COVERING CYBER

Media Coverage of Cyber Issues Since 2014

Sean Aday

Institute for Public Diplomacy and Global Communication

George Washington University

COVERING CYBER

MEDIA COVERAGE OF CYBER ISSUES SINCE 2014

ABOUT THE REPORT

This report analyzes media coverage of cyber issues in major American newspapers and network and cable news broadcasts since 2014 to assess how these issues are being framed in the press, and what aspects of this complex topic are reaching news audiences. In addition, specialty online media are analyzed in comparison to traditional media coverage.

The report shows that cyber is becoming more prominent on the news agenda in the U.S., but that it is simultaneously receiving less substantive coverage. Cyber is thus more likely to be covered as an event than as policy. The report discusses implications of these and other findings.

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 primarily analyzed coverage of cyber related issues in 20 of the highest circulation newspapers in the United States, as well as that on all three network newscasts and CNN and Fox News Channel, from January 2014-June 2017. The major findings from this analysis are:

- **Overall trend:** Although total coverage is fairly constant in 2014 and 2015, there was approximately a 27 percent increase from 2015 to 2016, and coverage through the first six months of 2017 had already nearly matched the amount of the preceding year, spurred in large part by stories about possible Russian involvement in the 2016 Presidential election.

- **Despite more attention to them, cyber stories were not prominently featured in the news.** Cyber stories rarely ran on A1 or led newscasts.

- **Cyber is primarily a hacking and cyber security story:** Looking at "main subject," these were the most common types of stories all three years.

- **Cyber security became more of an issue during this time.** Stories about cyber security issues related to the government jumped from 4.5 percent in 2014, to 12.8 percent in 2016.

- **In 2016, cyber increasingly became a political story.** In 2016, there was a surge in politically related cyber stories, as the issue became more relevant to the presidential campaign.

- **Yet despite the rise of *political* cyber stories in 2016, the issue is less often talked about in terms of *policy*.** For example, stories were increasingly more likely to be framed *episodically* (a hack happened, for example) as opposed to *thematically* or *substantively* (what this means and what can be done about it): 66.7 percent of stories were episodic in 2014, and that number soared to 93.9 percent in 2016. That said, newspaper coverage during the first half of 2017 became more substantively framed (though television coverage did not).

- **This is important because research shows that how stories are framed can influence who audiences think is responsible for addressing issues and problems:** Event driven, episodic frames, for instance, tend to lead people to see problems and solutions from an individual perspective (e.g., blaming crime on "bad seeds"), and to be less likely to see a role for government, institutions, or society in solving problems. Thematically framed stories often have the opposite effect.

- **The relatively few thematically framed stories from 2014-2016 tended to be in depth discussions about how to protect oneself against cyber crimes, especially hacking, not governmental or private sector policies.**

- **Cyber is a U.S.-centric issue in American media**. Stories rarely discussed the global ramifications of cyber issues. Instead, about three-quarters of print stories focused on the United States, while between 88 and 97 percent of those on TV did.

- **"Villains" in cyber stories are typically hackers, though also frequently governments, including the United States.** "Hackers" were the villain in 38-45 percent of the stories that had a villain between 2014 and 2016. In fact, "Hack" or some version of the word was one of the most common cyber-related words to appear in leads, and stories about hacking and hackers were common in page A1 stories about cyber issues.

  - The U.S. (in 2014), China (in 2015), and Russia (in 2016 and 2017) traded off being the countries most likely to be villains, showing up in about 20-25 percent of stories that had villains. Interestingly, in stories about the Snowden affair, the U.S. government was commonly framed as the villain.
  - Despite many stories about cyber security issues in the tech industry, corporations only show up in about 7-10 percent of the stories as villains.

- **Another way to think about this is that villains are far more likely to be "hackers" than tech giants potentially invading customers' privacy**. For example, government-related privacy issues were commonly found in tech blogs inside the paper rather than on page A1.

- **Who speaks? The tech industry and the U.S. government.** Looking at all direct quotes, tech security experts, corporate officials, and especially U.S. government officials dominated the conversation about cyber issues.

- **Who isn't heard?** By contrast, privacy experts, citizens, and international experts were rarely quoted, reflecting both the episodic nature of most stories and the greater focus on cyber crime and hacking rather than potential concerns with the industry or government *vis a vis* customers and the public.

- **Cyber is a national media story.** We found very little print coverage of this issue in the mainstream media outside of the big national papers.

- **Online specialty media tend to cover cyber issues far more substantively than mainstream news.** Untethered to a need for immediacy, and produced by specialists for a selective audience, digital media such as *Verge* and *Ars Technica* are able to go into far more depth on these issues than daily news organizations are capable or willing to do.

