostly avoided being sucked into the polarization vortex that has defined 21st Century American politics. This is somewhat ironic given that many assume (though scholarly research is more skeptical) that social media exacerbate partisan polarization. But at the policy and national security level, at least, there still seems room to talk across the aisle about many cyber issues. That has no doubt played a part in the media's willingness to cover these issues substantively, as they are not as likely to fall into established patterns of he said-she said partisan storytelling.

The cyber story continues to evolve, and like all technologies it does so in ways that are potentially a boon to society but also maybe a peril. Even AI is a topic that can't be pigeonholed as good or bad. ChatGPT and its ilk, for instance, can be great tools for efficiency in many areas of life. Yet we are already seeing examples of how the technology's effects and influence can be pernicious, from plagiarism, to replacing writers in Hollywood and other fields, to spreading misinformation. AI can no doubt improve business efficiency and the global economy in many ways, but will it also create massive unemployment or other financial and societal disruptions? Will it help solve the greatest threat to humankind, climate change, or will it exacerbate these challenges? The cryptocurrency stories that were so prominent in the latest analysis in this report, for instance, involved exactly these questions, as crypto advocates saw it as a way to create wealth and even democratize global finance, yet crypto mining also created environmental challenges.

It will be interesting to see how media coverage evolves alongside cyber issues. So far, the story has been largely positive. Reporters are covering the story more substantively than before, news organizations are devoting more space to telling cyber stories across an ever-widening array of topic areas, and citizen voices seem to be more prominent alongside elites, experts, and advocates. Perhaps most critically, the media at this stage seem to be covering cyber in a way that can help create more government accountability and responsiveness to public concerns and freedoms.

APPENDIX 1: METHODOLOGY

The main thrust of this study involved an analysis of the *New York Times, Washington Post, Wall Street Journal,* CBS Evening News, and the early evening newscasts on CNN and Fox News Channel from July 1, 2020 through March 31, 2023. Newspapers were selected based on their well-established prominence within the industry, tendency to set the agenda for other media, and findings in previous studies that regional papers did not cover cyber much at all, and when they did it was usually through the reporting of these news organizations or wire services. Because for each of the years studied the number of stories about cyber-related topics went into the low five figures, it was impossible to conduct a census of all stories and thus we sampled every third article retrieved for each news organization from databases such as Lexis-Nexis and ProQuest, and from Google searches.

Before coding began, a team of graduate student coders was trained to understand the variables of interest based on detailed coding guidelines devised by the Principal Investigator (available upon request). Coders then practiced on a set of stories not included in the sample that would ultimately be used for the study, in order to establish acceptable levels of inter-coder reliability before actual coding began. Once all coders reached acceptable levels of inter-coder reliability, the team began coding the articles in the sample drawn for the study.