Andrea Zeffiro, Gil Niessen, Clementine Oberst, Sam McEwan, Alexis-Carlota Cochrane, Joshua Durand

Discourses on cybersecurity

The politics of the data breach as a security crisis

DISCOURSES ON CYBERSECURITY. THE POLITICS OF THE DATA BREACH AS A SECURITY CRISIS

Cybersecurity is a complex topic that is no longer limited to the information technology industry or national security agencies. It intersects with multiple facets of contemporary life, affecting individuals, organizations, and nation-states in increasingly interlocking ways. We examine one aspect of cybersecurity: data breaches. Our contribution stems from a larger multi-year project that traces the emergence of data breaches as a security crisis from 2005 to the present. We focus on how these events are construed as security crises through the normalizing discourses of cybersecurity rhetoric and mainstream media. Our analysis centers on three pairings or cases: the 2007 Tjx companies data breach and the Fourth intergovernmental panel on climate change report, the 2013 Yahoo data breach and Edward Snowden National security agency disclosures, and the 2018 MyFitnessPal data breach and the Gatwick drone incident. Our preliminary findings respond to two related questions. What historical conditions, practices, techniques, and deployments of power have shaped dominant cultural understandings of data breaches as security crises? How has knowledge about data breaches been circulated and obscured by dominant security crisis discourses? By engaging with these questions, we examine how data breaches materialize into intelligible objects and events along two axes: the hegemony of the security crisis and the normalization of surveillance capitalism. We argue that data breaches are social, political, and cultural processes rather than strictly neutral technological phenomena.

KEYWORDS *Cybersecurity, Data Breach, Security Crisis, Critical Discourse Analysis, North America.*

Andrea Zeffiro, Department of Communication Studies and Media Arts and the Lewis and Rith Sherman Centre for Digital Scholarship, McMaster University – Hamilton, On, Canada – email: zeffiroa@mcmaster.ca, orcid: 0000-0002-3741-4982.

Gil Niessen, Department of Communication Studies and Media Arts, McMaster University – Hamilton, On, Canada – email: niessenj@mcmaster.ca, orcid: 0000-0002-7502-6630.

Clementine Oberst, Department of Communication Studies and Media Arts, McMaster University – Hamilton, On, Canada – email: oberstc@mcmaster.ca, orcid: 0000-0002-0662-6501.

Samantha McEwan, Department of Communication Studies and Media Arts, McMaster University – Hamilton, On, Canada – email: mcewas1@mcmaster.ca, orcid: 0000-0002-5961-9217.

Alexis-Carlota Cochrane, Department of Communication Studies and Media Arts, McMaster University – Hamilton, On, Canada – email: alexiscarlota@mcmaster.ca, orcid: 0000-0001-5185-6966.

Joshua Durand, Department of Communication Studies and Media Arts, McMaster University – Hamilton, On, Canada – email: durandj@mcmaster.ca.

ISSN 2785-0072

1. Introduction

In 2019, the World economic forum identified online data thefts and large-scale cyberattacks as a global threat, placing data breaches alongside global crises like climate change and geopolitical conflict (Myers and Whiting 2019). Cybersecurity is a complex topic that is no longer limited to the information technology industry or national security agencies. It intersects with multiple facets of contemporary life, affecting individuals, organizations, and nation-states in increasingly interlocking ways. Our contribution examines one aspect of cybersecurity: data breaches. The term «data breach» describes a technological crisis marked by unauthorized access to and loss of control of private, confidential, and sensitive data. Data breaches are not a new phenomenon (Diamond 1984). However, over the last fifteen years, the volume, velocity, variety, and variability of consumer data generated across platforms and between devices has meant that private, confidential, and sensitive data is circulated and collected at an unprecedented rate (Kitchen 2014) that when coupled with consumers' willingness to share personal information has contributed to an «era of big data breaches» (Parent 2019).

Our contribution to the special issue on the political dimensions of cybersecurity stems from a larger multi-year project[1] that traces the emergence of data breaches as a security crisis from 2005 to the present. We focus on how these events are construed as security crises through cybersecurity rhetoric and mainstream media. In total, we have examined 32 cases. For each year from 2005 to the present, we paired a data breach event with a geopolitical security crisis and analyzed approximately 10-15 primary sources for each year using critical discourse analysis (Fairclough 1992, 2010; Jiwani and Richardson 2011; Roderick 2016) to understand how data breaches are engendered through discursive practices (Foucault 1972). Knowledge about data breaches is produced through the ways these events are talked about and represented. We examine the link between data breaches and geopolitical crises through language by studying the differences and similarities in how these are constructed under the overarching framework of surveillance capitalism (Zuboff 2019). Our analysis centers on how data breaches are construed as crises through news media. We consider these discourses of security crises as examples of what Michel Foucault (1972, 1978) described as normalizing discourses. According to Foucault (1980), power/knowledge operates through selective discourses and discursive practices in particular institutional settings to normalize practices

[1] The research project is generously supported by the Social Sciences and Humanities Research Council of Canada.

and actions. Normalization is a process propelled by discursive strategies that introduce and maintain new standards of representing a specific phenomenon in public discourse. We examine how techniques of normalization function toward the production, negotiation, and management (Reed 2000) of data breaches as security crises.

Our analysis centers on three pairings or cases: the 2007 Tjx companies data breach and the Fourth intergovernmental panel on climate change report, the 2013 Yahoo data breach and Edward Snowden National security agency (Nsa) disclosures, and the 2018 MyFitnessPal data breach and the Gatwick drone incident. Our preliminary findings respond to two related questions. What historical conditions, practices, techniques, and deployments of power have shaped dominant cultural understandings of data breaches as security crises? How has knowledge about data breaches been circulated and obscured by dominant security crisis discourses? By engaging with these questions, we examine how data breaches materialize into intelligible objects and events along two axes: the hegemony of the security crisis and the normalization of surveillance capitalism. We argue that data breaches are social, political, and cultural processes rather than strictly neutral technological phenomena.

The larger project from which our paper stems traces the construction of the data breach as a security crisis from 2005 to the present. The year 2005 was chosen as a starting point for two reasons. First, in the early to mid-2000s, «virus» was still used as an analogy to biological viruses to explain cybersecurity threats. The focus of the project is not on the virus; however, we want to account for the shift from virus to breach because the change in language reflects not only technological advancements at a certain historical moment but also the ways those advancements are understood and articulated through language that leverages non-technological crises. Second, in 2005 North America was on the cusp of widespread smartphone adoption, and Apple introduced the smartphone only 2 years later in 2007 (Burgess 2012). By the end of 2012, 1 billion smartphones were in use worldwide (Reisinger 2012). Studying data breaches over the last 15 years accounts for the shift from desktop computing structures to ubiquitous cloud computing infrastructures through which pervasive data collection is the norm.