INTRODUCTION

In the spring of 2007, Estonia decided it wanted to relocate a monument to Soviet forces in WWII prominently located in the capital city of Tallinn. The Russian government issued a stern warning to the Estonians that such a decision would result in serious retribution. On the belief that being a sovereign nation meant being able to at least make seemingly banal decisions about statuary, the Estonians went ahead with the removal. Suddenly, on April 27th, citizens of the small Baltic state began noticing that websites weren't loading, and that in fact the entire internet seemed to be shutting down. Things worsened at midnight on May 9th, VE Day in Russia and the occasion for a major celebration of national pride in a country that lost an estimated 20 million in the Second World War. The coincidental timing was not lost on the Estonians.[1]

More than ten years later most observers mark the incident, which virtually everyone attributes to the Russians despite their official denials, as the first in a growing number of politically motivated cyber attacks. In fact, the Estonian case was the first time the *New York Times* used the term "cyber war" to describe an attack.[2] Many of these attacks, including the suspected hack of the Democratic National Committee during the 2016 U.S. presidential election, are presumed to have been conducted by the Russians, but other countries have been accused of similar attacks, including the Chinese and the United States itself.

Add to these incidents major hacks of consumer databases such as Equifax and Yahoo!, and controversial cases of government surveillance of American citizens revealed in the Wikileaks and Edward Snowden cases, and one starts to get a sense of the increasing gravity and pervasiveness of cyber related issues. Then of course there's the seemingly more pedestrian and even positive ways in which technology is making many people's lives easier and even more fun, from IPhones to new ways of staying in touch and informed through social media. Yet even these have been shown to have potentially pernicious implications, such as the spread of "Fake News" on Facebook during the 2016 presidential election.

The press may be the most important institution when it comes to contextualizing and making sense of a topic as varied and significant as "cyber." The cyber story, after all, involves several touchstones of journalism: informing the public, holding policymakers accountable, even entertainment. Yet precisely because there isn't a single "cyber story," it is important to ask what stories the media are telling, and how they tell them.

[1] Emily Tamkin (2017). "10 Years After the Landmark Attack on Estonia, Is the World Better Prepared for Cyber Threats?" *Foreign Policy*, April 27, 2017. http://foreignpolicy.com/2017/04/27/10-years-after-the-landmark-attack-on-estonia-is-the-world-better-prepared-for-cyber-threats/

[2] Cyrus Farivar (2009). "A Brief Examination of Media Coverage of Cyberattacks (2007-Present)." In Christian Czosseck, Kenneth Geers, Eds. *The Virtual Battlefield: Perspectives on Cyber War*, Cryptology and Information Security Series, v. 3, pp: 182-188. DOI: 10.3233/978-1-60750-060-5-182

This report takes a comprehensive look at American mainstream media coverage of cyber-related issues from 2014 through the first half of 2017 to understand better what news audiences would have learned about this topic during this eventful period. It does so by sampling about 6,000 stories from 20 of the highest circulation newspapers, all three network newscasts, and the nightly news equivalents on CNN and Fox News Channel, and conducting a detailed content analysis of what topics were covered, how they were framed, what sources were quoted, and, where relevant, who the “villains” in cyber stories were. In addition, we conducted subanalyses of specialty online websites that focus on cyber issues as a point of comparison to the mainstream media.

This report thus represents a baseline of how the press has covered cyber during the years the various aspects of the issue began to take a prominent place on the global, media, and policy stages.

