Much Ado About Hacking? How News Media in Germany, the United Kingdom, and the United States Report Cyber Threats

Authors: Christine Buse, Florian Meissner (Heinrich Heine University Düsseldorf, Germany)

Abstract: *Cyber security has become a key challenge for governments, companies, and citizens. This study conceptualizes media reporting as the phenomenon that binds these actors together. However, we know little about how threats to cyber security are reported. As a first step towards filling this gap, this study examines the reporting done by leading quality news websites in Germany, the United Kingdom, and the United States. Building on media reality theory and framing theory, a content analysis of 581 news articles related to cyber threats was conducted. U.K. news outlets alone accounted for more than half of the articles. In all three countries, hacking was by far the most prominent issue. There was also a clear focus on domestic events and actors. To conclude, media realities are typically shaped by national perspectives, despite the fact that cyber threats are a global phenomenon. Our findings furthermore imply that the news media successfully contributes to raising audiences' awareness of cyber threats but rarely discusses behaviors that would improve cyber security.*

Keywords: Cybercrime, cyber terrorism, cyber war, hackers, journalism, content analysis

1. Introduction

As digitization permeates our societies, cyber security has become a core challenge. It affects politics, the economy, and civil society alike. While the Internet holds numerous opportunities, it is also a venue for criminally and politically motivated cyberattacks that threaten our privacy, property, and the integrity of democratic processes. Such attacks also endanger critical infrastructures like hospitals and public transport. One important example is the WannaCry ransomware that affected both individuals and organizations across the globe in May 2017. It is suspected that North Korean hackers were behind this attack, causing billions of dollars in damages (Volz, 2017).

Cyberattacks by state and non-state actors with criminal and/or political intent are growing in number and professionalism (Deibert, 2017; Federal Bureau of Investigation, 2018). The concept of cyber security has thus been discussed more widely in recent years. According to Dunn Cavelty (2010, p. 155), cyber security "refers to a set of activities and measures, technical

and non-technical, intended to protect the…cyberspace, but also devices, software, and the information they contain and communicate." While there are epistemological debates about what constitutes security (Burgess, 2008), in the context of technology, the term usually accentuates malicious risks, while safety refers to accidental risks (Pièrre-Cambacédès & Chaudet, 2010). To emphasize the malicious character of the phenomenon in question, we predominantly use the term cyber threats in this paper.

Traditionally, the state has been in charge of countering threats to security, but this idea has become obsolete in cyberspace. Collaboration with industry and civil society is required for the state to improve and maintain cyber security. The European Commission (2013, p. 4) asserted in its *Cybersecurity Strategy of the European Union* that "All relevant actors, whether public authorities, the private sector or individual citizens, need to recognize this shared responsibility [and] take action to protect themselves." We therefore follow Mueller's (2010, p. 9) definition and suggest a broad understanding of Internet governance that effectively includes all actors mentioned above. But what are the connections between them? We argue they can be found in public debates about cyber threats and cyber security. However, we have very little systematic knowledge of what characterizes these debates, let alone how the debates figure across national borders. Given the increasing relevance of cyber threats and the growing expectation that everybody is expected to take at least basic actions for self-protection in cyberspace, it is necessary to conduct detailed investigations of how news media report these issues.

As a first step toward filling this gap, our study examined the reporting done by leading quality news websites across three countries. We focused on online coverage because we expected cyber threats to be an important issue in digital news. The leading research question (RQ) was as follows: Which similarities and dissimilarities can be observed in German, U.K., and U.S. online media coverage of cyber threats?

Based on the leading RQ, we developed five sub-RQs that address different dimensions of media coverage:

1. What was the main topic of the online media coverage?
2. Which temporal dimension was addressed in the online media coverage?
3. Where did the main topic discussed in the online media coverage take place?
4. Which actors were linked to the main topic discussed in the online media coverage?

5. Which media frames were applied in the online media coverage?
6. What is the valence and tenor of the online media coverage?

For our analysis, we draw from both media reality theory as well as framing theory. Both approaches—including why they were chosen as theoretical background for this study—are explained in the following section.

2. Theoretical approaches

2.1. The media reality approach

The media reality approach by Winfried Schulz (1976; 2011) views news reporting not as a mirror of physical reality but as the result of a filtering process based on journalistic selection criteria. In this media reality, some issues can appear significantly more or less prevalent compared to their prevalence in the real world. This is why crime reporting and official crime statistics, for instance, often seem to be out of touch. Of course, this has important implications for the way news media audiences perceive a phenomenon (Schulz, 2011, p. 76; see also Henn & Vowe, 2015). Empirical research in this field is therefore typically aimed at studying how reality is constructed in the media coverage under investigation. It often looks at the selection criteria, such as news values, and interpretive patterns, such as framing.

For research on news values, a key reference is the study by Galtung and Ruge (1965), who found that frequency, (attention) threshold, unambiguity, meaningfulness, consonance, unexpectedness, continuity, and composition were universal news values (which they referred to as news factors). With regard to news reporting in the "north-western corner of the world," (Galtung & Ruge, 1965, p. 68) they found reference to elite nations, elite people, personalization, and negativism to be further important criteria. Galtung and Ruge assumed that the more news factors apply to a given issue, the higher the chance that the media will report it. Many scholars have since tested and refined this set of news values. For instance, Harcup and O'Neill (2001) added that another selection criterion was whether news fits a media organization's own agenda. Maier, Ruhrmann, and Klietsch (2006) showed that conflict and violence have become more significant news values. In a more recent study, Harcup and O'Neill (2017, p. 1481) found that social media have led to the emergence of news values such as shareability.

According to Staab (1990, p. 208), news value theory is a model for the description and analysis of structures within media reality. This approach is commonly applied to understand which topics are reported and how. Based on news value theory, a set of structural dimensions has been developed and applied in the analysis of media coverage, such as temporal, topical, personal, spatial, and normative dimensions (Wilke, 1984, pp. 115–174). Among others, Henn and Vowe (2015, pp. 345–346) built on Wilke's work by investigating the weighting of an issue as well as topical, temporal, spatial, and personal dimensions of media reality. Given this systematic and well-established approach, we decided to use the same operationalization for our study.