We have examined 32 cases in total; we chose two cases per year from 2005 to the present, pairing a data breach event with a geopolitical security crisis. First, we chose a data breach case with geopolitical significance. We then chose a geopolitical security crises companion case within the same year that shared similarities with the data breach case in terms of how it was construed as a security crisis. For cases in the early years, it was sometimes difficult to demarcate the geopolitical significance of a data breach because these events were not yet ascribed to the same level of significance as they are today. In turn, we selected high-profile data breach cases because these had more coverage, and the coverage contributed to the discursive construction of data breaches. For example, the 2007 Tjx companies data breach is notable because, at the time, it was considered the largest data breach in history (Swartz 2007). Our analysis shows how, unlike more contemporary sources that seek to pinpoint the cause of a breach or identify the malicious actors responsible for it, in 2007, data breaches were conceptualized as an inevitable consequence of technological progress. When searching for a companion case, we discovered that framing technological and scientific progress as inevitable was also encapsulated by how the fourth intergovernmental panel on climate change (Ipcc) report was taken up. Our findings reveal divisiveness in how the inevitability of the climate crisis was positioned as a necessary trade-off with progress or outrightly denied. The Tjx and Ipcc pairing differs from the technology thematic linking the 2013 Yahoo data breach and Edward Snowden Nsa disclosures, and the 2018 MyFitnessPal data breach and the Gatwick drone incident. However, the framing of technoscientific progress as inevitable and self-propelled is worth noting because, in later years, data breaches are no longer framed in such a way. Instead, the data breach as a security crisis is rendered as exceptional. The normalizing discourse of the data breach as a security crisis, as we argue, is core to the logic of surveillance capitalism and the expansion of datafication. Moreover, we discerned from the cases in the later years how an increasing number of complex and interlocking technoscientific issues are redefined through an abstract and universalizing hegemony of security crisis.

2. Cybersecurity as a social practice

Our research is informed by scholarship that approaches cybersecurity as a social practice (Ashenden 2021; Dunn Cavelty 2018; Gjesvik and Szulecki 2022; Stevens 2020). Through this lens, cybersecurity constitutes a set of activities comprising meanings, symbols, competencies, procedures, materials, and technologies (Ashenden 2021, 3). It is enacted and stabilized through the circulation of knowledge about insecurities, with a specific focus on the practices engaged in discovering, exploiting and removing those insecurities (Dunn Cavelty 2018, 27). Therefore, as a practice, cybersecurity is not produced naturally. How it is perceived and operationalized emerges from a multifaceted domain of technologies, processes, practices and socio-technical arrangements congealing around interest with security in and through ubiquitous computing (Stevens 2020, 133).

Scholars in the field of critical security studies adopt a critical constructivist approach to cybersecurity, positioning cyber + security as a complex site of interaction. Cybersecurity encompasses a range of people, technologies and organizations, and heterogeneous discourses and practices with competing purposes and contradictory conceptualizations of the thing to be secured (Hensen and Nissenbaum 2009). Security in this configuration is understood as a discursive and political practice; it is produced through historical, cultural, and political legacies (Hensen and Nissenbaum 2009, 1156; Rothschild 1995). «Constituting something as a (security problem) while simultaneously defining something as not» write Lene Hensen and Helen Nissenbaum (2009, 1156), «has significant consequences in that it endows (the problem) with a status and priority that (non-security problems) do not have». The authors chart the shift from computer security to cybersecurity and examine the political and normative ramifications of formulating cyber issues as security problems. They trace cybersecurity as having emerged from the post-Cold War agenda in response to technological innovations and changing geopolitical conditions (Hensen and Nissenbaum 2009, 1155).

In the 1990s, computer scientists first used cybersecurity to categorize a series of insecurities related to networked computers. Security was treated primarily as a technical problem, despite being «a rich, complex, and contested concept with variable shadings of specialized and general meanings» (Nissenbaum 2005, 62). As computer scientists and professionals grappled with how to protect computer systems and their users from attacks (Nissenbaum 2005, 63), the cybersecurity discourses circulated by the media, private corporations and American politicians likened threats to networked computers as «electronic Pearl Harbors» and «weapons of mass disruption» to conjure significant threats to the Western world (Hansen and Nissenbaum 2009, 1155).

Following September 11, 2001, discourses of cyberspace as security crises changed dramatically (Cap 2017; Dunn Cavelty 2008b; Hansen and Nissenbaum 2009; Lawson 2013; Nissenbaum 2005). The cybersecurity rhetoric from Us government officials positioned dangers as imminent, dire and urgent, situating cyberspace as an «embattled frontier» (Nissenbaum 2005, 67) and making ample use of public anxiety after 9/11. For example, in an Abc News interview in September 2002, former Special White House Advisor for Cyberspace Security Richard Clarke explained how «cyberterrorism is easier to do than building a weapon of mass destruction. Cyberattacks are a weapon of mass disruption, and they're a lot cheaper and easier» (Cap 2017, 59). In traditional security policy, hostile actors are defined as potentially threatening states or governments, but in cyberterrorism, non-state actors also pose a threat. These anonymous adversaries penetrating information systems from virtually anywhere in the world rupture the traditional understanding of security. That the identity location and goals of the enemy are rendered murky or remain unknown augments the sense of uncertainty and fear (Cap 2017, 61). In turn, «security discourse not only heightens the salience and priority of designated threats», writes Nissenbaum, «but bestows legitimacy on a particular range of reactions» (Nissenbaum 2005, 69). The extraordinary measures adopted under the guise of security typically bend the rules of standard governance and break from routine democratic procedures (Nissenbaum 2005). For this reason, Nissenbaum encourages us to remain attentive to how conceptions of security inform computer security domains because each warrant specific defensive activities (Nissenbaum 2005, 69)

How cyber threat discourses are constructed is also expressive of broader public anxieties and fears. For example, professional and popular discussions of computer viruses in the 1990s capitalized on analogies to biological viruses, notably the Aids crisis, and imported from popular and medical discourses ideas and anxieties about self-contained bodies that must be protected from outside threats (Helmreich 2000; McKinney and Mulvin 2019; Parikka 205; Ross 1991; Rushkoff 1996). The shift in emphasis from virus to breach has arisen based on the characteristics of technology at a certain point in time. With the shift from the networking of remote desktops to ubiquitous cloud computing, the modification in language from virus to breach is representative also of how experts and non-experts alike leverage the language of cultural anxieties to explain the complex, abstract, and arcane vulnerabilities of ubiquitous networked computing (Eriksson 2001; Sampson 2007; Yan 2003). Like scholars examining the virus, we also understand data breach representations as discursive and examine how representations can change cybersecurity practices (Dunn Cavelty 2007, 2013; Lupton 2004; Lapointe 2004).