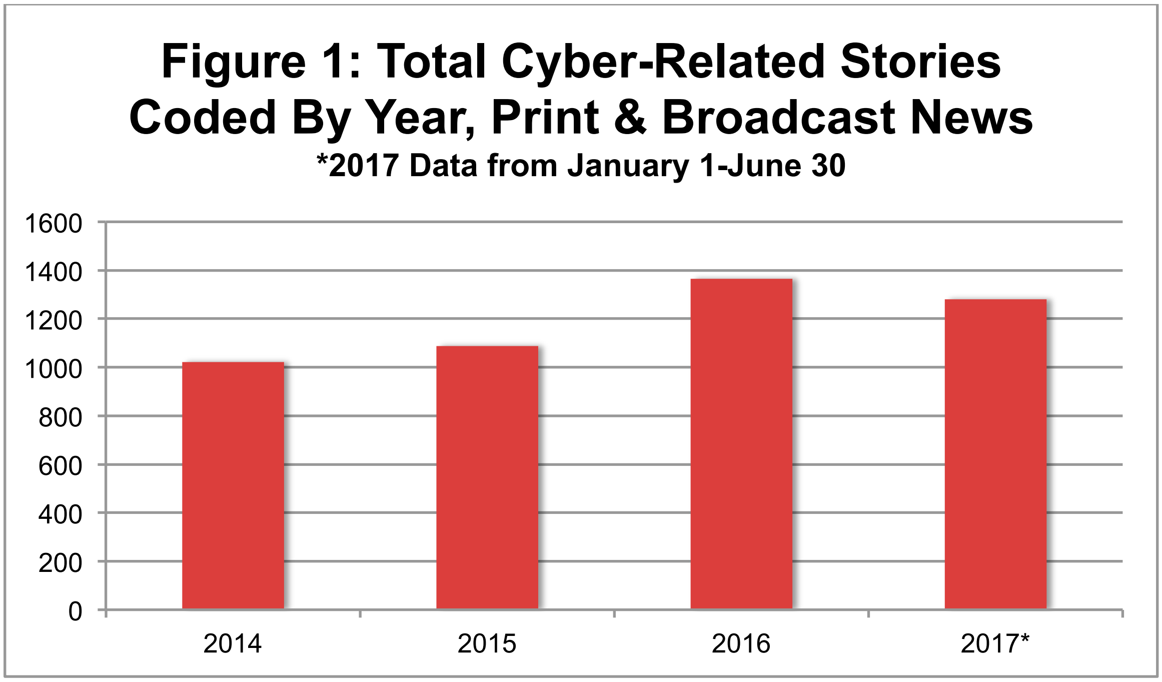
FINDINGS

More Coverage, but Less Substance

As cyber related issues become more central to our lives, so have they begun to receive more media attention. Though total coverage remained relatively consistent from 2014 to 2015, across all media analyzed the number of stories about cyber issues jumped 27 percent in 2016. This reflects not only a greater understanding of the myriad ways in which people’s daily lives intersect with cyber, but also the unprecedented attention paid to it during the historic 2016 presidential election as questions were raised about Russian hacking of the Democrats, Hillary Clinton’s emails (itself a story that ended up overlapping with the Russian hacking storyline), and potential collusion between the campaign of Donald Trump and the Russians. During the first half of 2017, cyber stories already nearly matched the amount of coverage from the year before as these and other storylines continued to dominate the news (Figure 1).

Although media devoted more attention to cyber stories, they didn’t necessarily feature them prominently. Certainly there were major stories accompanied by blaring headlines, but these were not the norm and typically faded quickly into the deeper recesses of the news hole. Only 4.2 percent of cyber stories in newspapers ran on page A1, for instance, and fewer than 2 percent were the lead story on nightly newscasts.

More importantly, when we look closer at *how* cyber stories were covered, the news isn’t entirely positive despite increases over time. Most of this coverage was event-driven and superficial, not substantive. For instance, cyber didn’t show up in election coverage because journalists were analyzing candidates’ policy proposals so much as because of the events described above and the partisan posturing about them. Less attention was paid to how a new administration would address the many aspects of cyber policy, ranging from stimulating innovation, to balancing security and privacy concerns, to countering external cyber threats. Instead, cyber stories during the campaign mostly focused on more superficial he said-she said horse race stories, and how new revelations about Russian hacking, or old ones about Clinton’s emails, might determine the election’s outcome.

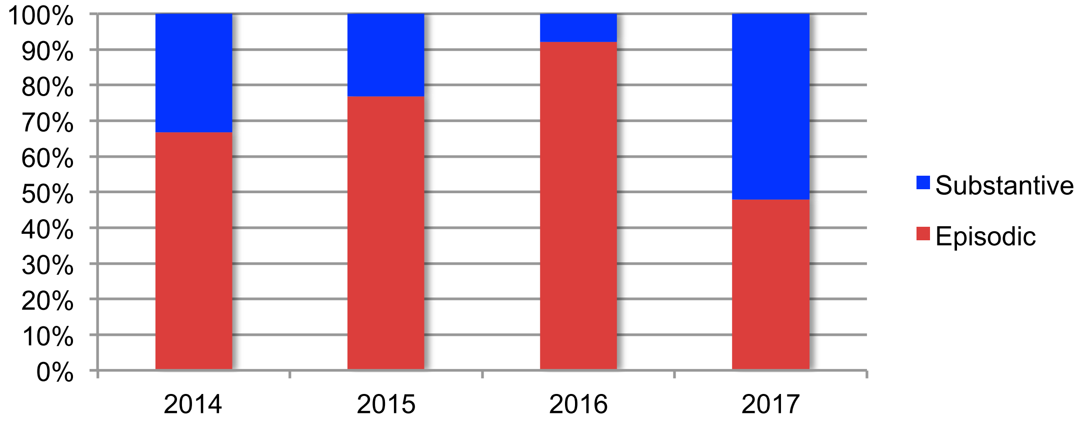


This is a microcosm of perhaps the most important finding of this study: **as a whole, the news media are generally more likely to cover cyber issues superficially, in an episodic, event-driven way, than to discuss them more substantively**. In particular, cyber *policy* stories were rare during most of the period studied. More troubling, the press avoided substantive coverage *more* as time went on. As Figure 2 shows, episodic, event-driven stories increased from about two-thirds of all cyber stories in 2014, to about three-quarters of stories in 2015, and more than 90 percent in 2016. Another way of thinking about this is, as cyber became more important and was covered more, that coverage became less substantive. It is especially disturbing that this was especially the case during an election in which cyber security and cyber threats were a major, and disturbing, part of the story, and when voters could have greatly benefited from a more thoughtful discussion of how the candidates would address those issues.

One note of optimism, however, lies inside the numbers from the first half of 2017. Although broadcast news continued to favor episodic frames for cyber stories more than 90 percent of the time, newspapers reversed course: nearly 60 percent of their cyber coverage employed substantive frames. Given the gravity of many of the major storylines in 2017, this is welcome news.

Still, the preponderance of coverage across all media during the period studied relied heavily on less in-depth coverage. Past research on media coverage of policy, politics, and elections, however, tells us these trends are not unusual. One of the most persistent findings in media and political communication research is that the press generally favors episodic and superficial coverage to more substantive explorations. This is especially true in coverage of contentious politics, such as hotly debated policy issues like health care reform, and election campaigns. (By contrast, media are more likely to discuss the substance of policy proposals, as well as candidates' policy prescriptions, when the issues aren't as volatile and in campaigns that aren't seen as being very competitive.)[3] Clearly there are exceptions to these trends. Some publications, and some reporters, are more inclined to cover issues substantively than others. But generally, this is not the case. Scholars have offered many explanations for why this is so – deadline pressures make episodic stories easier to write; these stories lend themselves to the said-she said journalism that allows reporters to avoid the appearance of taking sides; episodic stories can seem more melodramatic – but the trend is clear and persistent. We find yet another example of it in this study.