2.2. Framing theory

This study furthermore draws from framing analysis (Entman, 1993; Matthes, 2014) to provide an understanding of the interpretive patterns that constitute a further pillar of media reality. Frames are the product of a process in the course of which individual segments of reality are emphasized in a way that suggests certain problem definitions, causal interpretations, moral evaluations, or recommendations for action (Maurer, 2017, pp. 84–85). Framing is a natural and omnipresent element of human communication and therefore occurs during all phases and levels of the mass-mediated communication process (Dahinden, 2006, p. 13). It is common to distinguish between journalistic frames, media frames, and audience frames (Entman, 1993, pp. 52–53; Matthes, 2014, p. 15; Maurer, 2017, pp. 83–84; Scheufele, 2004, p. 403). Journalistic frames are cognitive frameworks that influence the journalistic selection and production process. They can be reconstructed through interviews or newsroom observation. The result of this process is media frames, which can be reconstructed from the content of media reporting. The third category, audience frames, can be studied through media effect research. This study is aimed at the content of media reporting and therefore focuses on media frames, which are known to shape audience frames, at least to a certain degree (Nisbet, Hart, Myers, & Ellithorpe, 2013; Wolling & Arlt, 2015).

A popular and theoretically guided approach in framing research is the analysis of so-called basic frames that are generic and thus not related to a particular topic. Semetko and Valkenburg (2000, pp. 95–100) developed the following set of basic frames:

- Conflict frame: emphasizes conflicts between individuals, groups, and/or institutions and typically follows a winner-loser logic;

- Human interest frame: offers a personalized and often emotional perspective and focuses on personal experiences, private situations, and fateful events;
- Economic consequences frame: emphasizes the economic effects of a situation or incident at the individual, group, institutional, regional, or state level;
- Morality frame: connects a topic or event with certain norms or values and often makes an explicit or implicit judgment; and
- Attribution of responsibility frame: presents an event, topic, or problem in a way that the cause or required action is attributed to an individual, a group, the government, etc.

According to Semetko and Valkenburg (2000), the attribution of responsibility, conflict, and economic consequences frames typically dominate media reporting. However, the prevalence of the individual basic frames depends on the media genre (e.g., the attribution of responsibility and conflict frames are often prevalent in quality newspapers). As the analysis of basic frames is empirically tested and widely accepted (Lecheler & de Vreese, 2019, p. 4; Matthes & Kohring, 2004, p. 60), we decided to use this approach to complement our analysis of media realities concerning cyber threats (see Section 6).

3. Cyber security

The "systemic risks" (Klinke & Renn, 2006) emanating from cyberspace are associated with high levels of uncertainty, complexity, and ambiguity. Larger incidents like the WannaCry attack in 2017 can affect countries across the globe. More and more governments are developing cyber security strategies as cyberattacks by criminal and political actors have increased. Therefore, cyber security is characterized as "one of the critical questions of global politics in the 21st century" (Deibert, 2017, p. 172).

Threats to cyber security have been increasingly problematized in the field of security studies. For some scholars, it is one of the objects that constitutes the field of new security studies (Burgess, 2010; Dunn Cavelty, 2010). Other scholars, however, have argued that information technology, including the Internet, has been securitized from the very beginning because it originated from military technology (Bastl, Mareš, & Tvrdá, 2015, p. 50). This seems to be the case especially in the United States, where the Internet was invented and where the first cyber security policies date back to the mid-1980s (Dunn Cavelty, 2008). The European Union and

its member states are remarkably late in establishing such standards; Germany, for instance, passed its first cyber strategy in 2011.

Today, administrations worldwide find themselves in a contradictory position as cyberspace is both the object and tool of security policy (Deibert, 2017). The Snowden leaks of 2013 shed light on the massive surveillance programs conducted by Western intelligence agencies. There has since been debate about and tension between surveillance, privacy, and security (Friedewald, Burgess, Čas, Bellanova, & Peissl, 2017).

The security studies community has increasingly recognized the need to investigate how news media report cyber security (Dunn Cavelty, 2016). However, very few systematic studies have been conducted by security studies scholars. An exception is the research by Jarvis, Macdonald, and Whiting (2015; 2017), who found that there is no homogeneous reporting of cyber terrorism, but instead, international media showed varying levels of anxiety and different conceptions of cyber terrorists.

4. News reporting about cyber security

In the early years of digitization, little academic attention was given to how this technological revolution was communicated in society. Studies from the United States and Canada indicated that while a celebratory tone dominated media coverage of the information highway (Sklar, 1997), risks like computer viruses were debated as early as the mid-1980s (Patnode, 2003). Cyber security later became a more pronounced theme in North American communication research, with studies focusing on threats such as cybercrime (Hallahan, 2010), cyber terrorism (Eid, 2010), or the phenomenon of hacktivists like WikiLeaks (Hindman & Thomas, 2013).

In Germany, early media reporting of digitization included both euphoric and apocalyptic assessments (Beck & Vowe, 1995). Later studies building on the exploratory work of Beck and Vowe showed that multimedia was predominantly seen in a positive light by the German media (Rössler, 2001). The study by Zeller, Wolling, and Porten-Cheé (2010), however, revealed growing concern with security issues related to digitization. In a longitudinal study between 2000 and 2012, Oggolder (2015) showed how public perceptions of the Internet in various European countries, including Germany and the United Kingdom, changed from economic enthusiasm to more sober and sometimes critical assessments.