Likewise, other scholars have pointed out how threat discourses are also concerned with technological progress and its consequences (Cap 2017, 53). Cyber-doom scenarios are a contemporary manifestation of fears about «technology-out-of-control» in Western society (Lawson 2013, 87). Despite the shifting and persistent ambiguity for what is being threatened and by whom, these scenarios have endured over the last three decades as a rhetorical tactic for motivating and mobilizing a response to cybersecurity crises (Lawson 2013, 87). Cyber threat discourses that lean on other threat analogies produce the subject to be protected and the related harm, fear, and danger. Moreover, these «legitimizing discourses» are produced not necessarily by state leaders but by individuals acting on behalf of the general public, like scientists, journalists, and media experts (Cap 2017).

News media coverage also produces and circulates cybersecurity discourses. How the issues are represented by news media can influence knowledge of and attitudes toward emerging technologies and their risks. Surveys on Information communication technology (Ict) risk perception and awareness have identified the news media as a key source of information (see Boholm 2021). Coverage can positively impact readers by making them aware of threats and risks and promoting cyber hygiene, just as sensationalistic coverage can contribute to misconceptions about issues like cyberterrorism and cybercrime and hold consequences for policy priorities (Boholm 2021). A recent study examining 25 years (1995-2019) of cyber threat representation from three Swedish newspapers reveals newspaper representation of cyber threats was largely «amplification without the event», meaning there was coverage without necessarily linking to it topical events (Boholm 2021). The study's author, Max Boholm, considers how information security and cybersecurity are societal concerns due to the dependence on Icts. These issues have been elevated in importance with other geopolitical crises because information communication technologies and cybersecurity are cross-sectoral concerns. Nevertheless, because of the prevalence and weight given to these events, as Boholm notes, news media representation plays an important role in the shaping of public discourses. Similarly, an earlier study on how social science fiction contributes to the production of knowledge about cybercrime revealed how news reports reinforce existing fears by making vague predictions about what could happen with what is happening, making it seem like cybercrime is far more prevalent than it is (Wall 2008a). This practice presents cyber threats as extremely prevalent and threatening, and molds public media opinions and expectations about threats and vulnerabilities (Wall 2008b).

How cybersecurity is framed is indicative of a power struggle for a shared narrative about what counts as threats, risks and insecurities. Framing establishes and upholds Metaphors and symbols that encourage specific ways of perceiving phenomena (Eriksson 2001). Cait McKinney and Dylan Mulvin (2019, 482) reflect on how analogies of the Aids crisis framed discussions of computer viruses in the 1990s continue to govern how we perceive digital networks and infrastructures: «metaphors and analogies do cultural work: explicating a complex idea, communicating and underestimating a problem's severity, building empathy, or assigning stigma by articulating something new to a more familiar object». Metaphors employed to explain new technology, and technology changes, also influence what actions and interventions are acceptable in response (Nardi and O'Day 1999).

Data and data security inspire a variety of metaphors. Data is often compared analogously to extractive industries, market industries, or natural phenomena (Watson 2016; Hwang and Levy 2015; Puschman and Burgess 2014). Data can be mined; data can be an asset; data can move in streams, lakes, and clouds; data can be liquid, solid, or gaseous (Hwang and Levy 2015). In many cases, discussions about data focus so wholly on the nature and quality of the data that human actors are obscured entirely. When human embodiment and action appear absent, responses are necessarily constrained to the technical domain (Stark and Hoffman 2019; Watson 2016). When data systems are «breached», news media and spokespeople often use framing that imbues data with valuable, dangerous, and inexhaustible characteristics. Examining the comparison of cyberspace to the western American frontier, Alfred C. Yen (2003, 1209) explains how apt metaphors are helpful because they «stimulate the imagination, drawing attention to patterns and possibilities that would otherwise have escaped attention». However, metaphors also obfuscate by restricting our perception of a particular phenomenon such that we fail to question our vantage point (Lapointe 2011, 17). As these metaphors become normalized, they stand in for reality and are applied as the foundation for future beliefs and actions (Yen 2003, 1209).

Deciphering how language is used to prioritize certain understandings of the world and suggest responses, as well as who is dictating these understandings, is critical. The metaphors at play can obscure key political, social, cultural, and economic assumptions if we lose sight of the processes and practices behind data breach narratives. In turn, knowledge about cybersecurity is produced, circulated and legitimized through how it is discussed and represented. Like cybersecurity, the data breach is simultaneously a technical and cultural formation, with significant consequences for the political responses that arise from it (Stevens 2020).

3. Methods

Our data sample consists of primary sources from a wide range of international events and publications. We gathered our documents using the Dow Jones search engine Factiva. While primarily a business news database, Factiva is a global archive for newspapers, trade journals, blogs, and websites. We chose Factiva for its expansive, international coverage that could yield relevant results for data breach cases and geopolitical crises. The research team developed a framework for identifying key terms and phrases. For a given case study, we combined search terms like («MyFitnessPal» and «data breach»). When filtering results, we limited the date range to a year of the public release of information about a data breach. From the results, we examined the five sources that published about a given case most frequently in the specified year. Our sources regularly included publications such as the Associated Press, Bbc, and «The New York Times», though with some case studies, we did incorporate other international and local news sources when relevant and available. While many sources are renowned in journalism, the reputability of sources was not our primary aim since understanding media discourses necessarily includes a variety of views. The number of results for a given topic varied. We then filtered each publication's results by relevance. Each search considered the full text of the newspaper articles, and relevant sources were then further examined by researchers manually to ensure that each article was primarily about the given case, contained enough information for analysis, and was not a republish of another source. We collected 5 articles from each source that best captured these criteria. In total, we have worked with 320 primary sources. For the three primary cases in this paper, our sample is 30 sources.

The research team approached data collection and analysis in a two-fold manner. First, for every data breach case, summaries were written for each primary source, along with a summative or higher-level narrative for every case, which noted descriptions and metaphors used to qualify the following categories: perpetrators, breach framing, perceived risk, victims, and data. Second, we entered observations into an excel spreadsheet, tracking the language and expressions used to describe the victims and perpetrators, the breach, the data compromised, and the crisis framing. We identified a geopolitical security crisis companion case for every data breach within the same year. For each companion case, we found primary sources and analyzed those sources in the same manner as the data breach cases. Some framing categories shifted by necessity; for instance, many companion cases did not specifically discuss a breach or data. Instead, we noted a case's incident framing and removed the category for describing data and breach framing.

Because the project seeks to critically understand the layered contexts of circulation through which the term data breach signifies and how the term is used and understood, we used manual rather than automated methods to collect primary sources. The manual collection of sources advances and provides us with a more nuanced understanding of the interconnections between and across sources.