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



A fair question to ask is, so what? Why does it matter if coverage is more or less policy-oriented? Certainly, daily journalism – which is, after all, what we studied here – focuses mostly on *what happened* more than *why it happened* and *what it means*, which are perhaps more well-suited to weekend thought pieces, magazines, and niche media. Indeed, in a sub-analysis of technology-oriented digital media, we find that coverage at these outlets became *more substantive* over time, the opposite of what we found in our analysis of mainstream media. To be sure, most coverage even in these publications was episodic, but more thematic stories increased from about 20 percent in 2014 to nearly half (44 percent) in 2016.

There are at least three reasons to be concerned about the trend toward less substantive coverage in mainstream media, however, especially given its wider audience than niche online publications. First, regardless of the news media's understandable emphasis on immediacy, especially in a 24-hour media environment, the fact is that most people still turn to them to not only learn what happened, but also to understand why it matters. What our data show is a media that is increasingly telling its audience that cyber issues are important and even often worrisome, but not providing much context about what can be, should be, or is being done about them.

[3] Cappella and Jamieson (1997). *Spiral of Cynicism: The Press and the Public Good*, Oxford University Press.

Second, media attention to an issue not only makes it more likely that issue will be seen as important to the public, it can force it on the policy agenda, as well. Yet without more substantive discussion of the issue's parameters, and what the proper role for the public and private sectors might be, there is likely to be less pressure on, or incentive for, officials to prioritize them. Similarly, it is less likely that constituents will learn about the efforts of those elected officials who are taking cyber issues seriously. One of the most important roles for media in a large, diverse, and busy society is to be that go-between between representatives and the people, and generally speaking the press could do a better job on this front regarding cyber issues.

Third, research shows that whether the press covers stories from an episodic or more substantive frame can have profound implications for how audiences think of a problem, its solutions, and the role of individuals, institutions, society, and government in addressing those issues. Beginning with pioneering work by Stanford's Shanto Iyengar[4], this research demonstrates that when people read or see a lot of episodically-framed stories about a variety of issues (e.g., crime, terrorism, poverty), they are more likely to think of them as being individual-level problems, and to see less of a role for government, institutions, and society in solving them. By contrast, when audiences are exposed to more thematic or substantive stories, they are more likely to take the opposite view. (These findings hold even after controlling for possible confounding variables like political ideology, gender, race, etc.) This isn't to say there is a right or wrong answer to how to deal with the challenges posed by cyber (or crime, terrorism, or poverty); it is just to say that an imbalance in framing of these issues as we see in our data is likely to have implications for how the public views them and what they expect of policymakers and the tech industry.

This discussion is reinforced by the data regarding what *about* cyber gets the most coverage. **Over the three and a half years we analyzed, a constant was the prevalence of cyber stories that revolved around "hacking" incidents and cyber attacks.** Stories about actual cyber attacks or hacks were the most common main subject in both print (26.7 percent of stories) and broadcast (47.2 percent) cyber stories. The terms "hacking" and "cyber attack" appeared in 40.5 percent of lead paragraphs (defined here as the first paragraph) in print stories, far eclipsing the second most common cyber-related term, "privacy" (17.5 percent of leads). Consistent with our findings regarding episodic coverage, the vast majority of these stories about hacking were about *events*, not substantive discussions of how to prevent hacking, or governmental or private sector policies to prevent hacking and protect consumers.

We also find remarkable consistency between print and broadcast news agendas in their cyber coverage, despite obvious differences in format, audience, and business models. For the most part, the same topics comprised the bulk of coverage in each, as shown by the top five main subjects (Table 1). Various aspects of cyber security dominated the coverage, reflecting the importance of different hacking storylines over the period studied.

[4] Shanto Iyengar (1994). *Is Anyone Responsible? How Television Frames Political Issues*, University of Chicago Press.

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

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

The prominence of each of these storylines varied year to year. As already mentioned, for instance, cyber became more of a political story in 2016 thanks to the presidential campaign. Still, these findings provide an important insight into the underlying news norms that journalists use to determine what makes a story newsworthy. Cyber stories during the period studied were mostly driven by various incidents of hacking, cyber attacks, and surveillance.

We also see a significant increase in stories primarily about cyber *attacks* in the first half of 2017. Whereas these stories had hovered between 20 and 27 percent of total stories between 2014-2016, in 2017 that jumped to 51.4 percent. This reflects the dominance of the Russian election hacking storyline following the 2016 presidential election.

Stories about the technology industry that weren't about cyber security (which again, usually followed some major hacking event and fell off the news agenda soon after) were mostly stories about new technologies such as smart home products, or business-oriented stories about companies in Silicon Valley and elsewhere. Continuing with our theme thus far, very few of these stories were about the proper role of the tech industry in creating a more secure cyber environment that also protects users' privacy, though more of those began appearing following the revelations of "fake news" and disinformation campaigns waged during the 2016 campaign on social media platforms such as Facebook. The vast majority of stories about the technology of cyber in our dataset, however, were more product or business oriented.