The Snowden leaks of 2013 triggered further internationalization of research on cyber security communication. Scholars from diverse national backgrounds and sub-disciplines like political communication (Dencik & Cable, 2017; Dimmroth, Steiger, & Schünemann, 2017; Wäscher, 2016) and journalism (Johnson, 2016; Ruby, Goggin, & Keane, 2016; Thorsen, 2016) addressed the communicative negotiation of security versus privacy between a variety of actors. In a cross-national view of media reporting concerning Internet governance, the political conflict about privacy and the emphasis on regulation were found to be most pronounced in German media, whereas in the United States, a deregulatory attitude and an external security concept prevailed (Löblich & Karppinen, 2014). However, after the Cambridge Analytica scandal, there has been a more intense debate about the abuse of personal data online in the United States, and awareness of cyber risks has been increasing (Edelman, 2018; Pew Research Center, 2018).

Our literature review shows that the research corpus on communication about cyber threats and cyber security is still limited. For instance, studies seldom provide a broader overview of the subject but instead focus on particular aspects. Moreover, very few studies include an international comparison.

5. International comparative journalism research

There is a broad consensus that comparative journalism research requires a decent amount of contextualization with regard to the various contextual factors shaping media coverage in a given society (e.g., Meissner, 2019). One important way to address this is to look at the countries under investigation from a media system perspective (e.g., Blum, 2014; Hallin & Mancini, 2004; 2012). Media system research views journalism predominantly from a political perspective (i.e., the political system is considered the main determinant of a media system). There are other important ways to approach this field, most notably the study of journalistic cultures.[1] However, for the purpose of this study, we chose the media systems perspective as cyber security is a highly politicized topic (see Section 3).

With regard to North American and European media systems, Hallin and Mancini (2004) distinguished between a polarized pluralist, a democratic corporatist, and a liberal model. For instance, Germany was categorized as a democratic corporatist media system, meaning it is shaped by political parallelism (the leanings of media organizations mirror the established

[1] For an overview, see Meissner (2019, pp. 13–36).

political parties), has a strong press tradition (note the data are from the beginning of the 2000s), a strong public service media, and a relatively high degree of journalistic professionalism. The liberal model, which both the United Kingdom and the United States belong to, is similar to the democratic corporatist model, but is rather shaped by market logic than by political parallelism.

A more recent approach was developed by Blum (2014). Based on an analysis of 23 media systems from both Western and non-Western regions, he grouped media systems across the world according to degrees of liberalism:

1. Liberal model (e.g., United States, Brazil)
2. Public service model (e.g., Germany, United Kingdom)
3. Clientelist model (e.g., Italy, Ghana)
4. Shock model (e.g., Russia, Thailand)
5. Patriot model (e.g., Iran, Belarus)
6. Commando model (e.g., China, Cuba)

Blum (2014, p. 294) counted both the liberal and public service models as part of a "liberal line," while clientelist and shock models represent the "middle line," and patriot and commando models are the "regulated line." His analysis confirmed the finding by Hallin and Mancini (2004) that the differences between the three media systems under investigation in this study (Germany, United Kingdom, United States) are limited. Our study therefore represents a "most similar systems" design (Esser & Vliegenthart, 2017). Such an approach is very common in comparative communication research. It is based on the assumption that the influence of an independent variable (in this case, media reporting of cyber threats) can only be described in detail if intervening variables (such as large differences between media systems) are avoided as much as possible.

6. Method and sample

Because of the normative importance that journalistic news offers and the development of the Internet as a major source of information (Hölig & Hasebrink, 2018), we conducted a quantitative content analysis of online news articles from the German newspapers the *Frankfurter Allgemeine Zeitung* (FAZ.NET) and the *Süddeutsche Zeitung* (Süddeutsche.de), the U.K. newspapers, *The Guardian* (TheGuardian.com) and *The Telegraph* (Telegraph.co.uk), and the U.S. newspapers *The New York Times* (NYTimes.com) and *The Washington Post*

(Washingtonpost.com). These news outlets were chosen due to their position as leading quality online news media, high numbers of users, and accessibility (Rühle, 2018; Thurman, 2014). The period under investigation was April 1, 2017 to July 31, 2018 and thus included the attack on Emmanuel Macron's election campaign team in the course of the 2017 French presidential election; the WannaCry ransomware attack, which affected National Health Service hospitals in England and Scotland as well as organizations worldwide; the cyberattack on the U.S. financial services provider *Equifax*; the BadRabbit malware attack; the implementation of U.S. sanctions against Russian hackers in March 2018; and the attack on the data network of the German Bundestag and the German Federal Foreign Office.

The articles were selected in two steps. In the first step, all articles which contained topical keywords related to cyber threats in the headline, subheading, or first paragraph were collected via the LexisNexis news archive or the respective news website. The keywords were derived from scientific literature such as the conceptual overview provided by Jarvis and Macdonald (2014). Articles about fictional products, such as film reviews or book reviews, sponsored articles, letters to the editor, advertisements, newsletters, and press reviews, were not included. Also, if cyber threats were only marginally discussed in the coverage, the articles were excluded from further analysis. Out of the remaining articles, every second one was included in the analysis (N = 581). In the coding process, the headline, subheading, body text, and contents of separate text units were analyzed. Hyperlinks, pictures, videos, graphics, sound documents, ads, pop-ups, navigation elements, and comments were not included in the analysis.

The codebook was developed on the basis of the news value theory (Galtung & Ruge, 1965; Schulz, 2011; Wilke, 1984) and the concept of framing (Lecheler & de Vreese, 2019). The categories related to characteristics of articles included the main topic, temporal dimension of the article, location of the main topic, and actors linked to the main topic. Additionally, generic news frames—such as the conflict, human interest, economic consequences, morality, and attribution of responsibility frames—were coded (Semetko & Valkenburg, 2000). Further, we decided to analyze the valence and tone of the articles. The valence of the coverage indicated whether the main topic of the article was reported in a positive, ambivalent, negative, or neutral way. The tenor of the news media coverage is related to the provided outlook on future developments, such as pessimistic, ambivalent, positive, or neutral expectations.