Critical discourse analysis was employed to analyze the primary sources. We focused on words and phrases containing ideological associations and metaphorical content in framing security crises (Gill 2000). Critical discourse analysis was used to identify the values, beliefs, and assumptions communicated in and across the cases. Although we approached the analysis in pairs by coupling a data breach case with a geopolitical security crisis within the same year, we sought to understand the «creation and composition» of data breaches as security crises in conjunction with «connective and collective political effects» of the framing of security realities more broadly (Liebetrau and Christensen 2021, 34). Because our aim with the larger project is to consider how data breaches are constituted as security crises and how this framing connects to the social, political, and historical contexts in which they circulate (Jancsary *et al.* 2016; Jiwani and Richardson, 2011; Van Dijk 2011), discourse analysis is a viable method to tease out how technology and technological phenomena like the data breach is discursively constructed. It is through an analysis of normalized technologies that constellations of social and political forces are revealed (Roderick 2018).

4. Case studies

The following cases represent only 6 of the 32 we analyzed as part of the larger project. These pairings include the 2007 Tjx companies data breach and the fourth Intergovernmental panel on climate change report (Ipcc), the 2013 Yahoo data breach and Edward Snowden Nsa disclosures, the 2018 MyFitnessPal data breach and the Gatwick drone incident. We chose these pairs because each is anchored approximately 5 years apart across the 15 years of the project. Furthermore, the pairings encompass heterogeneous sets of security crises in terms of data breaches and geopolitical crises.

Our analysis centers on how data breaches are construed as crises through news media. However, we do not aim to define the breach through these representations or track discursive changes over time. We consider these discourses of security crises as examples of what Michel Foucault (1972, 1978) described as normalizing discourses. By constellating a range of technical and non-technical security crises, we examine what needs to be kept in place to make or produce the data breach a security crisis. As we argue, data breaches are not strictly technological phenomena. How data breaches are produced, negotiated and managed as security crises emerge from a matrix of meaning from the culture in which they are produced (Helmreich 2000, 474).

Tjx companies data breach and the fourth intergovernmental panel on climate change report

In the early months of 2007, it was revealed that an estimated 45 million Tjx customers had their data accessed through the covert installation of malicious software on an employee's computer (Npr 2007; «New York Times»

2007). Information like driver's licenses, credit card numbers, social security numbers, and personal addresses were among the most sensitive data stored in the Tjx company computer systems. At the time, the Tjx breach was considered one of the most significant data breaches in history (Swartz 2007), with some news coverage directly comparing it to the massive Card systems solutions breach in 2005 (Vijayan 2007). Both breaches and their ensuing investigations revealed an «arcane and sensitive» set of processes (Associated Press 2005) that suggested a reactive system of approaches to mitigate damage rather than a system of proactive measures meant to offer robust protection.

More broadly, news coverage of the Tjx breach revealed the company's missteps and misdirections as entities that collect and store data and grapple with the growing prevalence of data (in)security. Not only was Tjx inexplicably unaware of the breach for at least two years («New York Times» 2007), but an investigation conducted by the Office of the privacy commissioner of Canada (Opc) revealed that the company was negligent and misrepresented their data safeguarding efforts (Kerner 2007; Opc 2007). Contrary to this finding, the way the breach was most frequently reported conveyed a distinct effort to shift the burden of responsibility to actors outside the company, namely the credit card companies, banks, and those who gained unauthorized access to the data.

The use of loaded language informed how the Tjx breach and its fallout were communicated to consumers. Terms like «data thieves», «intruders», «injustice», and «criminal groups» are rooted in legal understandings of «breach» and advance a narrative of victimhood rather than accountability. This elides a more prudent interpretation of such language, in which the companies tasked with safeguarding data are more accurately understood as responsible «protectors». However, as affected consumers were to understand it, the «breach» that occurred was not a breach of trust nor a breach of duty. Indeed, this was merely an inevitable flaw of a system that could not keep up with the advancements of techniques used to breach them. As such, efforts by the company and investigative authorities to remedy the situation were primarily directed toward the banks and credit card companies «victimized» by being burdened with remunerating customers and identifying the anonymous perpetrators who hid behind sophisticated software.

The often-overwhelming sense of inevitability ascribed to data breaches is a theme shared in North American public discourses about the climate emergency. Following the publication of the Intergovernmental panel on climate change's (Ipcc) scientific report on April 6, 2007, the public response to the report became one of the first punctuating moments of the West's collective reckoning with climate change. Both a paralyzing fear and a hardened denial were inflamed by the proliferation of partisan media, cultural commentary, and special-interest lobbying – all of which produced conflicting narratives of environmental change.

Further, 2007 saw a turn in corporate messaging toward minimizing individual carbon footprints – a manifestation of the rise of so-called 'green marketing' – and a surge of environmental awareness in popular news and entertainment media (Widger 2007; Leonidu *et al.* 2011). Political and corporate entities were at once staunch in their refusal of the severity of climate change (and their responsibility for the most egregious contributions), and yet took advantage of the moment's uncertainty to capitalize on the moral panic that emerged in the wake of the Ipcc report's publication.

These socio-cultural circumstances would situate a once scientifically rooted debate as one that was now part of a growing culture war (Hoffman 2012) that engendered a deep-seated divide in North American society regarding how to address climate change. Indeed, an increasing North American skepticism would become a prominent feature of the cultural zeitgeist of 2007 (Capstick *et al.* 2015), fuelling doubts about the factual certainty of the Ipcc report's claims. Within this frame of public understanding, discourses of crisis – embodied in terms like «unequivocal», «grim», and «sobering» – infrequently emerged across national and regional news sources. In particular, the term «unequivocal» would be presented dichotomously: either as a direct quotation used to convey the gravity of the report's findings (Associated Press 2007) or in a facetious manner expressing the «hysteria» of the authors' assertions (Buchanan 2007).

The Yahoo data breach and Edward Snowden Nsa disclosures

The Yahoo breach of 2013 was the largest-ever theft of personal data and one of the largest data hacks on a single entity. The full extent of the breach was revealed in 2016 during American wireless network operator Verizon's prospective acquisition of the web services provider, three years after the data breach occurred. While initially believed to impact over one billion users, the Yahoo breach was later revealed to affect all three billion users on the platform (Perlroth 2017). Although cybersecurity failures and data mishandling have become commonalities for Yahoo, a data breach to this scale was not unforeseen.

In the year prior (2012), over 450,000 Yahoo user login credentials (emails and passwords) were leaked due to the provider's outdated cybersecurity practices. The significantly smaller breach was undertaken by a hacker group known as D33ds. As the breached data was stored in plaintext instead of an encrypted format and failed to meet cybersecurity standards, the group claimed that they hoped their breach would be a «wake-up call» for Yahoo and its server's various vulnerabilities (FitzGerald 2012). Similarly, the more significant 2013 breach also exploited Yahoo's cybersecurity vulnerabilities to gain access to information on the platform. Instead of hacking login credentials like in the previous breach, in 2013, hackers used Yahoo's software to forge small blocks of data called cookies to gain access to user accounts. Through this process, unauthorized third parties were able to «more convincingly impersonate another user» on the platform and trick Yahoo's system into allowing hackers access (FitzGerald 2016).