The Players in the Cyber Story

Media often rely on narratives to tell their stories, sometimes dramatic ones, and those narratives revolve around a cast of characters. Understanding the patterns in who gets to tell the story about cyber – its experts and villains – is an important way of understanding the overall media frame of this issue and what perspectives are privileged over others. To that end, we coded for which sources journalists selected for their first three direct quotes in a story, a total of more than 3600 quotes for the 2014-2016 period.[5]

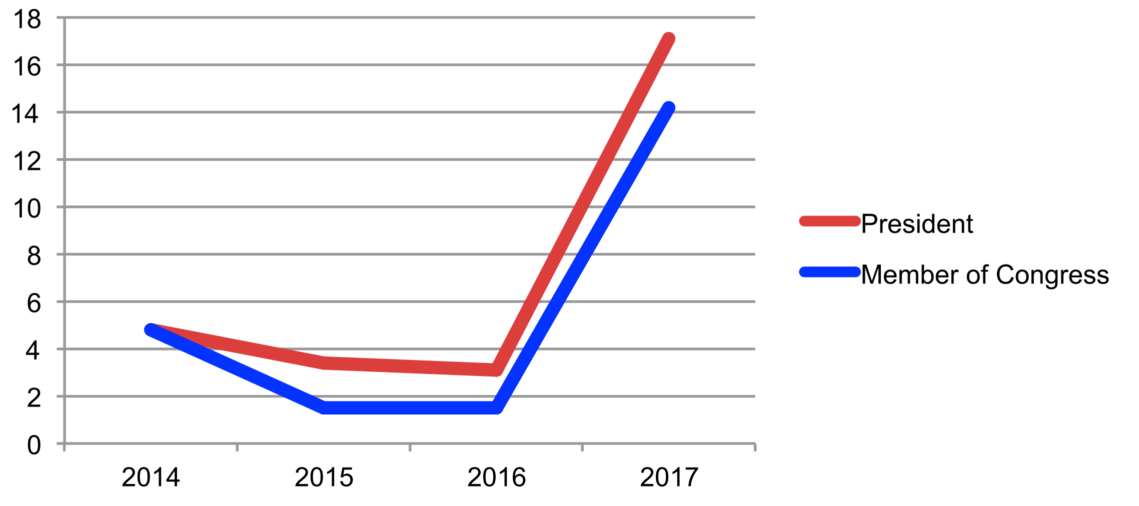
Nearly a quarter (23.6 percent) of sources quoted in cyber stories over this period were government officials, many of those in stories related to the 2016 presidential campaign. This reflects the rise of the issue on the political agenda, and its centrality to the last general

[5] For example, if a story included five direct quotes, we coded for the sources of the first three to appear.

election, though it’s important to note again that this shouldn’t be seen as evidence of a more detailed policy-level discussion in press coverage. Still, studies have long shown that news relies heavily on official, and especially government, sources, and cyber stories were no exception. This implies that should policymakers take the issue more seriously in the coming months and years it is clear they will find a megaphone for their ideas in the press and coverage might become more substantive.

An interesting and related finding regarding sources is that the President and members of Congress were far more likely to be the first person quoted in stories that ran during the first half of 2017 than in previous years (Figure 3). This reflects the dominance of the Trump Campaign-Russia Collusion story, as well as Trump’s revolution in presidential communication through Twitter, which drives a lot of media coverage.

Figure 3: Percent of Total First Quotes from President or Member of Congress



Industry officials were among the most common sources directly quoted in cyber stories, appearing in about half of the quotes across all stories. The most common types of industry sources were corporate security experts (reflecting the emphasis on consumer protection stories) and corporate officials (mainly in business stories, but also in the less common stories about the industry’s roles and responsibilities in addressing cyber-related challenges and concerns), each appearing in nearly a fifth of quotes across our dataset.

Anytime one is trying to understand media coverage, it is not only important to look at what *is* covered, but what is *not* covered, as well. To that end, it is worth noting the kinds of sources we don’t see quoted very often in cyber stories. Notably, these include privacy advocates/experts (8.2 percent of all quotes coded), citizens (2.3 percent), and international experts (0.1 percent). This is particularly telling given that some of the most important and concerning stories over the last four years involve issues of government cyber surveillance, hacking, foreign interference, cyber war and cyber espionage, and massive data breaches that threaten the privacy and security of tens of millions of Americans.[6]

These findings about who is and who isn't quoted raise concerns, but they aren't surprising. Research on media coverage of other issues shows it to be heavily biased toward government officials as opposed to everyday citizens, and to be ethnocentric in its orientation.[7] We see both tendencies reflected in coverage of cyber. Although questions about the proper balance between cyber security and digital privacy have been on the front pages of America's newspapers since at least the original Wikileaks revelations, and accelerated after the Snowden leaks and other investigative reports revealed secret efforts by the U.S. government to gather people's personal information, these stories have mostly been arenas for government officials to argue about the merits of these programs. To be sure, other experts at think tanks and elsewhere appear in some of these stories, but our data show they are drowned out by officials. (That said, it's worth noting those officials are often quoted disagreeing with each other.)