In a first step, formal attributes—such as the medium, publication date, and title of the article—were coded. In a second step, the main topic of the article was analyzed. If cyber threats were only marginally discussed or mentioned in the articles, these were excluded from the further analysis. The sample was analyzed by one coder. To verify the reliability of the measurement, both intra- and intercoder reliability were calculated using Holsti's coefficient of reliability. The results were satisfactory, with the coefficient ranging from 0.80 to 1.00 depending on the category.

7. Results

One striking result of our analysis was that the U.K. news outlets alone accounted for more than half (51.5%) of the articles included in the sample, followed by U.S. news outlets with 153 articles (26.3%), and German news outlets with 129 articles (22.2%) (Figure 1). While the number of articles is just one indicator of reporting intensity, this finding suggests that cyber threats were a more prominent news topic in the United Kingdom as compared to Germany or the United States. Possibly, this could be related to the extent of the WannaCry ransomware attack, which particularly affected the National Health Service in the United Kingdom. We found that 533 articles (91.7%) were factual reports while 44 (7.6%) were comments or editorials. Furthermore, there were four interviews (0.7%) included in the sample.

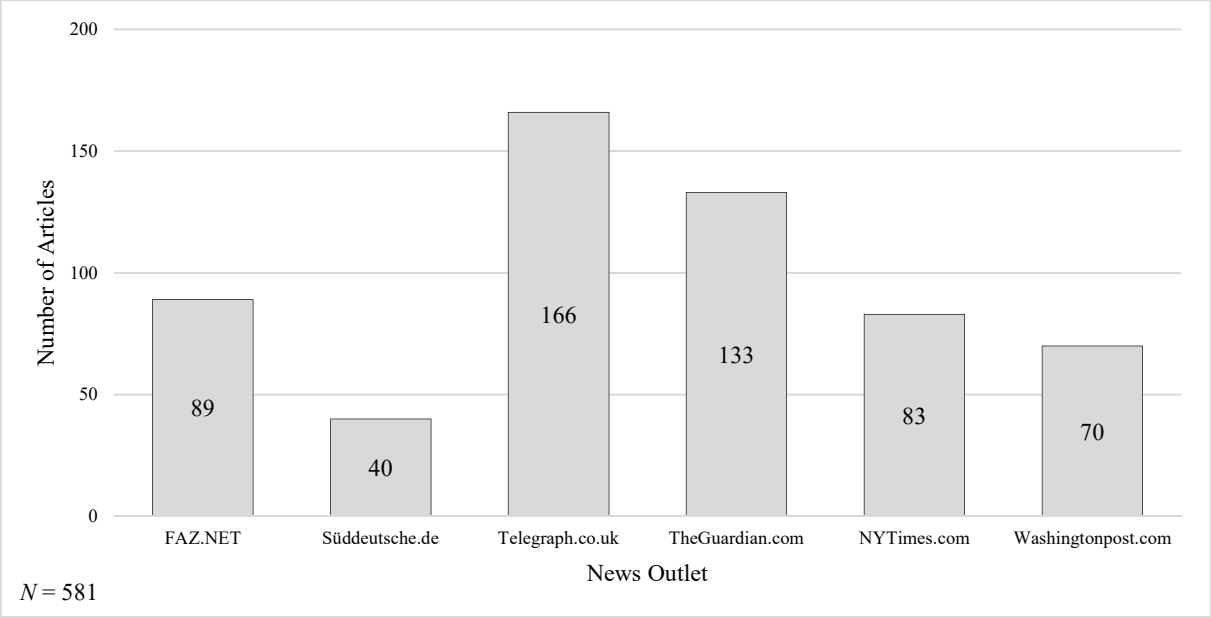

Figure 1. Number of articles published by the news outlets.

The share of comments and editorials was highest in *The Washington Post*, with 12 articles (17.1%), followed by *The Guardian*, with 16 articles (12.0%). Overall, however, the proportion of factual reports, regardless of language or country, dominated all news outlets.

7.1. Sub-RQ1: What was the main topic of the online media coverage?

In 454 (78.1%) of the 581 articles, cyber threats or certain types of cyber threats were the main topic of the reporting. In 127 (21.9%) of the articles, however, cyber threats were only marginally discussed or mentioned. The topics covered by the media during this time period did not vary substantially between countries. For instance, hacking was by far the most prominent issue across the German, U.K., and U.S. news outlets under investigation, with proportions ranging from 41.9% to 56.2% per country (Table 1). When reporting about hackers, news organizations referred almost exclusively to *black hats* (i.e., malicious hackers). However, news outlets did not differentiate between the terms *hacker* and *hacking*, but often applied both terms generously to different kinds of malicious online actors. Cyber terrorism (0.3%), cyber war (1.4%), cybercrime (2.4%), and cyber espionage (0.9%) played a subordinate role in reporting, while hacktivism, cracktivism, cyber sabotage, and cyber vandalism were not discussed as the main focus in any of the articles.

Table 1.

Main Topics of the Articles

			Coverage			Total
			Germany	United Kingdom	United States	
Main Topic	Cyber espionage	Number	2	2	1	5
		%	1.6%	0.7%	0.7%	0.9%
	Cyber terrorism	Number	0	2	0	2
		%	0.0%	0.7%	0.0%	0.3%
	Cyber war	Number	0	4	4	8
		%	0.0%	1.3%	2.6%	1.4%
	Hacking	Number	54	128	86	268
		%	41.9%	42.8%	56.2%	46.1%
	Cybercrime	Number	2	9	3	14
		%	1.6%	3.0%	2.0%	2.4%
	Cyber threats (in general)	Number	46	91	20	157
		%	35.7%	30.4%	31.1%	27.0%
	Other	Number	25	63	39	127
		%	19.4%	21.1%	25.5%	21.9%
	Total	Number	129	299	153	581
		%	100.0%	100.0%	100.0%	100.0%

The articles published by *The New York Times*, the *Süddeutsche Zeitung*, and *The Washington Post* had a strong focus on hacking, while the *Frankfurter Allgemeine Zeitung* and *The Telegraph* focused on both hacking and general cyber threats. In all three countries, online media coverage overwhelmingly focused on damages and threats, which accounted for approximately three out of every four reports (Table 2). Specific cyber security measures, meanwhile, received little attention, especially in Germany. While U.S. outlets reported more frequently about specific cyber security measures, the German and U.K. news outlets focused more on general security measures. Accordingly, only one article published by the *Frankfurter Allgemeine Zeitung* was related to specific security measures, such as investigations, trials, lawsuits, or warnings.