Thus, given Yahoo's history of breached information, much of the 2013 breach coverage references the provider's previous cybersecurity failures. Articles reporting on the breach cite third-party security professionals who provide their expert opinions on Yahoo's security standards, notably Yahoo's failure to meet best practices of the sector and encouraging users to consider switching to a safer provider (Dow Jones News Service 2012). Coverage of both the 2012 and 2013 Yahoo breaches outlined user security best practices to keep personal information protected, despite the fact that these breaches were server security issues that could not be altered by individual user practices and point instead to Yahoo's systemic vulnerabilities. Furthermore, terms like «impersonation», «intruders», «theft», «tricking», «phishing», and «cyber-attack» situate the breach as not only a large-scale attack on Yahoo user data but also indicate the possibility of acquired data being used to gain further access elsewhere.

As Yahoo's 2013 breach made vulnerable user information such as names, email addresses, telephone numbers, dates of birth, hashed passwords, security questions and their associated answers, coverage of this breach heavily considered how hackers could use this information to gain access to «more lucrative information» on the internet such as banking information, as well as the value of access to large amounts of personal data to support phishing schemes (Goel and Perlroth 2016). Furthermore, anxieties of identity theft, phishing schemes, and espionage were of key consideration throughout the breach's coverage, with language such as «impersonation», «information warfare», and «data as a weapon» situating the breached data's potentially dangerous usage throughout mainstream news coverage.

Anxieties of personal data protection, mass surveillance, and government secrecy were further catalyzed by computer intelligence consultant Edward Snowden's Nsa surveillance program disclosures in June of 2013. Snowden, a previous Nsa contractor, revealed that global surveillance programs being undertaken by the United States Department of Defense's intelligence agency were collecting the phone, location, and internet records of unknowing and nonconsenting citizens. He exposed the American security program Prism, which collected user data from tech giants such as Yahoo, Microsoft, Facebook, and Google under government request and Muscular, a European-based program which accessed Us data from outside the country to avoid judicial oversight allegedly (Gellman 2013). In his disclosures, Snowden argued that through programs like *Prism and Muscular*, the Us's «massive surveillance machine» was secretly exploiting the public through mass data collection. In an interview with the «Guardian», Snowden states that the motive behind these disclosures was to inform the public about the Us government's role in «destroy[ing] privacy, internet freedom and basic liberties for people around the world» (Greenwald *et al.*, 2013).

The disclosures engendered public scrutiny surrounding government surveillance, especially Americans' lack of privacy and consent to data usage. The coverage of Nsa disclosures included the terms «internet freedom», «secret surveillance», «public oversight», «information dominance», and «government surveillance programs» often disparaging the need for such government oversight, especially when citizens are non-consenting. With these considerations in mind, various articles within the Snowden coverage encouraged more ethical considerations of personal data. Although, this was also met with reports that questioned Snowden's creditability and justified the U.s. government's need for surveillance to combat terrorism post-9/11.

Mainly, advocacy for ethical data collection is reflected in Snowden's denouncement of the Nsa's actions, interrogating how much power and information government entities are and should be entitled to. The disclosure of Nsa surveillance programs to the greater public brought on cultural anxieties about the accessibility of personal data and whether the Us government's bulk accessing personal data without disclosure is unconstitutional. Snowden's whistleblowing and public response to the disclosures prompted a reform of the Nsa and Fbi through the 2015 creation of the Us Freedom act. The Freedom act modified provisions from the previous Patriot act enacted shortly after the September 11, 2001 attacks and claimed to provide law enforcement with investigatory tools in response to terrorism. However, research by the American Civil Liberties Union found that in 2015, the Patriot act was more frequently enacted to collect phone, computer, credit, and banking history in money laundering, immigration, and fraud (American civil liberties union, n.d.). Through the Patriot act, programs like Prism and Muscular were able to justify the collection of mass amounts of American telecommunications records with little to no grounds for investigation (Bradford 2019). Coverage of the Nsa Surveillance programs unquestionably shifted global understandings of data breaches from initially low-stake hacking of passwords and email accounts to much more sinister realities of impersonation, state surveillance and the destruction of privacy and liberty.

MyFitnessPal data breach and the Gatwick drone incident

In late March of 2018, MyFitnessPal, a popular website which tracks diet and exercise, disclosed a breach which affected all 150 million users. Athletic apparel company Under Armour, which owns MyFitnessPal, indicated that financial information was not compromised in the breach. Though a class-action lawsuit was launched, alleging corporate negligence in handling personal data, Under Armour denied any responsibility for the breach. Despite the large number of users affected, there was relatively little news coverage of this breach. Coverage was frequently positive towards Under Armour, praising the company's quick disclosure and «well-oiled» response plan (Mirza 2018). However, other coverage indicated that Under Armour «dropped the ball» in encrypting passwords using the «notoriously hackable» Sha-1 function (Yedioth Ahronoth 2018). As the breach occurred just weeks before the implementation of the Eu's Gdpr policy, the incident was frequently discussed in Uk-based press as an illustration of the need for better data protection through regulatory mechanisms.

The type of language used across the coverage varies. The most sensationalistic language is seen in articles that use the breach to promote cybersecurity software: «hackers», «data» «stolen», and «highly» personal information compromised (Kilpatrick 2018). Some sources advise individuals to better protect their data by using strong, unique passwords. Several of our breach cases show this individualization of a systemic problem. Many sources use neutral terminology such as «data associated» with user accounts, access by an «unauthorized party», or information «acquired» or «compromised». These terms align with the standardization of language associated with coverage of data breaches seen around the mid-2010s. While this level of standardization may result in more accurate terminology and less sensationalistic coverage, it may also conceal culpability, contributing to the sense of inevitability and unpreventability that largely shields corporations from accountability as stewards of personal information.

The Gatwick drone crisis more overtly betrays anxieties about the expansion of technology. While coverage of the MyFitnessPal breach conceals some of the most salient concerns about the commodification of information, the frantic and fast-paced Uk-based coverage of the Gatwick incident is intensely anxious. In December 2018, two drones were spotted above the airfields at Gatwick airport in London, affecting 1000 flights over three days and fuelling unfounded speculation about terrorism, drug smuggling, and a «lone-wolf eco-terrorist» (Mendick and Hymas, 2018) protesting plane travel. Much of the coverage uses sensationalistic language: «malicious act», «criminal activity», «chaos», and «mayhem», «rogue devices», «abuse» of technology, and airspace «violated». The drones are explicitly identified as a threat and Gatwick as vulnerable. The contrast in the language used in the MyFitnessPal and Gatwick incidents indicates that one is a newly emerging threat. At the same time, the other's risks have been normalized and absorbed into our lives.