Similarly, despite the global nature of virtually any cyber-related storyline, and especially those that have received some of the most attention (e.g., hacking), our data show that these are stories told largely through an American lens: 77 percent of the stories in our sample focused on the United States. This is important for a number of reasons, not least of which being that it deprives audiences of a more diverse array of experts and perspectives. (We've seen similar patterns in coverage of other issues over the years, most infamously perhaps being investigations into the possible presence of weapons of mass destruction in Iraq.) It also misunderstands a global issue like cyber as a national one.

Although the most important explanation for the U.S.-centric coverage of cyber is undoubtedly the well-documented ethnocentric nature of the mainstream media in America, other contributory explanations expose how changes in the news industry impact coverage of this, and other, issues. For instance, sociologists have long shown that one of the best ways to understand why news looks the way it does is to think of news work in terms of finding the most efficient way of reporting, writing, editing, and producing stories.[8] This means, for example, that the sources that are the most likely to be quoted are going to be the ones that are easiest to find and the most reliable. Government officials usually fit this description.

In the past, however, news organizations had more of an international presence, with bureaus spread across the globe. This made it easier to also find and include international sources for global stories. Since the early 1980s, however, there has been a contraction in the media industry that has led to a dramatic reduction in overseas reporting. The reasons for this

[6] In a coding scheme such as this, where a list of possible outcomes (in this case "sources") is determined *a priori,* there is always a concern about selection bias; i.e., that coders found certain types of sources were quoted and others not solely because they were looking for some and not others. We can be confident that this *wasn't* the case here, however, because we also included an "other" category to capture any sources quoted that weren't included on our list. If we were missing major categories of sources, we would find a significant number of observations coded as "other." We do not: fewer than 0.1 percent of sources quoted were coded as "other."

[7] Lance Bennett (2011). *News: The Politics of Illusion*, Pearson.

[8] Herbert Gans (2004). *Deciding What's News: A Study of CBS Evening News, NBC Nightly News, Newsweek, and Time (25th Anniversary Edition*, Northwestern University Press.

are myriad and more than we have time to explore here, but suffice to say the industry, and especially broadcasters, have increasing lacked the will or the way to cover the world outside America's borders in any substantive way. Hence the even greater reliance on U.S. government and domestic technology industry sources.

Indeed, we see this also in another finding from our dataset: news about cyber issues in American media is almost entirely one covered by *national* media. About 80 percent of print cyber stories in our sample came from papers with a national scope such as the *New York Times, Washington Post, Wall Street Journal,* and *USA Today*.[9] The regional papers in our sample rarely if ever covered these stories on their own, relying mostly on national wire service stories when they covered them at all. This also reflects the changing economics of the news industry, in which many local papers have gone out of business, and those that remain have often attempted to stay afloat by emphasizing a hyper-local approach to reporting, while cutting back on staff and other resources dramatically. This doesn't leave much room for specialized beat reporters covering topics like cyber that may seem too boutique a luxury for struggling newspapers.

Cyber Villains

Many cyber stories also implicitly or explicitly discuss villains, those responsible for hacking and spying, for instance. Sometimes these are stories with complex issues at stake, but which frame one group or entity as to blame for some misdeed. The various stories about Wikileaks or Snowden, for instance, could in theory be framed in a way that makes the leakers seem like villains for releasing classified information that could be potentially damaging to national security; or, alternatively, they could position the government as to blame for invading the privacy of citizens or violating the law. Of course, the stories could take a more balanced approach, but even that is not necessarily preferable. Some on either side of these issues might, for instance, see such efforts at balance as something more like false equivalency.

Our analysis coded for the presence of "villains" in stories, defined as a person or entity that is framed as being responsible for some negative cyber event or outcome. It's important to note that most stories did not have a "villain." This is partly due to the aforementioned finding that most stories were more superficial in nature, but also resulted from the fact that our coding guidelines explicitly stated that in order for an individual, group, or entity (e.g., a country) to be coded as a "villain," the discussion of them as such had to be *substantial*, and had to be specifically about their transgressions *related to cyber*. In other words, a passing reference to "past charges of NSA surveillance," or a discussion of "Russia's crackdown on dissidents," would not be coded as examples of villains because the first is not a substantive discussion, and the second is not necessarily about cyber-related issues.

In stories that did have villains, "hackers" were consistently the most common, assuming that role in 38-45 percent of these stories across the time period studied. This is consistent with our earlier findings regarding the primacy of "hacking" as a storyline. Interestingly, "hackers" is

[9] This argument isn't relevant to our broadcast data since all the channels we analyzed were national in scope.

an expansive term that can be applied to individuals, organized criminal groups, and those working for governments. In our analysis, we coded villains as “hackers” when that word or some variant of it was the term used in the story, and when the story didn’t clearly establish that the hackers were employed by a specific entity such as a government or a company (in which case those would be coded as the villains). So the fact that “hackers” are commonly portrayed as villains shows the individual-level focus of this framing in many cyber stories.