Table 2.

Damages and Cyber Security Measures

			Coverage			Total
			Germany	United Kingdom	United States	
Damages and Cyber Security Measures	Specific cyberattacks and damages	Number	65	140	70	275
		%	62.5%	59.3%	61.4%	60.6%
	Security risks	Number	18	36	17	71
		%	17.3%	15.3%	14.9%	15.6%
	Specific cyber security measures	Number	5	22	17	44
		%	4.8%	9.3%	14.9%	9.7%
	General cyber security measures	Number	15	37	10	62
		%	14.4%	15.7%	8.8%	13.7%
	Unidentifiable	Number	1	1	0	2
		%	1.0%	0.4%	0.0%	0.4%
Total		Number	104	236	114	454
		%	100.0%	100.0%	100.0%	100.0%

7.2. Sub-RQ2: Which temporal dimension was addressed in the online media coverage?

The reports under investigation typically focused on current events, with percentages between 79.2% (U.K. media) and 92.3% (German media). Past events received very little attention, while future developments ranged from 4.8% (German media) to 15.7% (U.K. media). Also, we found variations in focus between the news organizations within a country. For instance, within the U.K. news outlets, 20.4% of the articles published by *The Telegraph* focused on future events compared to only 9.4% of the articles published by *The Guardian*. This corresponded to the proportion of articles covering future developments published by the *Süddeutsche Zeitung* and *The Washington Post*.

7.3. Sub-RQ3: Where did the main topic discussed in the online media coverage take place?

In all countries, the focus was on domestic events and developments, with percentages between 33.7% (German media) and 60.5% (U.S. media). However, U.K. (14.0%) and German (18.3%) news outlets frequently covered incidents in the United States. The German coverage also paid considerable attention to global events and worldwide developments (22.1% of the articles). The percentages between the individual news sites differed moderately in each country. While 50.0% of the articles published by *The New York Times* and 75.0% of the articles published by *The Washington Post* referred to events in the United States, there was a smaller difference between *The Guardian* (40.4%) and *The Telegraph* (54.7%). One-third of the articles published by both the *Süddeutsche Zeitung* and the *Frankfurter Allgemeine Zeitung* focused on events and developments in Germany.

7.4. Sub-RQ4: Which actors were linked to the main topic discussed in the online media coverage?

From all 454 articles, a total of 1362 actors were included in the analysis. In all three countries, hackers were the most frequently mentioned actor in the articles (21.8%). About one-quarter of those hackers was mentioned in connection to a nationality or state (Table 3). With 45 mentions, Russian hackers played a significant role in the media reporting. North Korean and Chinese hackers were also frequently mentioned. In contrast to foreign hackers, domestic hackers were only mentioned once in German and once in U.S. news media coverage, while domestic hackers were mentioned four times in U.K. news media reporting. With 191 mentions, the second most frequently mentioned actors were companies (11.0%). Other frequently discussed actors included ministries and security agencies.

Frequently mentioned individual political actors included Donald Trump and Vladimir Putin, with 14 mentions each, and Emmanuel Macron, with seven mentions. Overall, however, political leaders only played a subordinate role in the news media coverage.

Table 3.

Hackers' Country of Origin

			Coverage			Total
			Germany	United Kingdom	United States	
Country of Origin	Not mentioned	Number	72	107	47	226
		%	88.9%	78.7%	58.8%	76.1%
	Russia	Number	8	16	21	45
		%	9.9%	11.8%	26.3%	15.2%
	China	Number	1	2	3	6
		%	1.2%	1.5%	3.8%	2.0%
	North Korea	Number	0	4	4	8
		%	0.0%	2.9%	5.0%	2.7%
	Iran	Number	0	0	3	3
		%	0.0%	0.0%	3.8%	1.0%
	Syria	Number	0	0	1	1
		%	0.0%	0.0%	1.3%	0.3%
	South Korea	Number	0	1	0	1
		%	0.0%	0.7%	0.0%	0.3%
	Romania	Number	0	0	1	1
		%	0.0%	0.0%	1.3%	0.3%
	Germany	Number	0	1	0	1
		%	0.0%	0.7%	0.0%	0.3%
	United Kingdom	Number	0	4	0	4
		%	0.0%	2.9%	0.0%	1.3%
	United States	Number	0	1	0	1
		%	0.0%	0.7%	0.0%	0.3%
Total		Number	81	136	80	297
		%	100.0%	100.0%	100.0%	100.0%

All in all, while German and U.K. news media often talked about hackers in general without connection to a state or nationality, the attribution of a national origin played an important role in the U.S. media reporting of cyber threats, especially with regard to Russian hackers.

7.5. Sub-RQ5: Which media frames were applied in the online media coverage?

Two basic frames played major roles and often co-occurred in the same article: the attribution of responsibility frame and the conflict frame (Table 4).

Table 4.

Frames

		Coverage		
		Germany	United Kingdom	United States
Frames	Attribution of responsibility	96.2%	91.5%	97.4%
	Conflict	64.4%	67.4%	88.6%
	Human interest	34.6%	33.5%	12.3%
	Economic consequences	30.8%	28.0%	26.3%
	Morality	7.7%	4.7%	0.9%

The attribution of responsibility frame was present in 94.1% of the articles. When talking about cyber threats, 45.4% of the articles blamed their own or a foreign government for the occurrence of a security threat, while 73.3% held an individual or a group responsible. Additionally, 25.6% of the articles asked the government to provide the solution to a security threat. Half of the coverage stressed the need for action, whereas 35.5% of the articles suggested direct solutions to problems regarding cyber security.