Despite the massive response of the press, law enforcement, and politicians, the Gatwick incident's only impact was the disruption of 140,000 passengers' holiday travel plans. While this disruption was significant, the safety and security threats emphasized in the substantial press speculation never materialized. The perpetrators were never found, nor any motive established, despite the deployment of extensive police and army resources. The volume of coverage was immense, with the incident reported by reputable news sources and the British tabloid press. Aside from the sensationalistic speculation, the coverage emphasizes safety concerns such as drones colliding with aircraft. Whether the risks identified are speculative, extreme, or mundane; the coverage indicates widespread anxieties about technological developments outpacing regulation. Many sources discuss the lack of control governments can exert over drones – and, more broadly, airspace – and the difficulty in enforcing existing regulations. Drones then emerge as an exemplar of modern anxieties over new technologies in general; they pose a variety of (real or imagined) safety and security threats, are challenging to control and regulate and can be relatively quickly and inexpensively purchased.

Further cultural anxieties are grafted onto the incident as it represents a general unease with that which cannot be contained. It is not difficult to imagine the link between the uncontrolled penetration of new technologies into British airspace and the upswing in xenophobia and anti-immigration sentiment in the Uk following the 2016 Brexit vote. Politicians from all parties, the British pilots' union, and journalists all expressed a need for greater regulation and emphasized how rapidly the drone market has expanded in recent years.

Many articles, particularly those published in the tabloid press, call for an expansion of law enforcement to deal with the threat of drones. Though the coverage emphasized the lack of avenues available to law enforcement to stop the drones, and officials failed to identify the perpetrators, this is nonetheless considered a necessity. The volume of police and military officers involved in unsuccessful efforts illustrates that security theatre may expand the reach of law enforcement. Although none of the imagined dangers posed by the drones materialized, the outsize coverage and breathless speculation, combined with the tremendous response by law enforcement, indicate how discourses surrounding the category of «security crisis» may be deployed to contain supposed technological threats, and their concomitant ideologies, through essentially conservative mechanisms.

5. Analysis

Normalizing surveillance capitalism

Across our case studies from 2005 to present, the risks of data breaches are frequently made tangible by indicating that personal information included in a breach can be used to perpetrate identity theft or financial fraud. There is little consideration that access to personal data may be a risk. The coverage of the MyFitnessPal breach emphasizes that financial data and identification documents were not affected, effectively downplaying the severity of the breach. Individuals are rendered responsible for their data, with the implication that data can be secured at the user's end; this obscures the role of corporate responsibility in data privacy issues and creates a false sense of security. The coverage rarely stresses the particular nature of personal health information being breached, nor is the company discussed as a part of the incredibly lucrative diet industry. Though some of the coverage does raise critical questions about corporate responsibility for data protection, it avoids engaging with the particularities of corporate ownership of personal health data.

Data collected by MyFitnessPal includes body weight and measurements and meals eaten; the website also integrates with other tools such as smartwatches, which may contain more detailed health data like heart rate, exact routes of runs or walks, and user-supplied information about menstrual cycles. The success of the website and its competitors indicates that this type of health information, combined with the pressures of diet culture (see Jovanovski and Jaeger 2022), can be commodified in the information age. As Gidaris (2019) notes, fitness trackers can be used as tools of surveillance under the guise of promoting health and fitness.

How, then, does the breach of this sort of data further extend the mandate of surveillance capitalism (Zuboff 2019)? Gidaris notes that health insurance companies use data generated by fitness trackers. Data on an individual's health is of great value to the privatized healthcare system and health insurance companies in the United States. This country boasted some 20 million MyFitnessPal users in 2018. The commodification of this information is congruent with a system in which health comes at a cost. While some articles indicate that

MyFitnessPal and Under Armour should take greater responsibility for the lax security measures resulting in the breach, they do not explore the implications of this particular type of personal information breach.

Correspondingly, public understandings of the Tjx breach were inextricably shaped and tempered by discourses of «crisis» in North American media in the early 2000s. In the case of the Tjx breach, by framing the act of installing malicious software as an act of criminality that could not otherwise have been prevented, the company advances a narrative of inevitability and avoids accountability to the consumer. Moreover, the assumptions made about the inevitability of data breaches are analogous to how the public understands the «breach» of environmental thresholds laid out in the 2007 Ipcc report. By shifting responsibility for robust preventative measures and attempting to relegate most of the damage control to external actors, Tjx and companies like it have almost universally maintained impunity. These companies fail to acknowledge that the ways consumers are encouraged to protect their data become irrelevant when the entities who collect and store that data fail to follow even the basic minimum level of security protocols.

As a phenomenon, data breaches can be difficult to grasp, compounded by how these events are presented as exceptional to the ordinary function of networks (Zeffiro 2022). This supposition is invested in the belief that networks are secure and securable. When a data breach occurs, the network or system is rendered insecure, and the focus is on restoring it to its normalized secure state. Scholars exploring arcane computer network vulnerabilities have gestured toward the inherent contradictions of the aspiration toward security. Writing on how the computer virus is an expression of informational capitalism, Jussi Parikka (2005, 9) explains how in the context of a risk society, security is not something within reach, «but only a shifting horizon, or a limit, which can be approached». Similarly, Tony Sampson (2007, 1) observes how, «the hypothetical robustness of the network, which purportedly emerged from its highly redundant distribution and random connectivity, is countered by increasing network vulnerability». Network vulnerabilities, as Sampson (2007, 2) argues, are an anticipated emergent property that undermines the assumed durability of digital networks.

We also observed how discourses of vulnerabilities could change during the coverage of a data breach event when pervaded by external security crises. For example, whereas the 2012 Yahoo breach coverage mainly focused on Yahoo's security failures and vulnerabilities, cybersecurity experts analyzing the 2013 breach argue there are dark web and even political espionage possibilities for criminals looking to monetize the breached data (New Vision 2016). Within the two Yahoo case studies, comprehension of how users related to and are affected by personal data breaches also shifted. In 2012, much of the Yahoo coverage focused heavily on the usernames and passwords breached and failed to address the users to whom the accounts and personal data belong. Whereas in 2013, the notion that personal data is only used to gain access to low-stakes online accounts is virtually diminished. Instead, the post-Snowden coverage situates data as valuable, dangerous, and inherently political.