Yet a lot of the major storylines over the last four years, including those about hacking, have involved governments. These range from massive leaks revealing U.S. government surveillance to possible Russian hacking during the 2016 U.S. presidential election. We see this reflected in the other common villains in cyber stories: Nation states. Specifically, the U.S., China, and Russia (in that order) traded off being the countries most likely to be framed as villains in cyber stories from 2014-2017, and Russian continued to be the primary villain during the first half of 2017.

Two points are important to make about this. First, it is interesting that in the Wikileaks and Snowden stories, the government is much more likely to be framed as a villain than the “hackers” (to use the term loosely). Whether this is a fair assessment or not depends on one’s perspective, of course, but it reveals something about the *media* orientation in these stories. There may be several reasons for this, including an inclination of those in the press to be especially sensitive to charges of government domestic spying since similar revelations in the 1960s and 1970s; the fact that in both cases the leakers worked with mainstream media to release the information; and/or other factors.

Second, the fact that the press alternated its focus on the three countries – despite the fact that each appears to have continued to engage in the behavior that caused it to be cast in the villain’s role – shows how media attention can be fleeting. In the case of U.S. surveillance, it is also indicative of the importance of policymakers in keeping issues on the agenda. Despite a few members of Congress continuing to raise alarms, for the most part a bi-partisan consensus generally supporting surveillance tactics has evolved. Studies consistently show that while events and activists can occasionally force an issue on the media agenda, without elites keeping it there, or without vocal elite conflict on the topic, the issue is likely to fade from media, public, and even policymaker attention. We see this phenomenon in our data on U.S. surveillance.

Finally, another interesting nugget in this analysis shows that corporations rarely appear as villains (only about 7-10 percent of the time), despite the high profile concerns expressed by many about privacy issues, and about the role some of these companies may play in abetting the spread of misinformation or even disinformation. Another way to think about this is that according to the press, cyber villains are far more likely to be “hackers” stealing data than tech giants invading customer privacy or giving a platform to “fake news.” This extends to the lack of prominence such stories received, as well. For example, privacy issues were commonly found in tech blogs inside the paper, but less likely to appear on Page A1.

MSM vs. Digital News

We also conducted a sub-analysis of online specialty news sites that focus substantively on cyber issues.[10] Unsurprisingly, the most notable difference between digital and mainstream media is that the former often spend more time, and go into more depth, discussing these topics. As mentioned above, by contrast with the mainstream press, digital media were far more likely to have substantively framed stories and ran far fewer episodic stories, and this became even truer as time went on and the topic rose on the public, press, and policymaker agendas. This reflects the niche, policy-oriented audience of these outlets, and the broader agenda (and audience) of the mainstream press.

That said, in other ways the digital media coverage of cyber resembled what we found in the mainstream press. Like the MSM, digital media were most likely to cover cyber from an American perspective, with between 86 and 93 percent of stories being U.S.-centric. Digital media outlets were also likely to cast the U.S. government as the chief villain in 2014 and the Russians as villains in 2016 and 2017. (China was less often a villain in online news as compared with mainstream media coverage.) In addition, digital media were likely to have as their main topic cyber attacks. Finally, corporate and U.S. government officials were also the most likely to be quoted in digital media cyber stories.

CONCLUSIONS

The last four years have seen a dramatic rise in attention to, and worries about, cyber-related issues. We see this reflected not only in our policy and politics, but also in our media coverage, where each year a greater number of stories about the topic appear in print, on air, and online. Over this period of time, major concerns have been raised about criminal hacking of personal data and how citizens can protect themselves; the pervasiveness of the most popular social media platforms and questions this raises about privacy and the spread of misinformation; whether foreign governments are infiltrating America's cyber ecosystem to disrupt and corrupt politics and perhaps even democracy itself; whether the U.S. government is violating its citizens' basic Constitutional rights in an effort to protect national security; and many other dimensions of this rapidly expanding issue. And of course in addition to all of those weighty and contentious issues, a great deal of press coverage is about more banal topics like the latest exciting gizmos, and the profit margins and stock prices of the companies that make them.

Much of what this study found regarding coverage of cyber resembles findings in previous studies of how other topics are treated in the mainstream press. Perhaps most significantly, media coverage of complex topics tends to be fairly episodic and event-driven, and less likely to engage in substantive discussions that convey a topic's complexity (though we see some improvement on this front in newspaper coverage in 2017). On one level this makes sense: daily journalism is mostly about what happened yesterday (or today, in the online news world), and its primary function might be said to surveil our society, not interpret it. Yet at

[10] *Wired*, *Arstechnica*, *The Verge*, *Politico Pro's* cyber vertical, *Lawfare's* cyber vertical, and *The Hill*.

the same time, scholars have long shown that an important reason why journalists engage in this type of coverage is less about mission and more about efficiency and routines: writing in depth on a topic can require time and expertise that journalists – who are typically generalists on deadline – do not have. This helps explain why we find the best coverage at elite publications (typically newspapers), where the resources exist to create cyber-related news beats, or at least where existing news beats (e.g., national security) overlap with cyber issues and where there are enough staff resources to cover multiple angles of the topic. In these cases, reporters have the expertise and expanded rolodex to do more in depth reporting, even on deadline.