The conflict frame was measured in 72% of the articles. With percentages ranging from 64.7% (German media) to 88.6% (U.S. media), the conflict frame was most prominent in U.S. media reports. Regarding the individual dimensions of the conflict frame, disagreements as well as different perspectives were discussed in more than 20% of the articles. Particularly striking is that allegations were made in 79.3% of the articles.

The human interest frame occurred in 28.4% of the articles. Compared to the German (34.6%) and U.K. (33.5%) coverage, the human interest frame was only used in 12.3% of U.S. reporting. Regarding this frame, 13.9% of the articles used emotionalizing rhetoric, while individual impacts were mentioned in 27.1% of the articles. The private lives of the actors were only discussed in 6.2% of the reports.

The economic consequences frame was present in 28.2% of the articles. There were no major differences between the countries for this frame. Financial gains and losses were dealt with in 24.0% of the articles. Costs were presented in 25.1% of the articles, while 24.4% talked about economic consequences.

The morality frame only occurred in 4.4% of the coverage. Regarding this, 2.6% of the articles contained a moral message. Religious issues were discussed in 3.7% of the articles.

7.6. Sub-RQ6. What is the valence and tenor of the online media coverage?

In 76.2% of the articles, the main topic was presented in a negative way. Comparatively, 15.6% of the articles reported neutrally, while only 0.9% of the articles gave a predominantly positive coverage of the main topic. When making statements about future developments, all but one of the articles were pessimistic and presented failures, regressions, and conflicts as possible or probable.

8. Conclusion

Based on these findings, we conclude that media realities are typically shaped by national perspectives—despite the fact that cyber threats are a global phenomenon. Our study furthermore revealed that reporting does not mirror the actual extent of individual cyber threats. Instead, media coverage is mainly geared toward particular phenomena like hacking, while other significant threats such as cybercrime are underrepresented. One possible explanation is that hacking has significant political implications and frequently involves state actors; therefore, it attracts more media attention. It also must be noted that hackers/hacking seem to be catch-all phrases when used by many news organizations. This shows that there is a need for debate about how to use more differentiated terms to accurately describe the different types of malicious online actors (see for instance Deibert, 2017).

Another key finding was that cyber threats were a much more prominent news topic in the United Kingdom as compared to Germany and the United States. While a partial explanation may be that the WannaCry ransomware attack particularly affected the National Health Service in the United Kingdom, we suggest that future research should look into whether U.K. media generally reports extensively about cyber threats—and if yes, why.

Furthermore, it is striking that almost all articles contained the attribution of responsibility frame, meaning the articles held an individual, group, or the government responsible for either the occurrence of or providing the solution to a cyber security threat. However, in most of the articles, there was no clear distinction between state-sponsored and independent attacks. This shows—along with the finding that a large proportion of coverage was related to hacking—that cyber threats remain a rather opaque phenomenon in news media reporting.

An important limitation of our study is that we examined only quality news websites. We suggest examining a broader and more diverse sample of online news websites for future

research in this field. When looking at reporting intensity, further indicators such as article length should also be included. Lastly, we did not consider important parameters such as editorial policies and/or the number of cyber experts in newsrooms, both of which may provide deeper insights into the why and how behind the reporting conducted by individual news organizations.

Finally, surveys have shown that citizens often feel overtaxed with trying to protect themselves online (Deutsches Institut für Vertrauen und Sicherheit im Internet, 2017). This implies that the news media successfully contribute to raising audiences' awareness of cyber threats but fails to empower users because they rarely discuss behaviors that would improve cyber security. This is supported by our result that approximately three out of four reports covered current cyber events, while concrete security measures only played a minor role, especially in German media coverage. Further studies should therefore examine ways in which communicators in the area of cyber security can influence public debates effectively and strengthen the discussion about secure online behavior.

References

Bastl, M., Mareš, M., & Tvrdá, K. (2015). Politik der Cybersicherheit auf nationaler, europäischer und internationaler Ebene: Eine Rahmenanalyse [Cyber security policy on a national, European, and international level: A framework analysis]. In H.-J. Lange & A. Bötticher (Eds.), Cyber-Sicherheit [*Cyber security*] (pp. 45–68). Wiesbaden, Germany: Springer.

Beck, K., & Vowe, G. (1995). Multimedia aus Sicht der Medien: Argumentationsmuster und Sichtweisen in der medialen Konstruktion [Multimedia from a media point of view. Argumentation patterns and perspectives in the medial construction]. *Rundfunk & Fernsehen*, *43*(4), 549–562.

Blum, R. (2014). Lautsprecher und Widersprecher: Ein Ansatz zum Vergleich der Mediensysteme [*Loudspeaker and dissenter: An approach to comparing media systems*]. Cologne, Germany: Herbert von Halem.

Burgess, J. P. (2008). The ethical challenges of human security in the age of globalisation. *International Social Science Journal*, *59*(1), 49–63.

Burgess, J. P. (2010). Introduction. In J. P. Burgess (Eds.), *The Routledge handbook of new security studies* (pp. 1–4). London, United Kingdom: Routledge.

Dahinden, U. (2006). Framing: Eine integrative Theorie der Massenkommunikation [Framing: An integrative theory of mass communication science]. Konstanz, Germany: UVK.

Deibert, R. (2017). Cyber-Security. In M. Dunn Cavelty & T. Balzacq (Eds.), *Routledge handbook of security studies* (pp. 172–182). London, United Kingdom: Routledge.

Dencik, L., & Cable, J. (2017). The advent of surveillance realism: Public opinion and activist responses to the Snowden leaks. *International Journal of Communication*, *11*, 763–781.