How data breaches are purported as security crises contradict the fundamental vulnerability of ubiquitous networked computing. The data breach, construed as abnormal, perpetuates the false assumption that the 2.5 quintillion bytes of data produced every day through a plethora of devices and physical objects over the Internet or other communications networks are inherently manageable, governable, and controllable. This is a crucial normalizing discourse because it upholds the conditions of surveillance capitalism (Zuboff 2020). As an economic system, surveillance capitalism hinges on extracting and commodifying personal data through the enticement of endless information and limitless ways for needs to be met through predictive modelling (p. 13). The coverage of these breach cases contributes to the concealment and, ultimately, the normalization of crucial mechanisms of information and surveillance capitalism and the expansion of datafication (Van Dijck 2014) into our daily lives.

The hegemony of security crises

Across the 32 cases of the larger project, we have observed how translating security crises largely relies on metaphors, analogies and cognitive hooks that can seize the broader public (Gjesvik and Szulecki 2022). This paper's small sample of cases illustrates different features of security crises. Nevertheless, we discern a hegemony of security crisis in how an increasing number of complex and interlocking issues are redefined in terms of an abstract and universalizing understanding of security crises (see also: Ensmenger 2012, 766) entrenched in analogies tied to national security and defence rhetoric.

In the Gatwick drone incident, drones are elevated as a type of new technology that carries physical and ideological threats to the nation. Discourses of security, safety, and regulation of new technologies were at the forefront of news coverage, using strong language to indicate an imminent threat rather than downplay crisis. A generalized fear of insecurity is contained by manufacturing a coherent, narrativized security crisis, onto which other cultural fears may be projected and managed. These discourses obscure underlying anxieties, such as fear of uncontrolled migration, while uncritically emphasizing law enforcement as a solution to real and imagined threats. The creation of the threat justifies an increase in security mechanisms, particularly those related to law enforcement and surveillance. The crisis, then, represents a mostly imagined threat to British sovereignty while manufacturing and concealing the real threats of over-policing and the extension of surveillance culture.

In the larger sample of cases, data breaches are commonly framed as technological crises in ubiquitous networked systems that result from bad actors exploiting or violating vulnerabilities in systems and exposing sensitive information (Cimpanu 2019; DeGroot 2020; Dns Stuff 2020; Ropek 2020; Sobers 2020; Swinhoe 2020). The potential threats are identified as malicious actors and adversary infrastructures. In contrast, counter-intelligence measures like threat hunting, penetration testing and threat intelligence are identified as potential measures to prevent breaches and mitigate insecurities (Cybersecurity & Infrastructure Security Agency 2020; Threat Connect, 2019; Vazquez 2020).

Discourses of cybersecurity and national security are increasingly difficult to separate. The coverage of the 2013 Yahoo Breach and the Snowden Nsa disclosures prompted mainstream concern surrounding the danger of personal data utilization by unsanctioned third parties. For example, in comparison to the more significant 2013 breach, Yahoo's 2012 breach coverage focused more on password protection and internet safety. Alternatively, the 2013 breach coverage is much more cognizant of data's potentiality, suggesting that the over three billion user credentials could be a vital tool in «industrial or state espionage» (New Vision 2016). Snowden's revelations that telecommunications records from tech giants, including Yahoo (Gellman, 2013), were being utilized to support American surveillance programs without their knowledge or consent could have informed these responses. In 2013 post-Snowden, we see the incorporation of claims that massive data collection could have been «state-sponsored» and «an espionage stage of an information warfare effort» (Chandler 2016).

More recently, on the cusp of the 2020 Us Presidential Election, for example, Cyber Risk Security (2020, 6) released its third quarter data breach report that emphasized: «cyber threat actors» as the «neglected threat» that «looms over the Us election». Following the investigation into the Equifax breach, which saw the United States Department of Justice's indictment against four members of China's People's Liberation Army, in a news briefing about the indictment, Attorney General William Barr used the occasion to «remind the Chinese government that we have the capability to remove the Internet's cloak of anonymity and find the hackers that nation repeatedly deploys against us» (Department of Justice 2020). This example demonstrates how processes of othering in establishing threats and objects to be protected (Gomes and Marques 2021), identify risks and threats, while evading discussion of the infrastructure and policies that permit widespread surveillance without consent (de Matos 2015; Thornborrow 1993).

Thierry Balzacq and Myriam Dunn Cavelty (2016) explain how in instances where there is a disruption to the stability of cybersecurity, the issues are made geopolitically relevant and more easily linked to enemy «others» (Balzacq and Cavelty 2016, 196). As Balzacq and Dunn Cavelty further reflect, «this type of politics is about the establishment of territoriality and borders in the virtual realm, about nationally owned space and a nationally definable space, based on physical infrastructures» (Balzacq and Cavelty 2016, 196). Indeed, how the Equifax breach is framed interlocks with the Trump administration's «inventory of risk consciousness» (Sandwell 2006, 39), which leveraged broader public anxieties and fears to grant legitimacy to a particular range of white supremacist reactions, such as when Trump tweeted about Covid-19 as «the Chinese virus», stoking xenophobic fears and anti-Asian racism (Hswen *et al.* 2021). Lucas Guerra (2021, 33) understands how whiteness and security both share a crucial common ground: «They entail a (right to exclude) – that is, to define those who enjoy the white privilege of being secured and those from whom one should be secured».

Discourses of security crises elucidate events in specific ways and constitute audiences in discourse by drawing boundaries around the «we» on whose behalf they claim to speak and the «you's» who are simultaneously addressed by linking fears and threats to «feelings, needs and interests» (Balzacq 2005, 184; Hensen and Nissenbaum 2009, 1165). Arun Kundnani and Deep Kumar (2015, 4) examine how the debate on national security surveillance that emerged in the United States following Snowden's disclosures was

> woefully inadequate, due to its failure to place questions of race and empire at the center of its analysis. It is racist ideas that form the basis for the ways national security surveillance is organized and deployed, racist fears that are whipped up to legitimize this surveillance to the American public, and the disproportionately targeted racialized groups that have been most effective in making sense of it and organizing opposition.

While the initial coverage of Snowden attracted sustained international coverage, months later, when it was revealed how the specific targets of Nsa surveillance placed under surveillance were prominent Muslim Americans despite there being no reasonable suspicion of any involvement in criminal activity, the stories scarcely registered in corporate news media (Kundnani and Kumar 2015). Deciphering how the «"we" – as the "subject" of security – is constructed through discourses of danger and safety», Maria Stern (2006, 188) identifies a «security paradox»; that any definition of security produces the subject to be protected, as well as producing the related harm, fear, and danger. For the subject of security to be "securable," it must be contained and named with contours dividing the included from excluded, marking that which is to be made secure from the dangerous "others" (Stern 2006, 192). In turn, the formation of a securable subject also stems from a notion of «good citizenship», which is an entitlement of Western and white privilege.