Yet it's important to remember that the consequences of this episodic coverage can be profound. Scholars have found, for instance, that a steady diet of this type of reporting can encourage audiences to see less of a role for society and government in confronting issues. And on a basic level, superficial coverage can lead to superficial thinking.

This is why it's important to note the exceptions to this type of coverage. Online niche media, for instance, are increasingly easier for journalists to find and use and can make important contributions to the discussion of cyber issues amongst the press, the public, and policymakers. We see that in our data from some of the Hewlett grantees, such as CSIS. We also see it in the words and deeds of a growing number of policymakers, such as Rep. Will Hurd (R-TX), who has made the creation of a "Cyber National Guard" a cornerstone of his policy agenda for 2018. Hurd described this proposal at the "Covering Cyber" event held at George Washington University, and sponsored by Hewlett, in October 2017:

> "If you're a kid in high school and you want to get a degree in something related to cyber security and you don't have the ability to pay for it, we're going to try to find you some scholarships…. Let's say you go to Texas A&M University for four years. You're going to come work in the federal government for four years not at NSA or cyber command, (but) at the Department of Interior, or the US Census Bureau, or you name it…. (There are) about ten thousand positions across the federal government in the IT space that have gone unfilled. And once you work for, let's call it four years, and you get a job in the private sector, the private sector is going to loan you back for the proverbial one week in a month, two weeks a year (as with the military's National Guard)."

Yet there is still a significant learning curve in Congress, where Hurd is one of only a handful of legislators with a background in computer science. A similar lack of expertise exists in the press. This is why bringing experts together with reporters and policymakers is so critical as cyber issues become more and more central in our lives: journalism is source-driven, and the better the sources, the better the journalism.

And the stakes are only getting increasingly higher. Take something as seemingly innocuous as "smart home" technology, also known as "the internet of things," which is rapidly moving from speculative Jetsons journalism to the hot new trend in people's daily lives. As we've seen in this study, a significant amount of media coverage of cyber focuses on consumer technology. What's not to love about a refrigerator that texts you a shopping list, or an app that lets you turn off the oven remotely? Yet in October 2017 the largest ever cyber attack on America's internet infrastructure infiltrated the country's cyber pathways not through computers, but through internet of things devices.[11]

If our appliances pose a threat from hacking, the implications for larger scale attacks by terrorists and nation states are even more concerning and challenging. Yet the answers, and even the questions, aren't easy. Former CIA and NSA director Michael Hayden made this clear at the "Covering Cyber" event when he said the U.S. would "absolutely" respond to a cyber attack with force. But when asked what constitutes a "digital act of war," Hayden said it's not clear, and part of the problem is people can't agree on the terms of the debate, or, crucially, what can be debated in public:

> "Actually it's undefined and I'm not personally sure, and that's part of the problem… We lack consensus because we've not had the adult discussion. We have not had the adult discussion because the participants don't share a common database. And we don't have a common database because this (discussion) within government is over-classified, and within the private sector it's kept secret for their own liability reasons…. The declaratory American policy is we will respond to a cyber attack based upon its effects not upon its means. But we haven't yet decided what box we want to drop cyber attacks against the United States into (i.e., law enforcement, military, or intelligence) and therefore we don't have a reflex of automatic guided response."

These concerns only make the media's role in making sense of the range of cyber issues more critical. One encouraging aspect of the coverage analyzed in this study is that, so far at least, cyber is not an issue like so many others that has devolved into partisan divides. To date, there isn't a discernible "Democrat" or "Republican" position on these issues, though to be sure root differences between the parties on, for instance, tradeoffs between national security and civil liberties, underlie policy discussions. And as the Russian hacking/collusion story continues to envelope the Trump White House, it's possible this could become mired in he said-she said reporting.

That would be unfortunate. What we find in this study is the media devoting more and more news hole to the cyber story, even if it isn't always in the substantive way one might prefer. Yet media don't operate in a vacuum, and as policymakers (and their staffs) begin to focus more on these issues, and events keep putting them on the public, policy, and press agendas, news organizations may find new veins of expertise and sourcing to cover the issue in a way that reflects its seriousness and complexity. In the end, explanatory, investigative, and accountability journalism will be needed to not only inform citizens, but also to pressure government and the tech industry to drop their veils and cooperate. As Rep. Hurd said at the "Covering Cyber" event:

[11] Tamkin (2017), "10 Years After The Landmark Attack on Estonia, Is the World Better Prepared for Cyber Threats?"

“…If the federal government thinks they can defend digital infrastructure by themselves, or the private sector thinks it can defend infrastructure by itself, (this) is the equivalent of the French thinking the Maginot line is going to defend them from the Germans. We have to work together.”

APPENDIX 1: METHODOLOGY

The main thrust of this study involved an analysis of major U.S. newspapers and network and cable news channels from 2014-2017. Newspapers were selected based on circulation, with most of the top 20 being included in our sample. (In the interests of regional diversity, we replaced some in the top 20 that came from cities with other representation in our sample with papers from other cities in the U.S. that also had relatively high circulations.) A secondary analysis looked at coverage in a selection of specialty online media sites known to focus on cyber issues. Because for each of the years studied the number of stories about cyber-related topics went into the low five figures, it was impossible 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. More than 6,000 stories ended up in our sample.

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.