Deutsches Institut für Vertrauen und Sicherheit im Internet. (2017). Digitalisierung – Deutsche fordern mehr Sicherheit: Was bedeutet das für Vertrauen und für Kommunikation? [Digitization—Germans demand more security: What does this mean for trust and communication?]. Retrieved from https://www.divsi.de/wp-

content/uploads/2018/02/DIVSI-Studie_Digitalisierung_Deutsche-fordern-mehr-Sicherheit_2017-08.pdf

Dimmroth, K., Steiger, S., & Schünemann, W. J. (2017). Outrage without consequences? Post-Snowden discourses and governmental practice in Germany. *Media and Communication*, *5*(1), 7–16.

Dunn Cavelty, M. (2008). Cyber-terror—looming threat or phantom menace? The framing of the US cyber-threat debate. *Journal of Information Technology & Politics*, *4*(1), 19–36.

Dunn Cavelty, M. (2010). Cyber-Security. In J. P. Burgess (Eds.), *The Routledge handbook of new security studies* (pp. 154–162). London, United Kingdom: Routledge.

Dunn Cavelty, M. (2016). Cyber-security and the media. In P. Robinson, P. M. Seib, & R. Fröhlich (Eds.), *Routledge handbooks. Routledge handbook of media, conflict and security* (pp. 270–281). London, United Kingdom: Routledge.

Edelman. (2018). *2018 Trust in technology*. Retrieved from https://www.edelman.com/post/trust-in-technology-2018

Eid, M. (2010). Cyber-terrorism and ethical journalism: A need for rationalism. *International Journal of Technoethics*, *1*(4), 1–19.

Entman, R. M. (1993). Framing: Toward clarification of a fractured paradigm. *Journal of Communication*, *43*(4), 51–58.

Esser, F., & Vliegenthart, R. (2017). Comparative research methods. In J. Matthes, C. S. Davis, & R. F. Potter (Eds.), *The international encyclopedia of communication research methods* (pp. 1–22). Hoboken, NJ: John Wiley & Sons.

European Commission. (2013). *Cybersecurity strategy of the European Union: An open, safe and secure cyberspace*. Retrieved from European Union website: https://eeas.europa.eu/archives/docs/policies/eu-cyber-security/cybsec_comm_en.pdf

Federal Bureau of Investigation (2018). *2017 Internet Crime Report*. Retrieved from https://pdf.ic3.gov/2017_IC3Report.pdf

Friedewald, M., Burgess, J. P., Čas, J., Bellanova, R., & Peissl, W. (Eds.). (2017). *Surveillance, privacy and security: Citizens' perspectives*. London, United Kingdom: Routledge.

Galtung, J., & Ruge, M. H. (1965). The structure of foreign news: The presentation of the Congo, Cuba and Cyprus crises in four Norwegian newspapers. *Journal of Peace Research, 2*(1), 64–91.

Hallahan, K. (2010). Crises and risk in cyberspace. In R. L. Heath & H. D. O'Hair (Eds.), *Handbook of Risk and Crisis Communication* (pp. 412–445). New York, NY: Routledge.

Hallin, D. C. & Mancini, P. (2004). *Comparing media systems: Three models of media and politics*. Cambridge, United Kingdom: Cambridge University Press.

Hallin, D. C. & Mancini, P. (2004). *Comparing media systems beyond the western world*. Cambridge, United Kingdom: Cambridge University Press.

Harcup, T., & O'Neill, D. (2001). What is news? Galtung and Ruge revisited. *Journalism Studies*, *2*(2), 261–280.

Harcup, T., & O'Neill, D. (2017). What is news? News values revisited (again). *Journalism Studies*, *18*(12), 1470–1488.

Henn, P., & Vowe, G. (2015). Facetten von Sicherheit und Unsicherheit: Welches Bild von Terrorismus, Kriminalität und Katastrophen zeigen die Medien [Facets of security and insecurity: What picture of terrorism, crime, and disasters do the media show]? *Medien & Kommunikationswissenschaft*, *63*(3), 341–362.

Hindman, E. B., & Thomas, R. J. (2013). When old and new media collide: The case of WikiLeaks. *New Media & Society*, *16*(4), 541–558.

Hölig, S., & Hasebrink (2018). Nachrichtennutzung und soziale Medien: Befunde aus dem Reuters Institute Digital News Survey 2018 [*News consumption and social media. Findings from the Reuters Institute Digital News Survey 2018*]. *Media Perspektiven*, *12*, 574–582.

Jarvis, L., & Macdonald, S. (2014). Locating cyberterrorism: How terrorism researchers use and view the cyber lexicon. *Perspectives on Terrorism, 8*(2), 52–65.

Jarvis, L., Macdonald, S., & Whiting, A. (2015). Constructing cyberterrorism as a security threat: A study of international news media coverage. *Perspectives on Terrorism*, *9*(1), 60–75.

Jarvis, L., Macdonald, S., & Whiting, A. (2017). Unpacking cyberterrorism discourse: Specificity, status, and scale in news media constructions of threat. *European Journal of International Security*, *2*(1), 64–87.

Johnson, C. N. (2016). A "Massive and Unprecedented Intrusion": A comparative analysis of American journalistic discourse surrounding three government surveillance scandals. *Digital Journalism*, *5*(3), 318–333.

Klinke, A., & Renn, O. (2006). Systemic risks as challenge for policy making in risk governance. *Forum Qualitative Sozialforschung*, *7*(1). Retrieved from https://nbn-resolving.org/urn:nbn:de:0114-fqs0601330

Lecheler, S., & de Vreese, C. H. (2019). *News framing effects*. London, United Kingdom: Routledge.

Löblich, M., & Karppinen, K. (2014). Guiding principles for internet Policy: A comparison of media coverage in four western countries. *The Information Society*, *30*(1), 45–59.

Maier, M., Ruhrmann, G., & Klietsch, K. (2006). Der Wert von Nachrichten im deutschen Fernsehen: Ergebnisse einer Inhaltsanalyse 1992-2004 [The value of news in German TV: Results from a content analysis 1992-2004]. Düsseldorf, Germany: Landesanstalt für Medien Nordrhein-Westfalen.

Matthes, J. (2014). *Framing*. Baden-Baden, Germany: Nomos.

Matthes, J., & Kohring, M. (2004). Die empirische Erfassung von Medien-Frames [The empirical measuring of media frames]. *Medien & Kommunikationswissenschaft*, *52*(1), 56–75.

Maurer, M. (2017). *Agenda-Setting*. Baden-Baden, Germany: Nomos.

Meissner, F. (2019). Kulturen der Katastrophenberichterstattung: Eine Interview-Studie zur Fukushima-Krise in deutschen und japanischen Medien [*Cultures of disaster reporting: An interview study on the Fukushima crisis in German and Japanese media*]. Wiesbaden, Germany: Springer VS.

Mueller, M. L. (2010). *Networks and states: The global politics of internet governance*. Cambridge, MA: MIT Press.

Nisbet, E. C., Hart, P.S., Myers, T.A., & Ellithorpe, M. (2013). Attitude change in competitive framing environments? The moderating role of open-/closed-mindedness, framing effects, and climate change. *Journal of Communication*, *63*(4), 766–785.

Oggolder, C. (2015). From virtual to social: Transforming concepts and images of the internet. *Information & Culture*, *50*(2), 181–196.

Patnode, R. (2003). Of viruses and victims: Framing the internet, 1988–1990. In ICA (Eds.), *Conference proceedings* (pp. 1–20).

Pew Research Center. (2018). *Americans are changing their relationship with Facebook*. Retrieved from http://www.pewresearch.org/fact-tank/2018/09/05/americans-are-changing-their-relationship-with-facebook/

Piètre-Cambacédès, L., & Chaudet, C. (2010). The SEMA referential framework: Avoiding ambiguities in the terms “security” and “safety”. *International Journal of Critical Infrastructure Protection*, *3*(2), 55–66.

Rössler, P. (2001). Between online heaven and cyberhell: The framing of 'the internet' by traditional media coverage in Germany]. *New Media & Society*, *3*(1), 49–66.

Ruby, F., Goggin, G., & Keane, J. (2016). “Comparative silence” still? Journalism, academia, and the five eyes of Edward Snowden. *Digital Journalism*, *5*(3), 353–367.

Rühle, A. (2018). Nachrichtennutzung und -bewertung in den USA: Eine vergleichende Sekundäranalyse der Nutzergewohnheiten [*News consumption and evaluation in the United States: A comparative secondary analysis of user habits*]. *Media Perspektiven*, *11*, 544–556.

Scheufele, B. (2004). Framing-effects approach: A theoretical and methodological critique. *Communications*, *29*(4), 401–428.

Schulz, W. (1976). *Die Konstruktion von Realität in den Nachrichtenmedien: Analyse der aktuellen Berichterstattung* [*The construction of reality in the news media: Analysis of current reporting*]. Freiburg, Germany: Karl Alber.

Schulz, W. (2011). *Politische Kommunikation: Theoretische Ansätze und Ergebnisse empirischer Forschung* [*Political communication: Theoretical approaches and results of empirical research*]. Wiesbaden, Germany: VS Verlag für Sozialwissenschaften.

Semetko, H. A., & Valkenburg, P. M. (2000). Framing European politics: A content analysis of press and television news. *Journal of Communication, 50*(2), 93–109.

Sklar, A. (1997). (De)constructing the (information) highway: Discourse analysis of Canadian popular press. *The Electronic Journal of Communication*, *7*(4). Retrieved from http://www.cios.org/EJCPUBLIC/007/4/007414.HTML

Staab, J. F. (1990). Nachrichtenwert-Theorie. Formale Struktur und empirischer Gehalt [News value theory: Formal structure and empirical content]. Freiburg, Germany: Karl Alber.

Thorsen, E. (2016). Cryptic journalism: News reporting of encryption. *Digital Journalism*, *5*(3), 299–317.

Thurman, N. (2014). Newspaper consumption in the digital age: Measuring multi-channel audience attention and brand popularity. *Digital Journalism*, 2(2), 156–178.

Wäscher, T. (2016). Framing resistance against surveillance: Political communication of privacy advocacy groups in the “Stop Watching Us” and “The Day We Fight Back” campaigns. *Digital Journalism*, *5*(3), 368–385.

Wilke, J. (1984). Nachrichtenauswahl und Medienrealität in vier Jahrhunderten: Eine Modellstudie zur Verbindung von historischer und empirischer Publizistikwissenschaft [*News selection and media reality in four centuries: A study relating historical and empirical communication research*]. Berlin, Germany: Walter de Gruyter.

Wolling, J., & Arlt, D. (2015). Informieren und Framen: Zum Einfluss der Medienberichterstattung auf Vorstellungen und Einstellungen zur Energiewende in Deutschland [Informing and framing: On the influence of media coverage of ideas and attitudes related to the energy transition in Germany]. In M. S. Schäfer, S. Kristiansen & H. Bonfadelli (Eds.), Wissenschaftskommunikation im Wandel [*Changes in science communication*] (pp. 288–314). Cologne, Germany: Herbert von Halem.

Volz, D. (2017). *U.S. blames North Korea for 'WannaCry' cyber attack*. Retrieved from: https://www.reuters.com/article/us-usa-cyber-northkorea/u-s-blames-north-korea-for-wannacry-cyber-attack-idUSKBN1ED00Q

Zeller, F., Wolling, J., & Porten-Cheé, P. (2010). Framing 0/1: Wie die Medien über die "Digitalisierung der Gesellschaft" berichten [How media report on the "digitization of society"]. *Medien & Kommunikationswissenschaft*, *58*(4), 503–524.