6. Conclusion

Data breaches can have profound geopolitical consequences. Nevertheless, how data breaches are made intelligible by cybersecurity rhetoric and mainstream media affects what the term data breach signifies as a security crisis, and how it is used and understood. We argue that data breaches cannot be understood as strictly technological phenomena. The 2007 Tjx companies data breach and the fourth Intergovernmental panel on climate change report, the 2013 Yahoo data breach and Edward Snowden Nsa disclosures, and the 2018 MyFitnessPal data breach and the Gatwick drone Incident reveal how security crises are discursively constituted and normalized. When a data breach is construed as a crisis of security, it is most often framed by a paradoxical normative assumption about ubiquitous computing as being simultaneously vulnerable and governable. The maintenance of this contradiction as a standard of data breaches normalizes the security crisis.

Ultimately, the aim of our article is to uproot the stability of data breaches by moving these events outside the logic of the hegemony of security crisis and the normalization of surveillance capitalism to reframe the crises. Because this is our first articulation of the larger project's findings, our contribution is experimental in the sense that it is not meant to be exhaustive or reveal a «truth». Rather our aim is to establish a foundation for further research on data breaches. Could a critical parsing of the stability of the data breach as a security crisis encourage alternatives to how personal data is collected, managed, commodified, in/secured, and weaponized? By decoupling an understanding of data breaches from purely technical systems in order to understand how data breaches correspond to other security crises within social and political constellations, we advance an examination of how dominant cultural understandings of data breaches as security crises are reproduced by and provoke a «matrix of domination», which includes but is not limited to white supremacy, heteropatriarchy, colonial capitalism, and the coloniality of knowledge (Collins 1990; Chock 2019). How data breaches are construed and understood as crises have profound implications for related issues like data privacy, data protection, and ubiquitous surveillance are contextualized, materialized, and translated into policy and practice.

References

American Civil Liberties Union (n.d.), *Surveillance under the Patriot Act*, https://www.aclu.org/issues/national-security/privacy-and-surveillance/surveillance- under-patriot-act (last accessed on 15th December 2022).

Ashenden, D. (2021), *The Future Human and Behavioural Challenges of Cybersecurity*, in P. Cornish (ed), *The Oxford Handbook of Cybersecurity*, Oxford, Oxford University Press, pp.723-734.

Associated Press (2007), *Tjx Says Theft of Credit Data Involved 45.7 Million Cards*, «New York Times», 30 March, https://www.nytimes.com/2007/03/30/business/30data.html.

Balzacq, T. and Cavelty, M. (2016), *A Theory of Actor-Network for Cybersecurity*, in «European Journal of International Security», 1(2), pp. 176-198.

Boholm, M. (2021), *Twenty-five Years of Cyber Threats in the News: a Study of Swedish Newspaper Coverage (1995–2019)*, in «Journal of Cybersecurity», 7(1), doi: 10.1093/cybsec/tyab016.

Bradford Franklin, S. (2019), Fulfilling the Promise of the Usa Freedom Act: Time to Truly End Bulk Collection of Americans' Calling Records, Just Security, https://www.justsecurity.org/63399/fulfilling-the-promise-of-the-usa-freedom-act-time-to-truly-end-bulk-collection-of-americans-calling-records (last accessed on 14th December 2022).

Buchanan, P. J. (2010), *Global Warming: Hoax of the Century*, in «Human Events», 66(9), pp. 15.

Burgess, J. (2012), *The iPhone Moment, the Apple Brand the Creative Consumer*, in L. Hjorth, J. Burgess and I. Richardson (eds), *Studying Mobile Media: Cultural Technologies, Mobile Communication, and the iPhone*, London, Routledge, pp. 28-42.

Cap, P. (2017), *The Language of Fear: Communicating Threat in Public Discourse*, London, Palgrave Macmillan.

Capstick, S., Whitmarsh, L., Poortinga, W., Pidgeon, N. and Upham, P. (2015), *International Trends in Public Perceptions of Climate Change over the Past Quarter Century*, in «Climate Change», 6(4), pp. 435-435.

Costanza-Chock, S. (2020), *Design Justice: Community-led Practices to Build the Worlds We Need*, Cambridge (Ma), Mit Press.

Chandler, M. (2016), *Yahoo Hack: Over One Billion User Accounts have been Stolen in Cyber Attack*, «London Evening Standard», 15 December, https://www.standard.co.uk/tech/yahoo-hack-over-one-billion-user-accounts-have-data-stolen-in-cyber-attack-a3420761.html.

Cimpanu, C. (2019), *The Scariest Hacks and Vulnerabilities of 2019*, ZdNet, 28 October, https://www.zdnet.com/article/the-scariest-hacks-and-vulnerabilities-of-2019.

Collins, P. H. (1990 [2000]), *Black Feminist Thought: Knowledge, Consciousness, and the Politics of Empowerment*, New York, Routledge.

Cybersecurity & Infrastructure Security Agency (2020), *Technical Approaches to Uncovering and Remediating Malicious Activity*, https://us-cert.cisa.gov/ncas/alerts/aa20-245a (last accessed on 14th December 2022).

De Groot, J. (2020), *Digital Guardian*, https://digitalguardian.com/blog/history-data-breaches (last accessed on 14th December 2022).

De Matos Alves, A. (2015), *Between the «Battlefield» Metaphor and Promises of Generativity: Contrasting Discourses on Cyberconflict*, in «Canadian Journal of Communication», 40(3), doi: 10.22230/cjc.2015v40n3a2742.

Diamond, S. (1984), *Credit File Password is Stolen*, «The New York Times», 22 June, https://www.nytimes.com/1984/06/22/business/credit-file-password-is-stolen.html.

Dns Stuff. (2020), *What is a Data Breach? Ultimate guide to Cybersecurity Breaches in 2020*, Dns Stuff, 23 August. https://www.dnsstuff.com/data-breach-101.

Dunn Cavelty, M. (2008), *Cyber-Terror. Looming Threat or Phantom Menace? The Framing of the Us Cyber-Threat Debate*, in «Journal of Information Technology & Politics», 4(1), pp. 19-36.

Dunn Cavelty, M. (2013), *From Cyber-Bombs to Political Fallout: Threat Representations with an Impact in the Cyber-Security Discourse*, in «International Studies Review», 15, pp. 105-122.

Dunn Cavelty, M. (2018), *Cybersecurity Research Meets Science and Technology Studies*, in «Politics and governance», 6(2), pp. 22-30

Ensmenger, N. (2012), *The Digital Construction of Technology: Rethinking the History of Computers in Society*, in «Technology and Culture», 53(4), pp. 753–776.

Eriksson, J. (2001), *Cyberplagues, It, and Security: Threat Politics in the Information Age*, in «Journal of Contingencies and Crisis Management», 9(4), pp. 211–222.

Fairclough, N. (1992), *Discourse and Social Change*, Cambridge (Ma), Polity Press.

Fairclough, N. (2010), *Critical Discourse Analysis: The Critical Study of Language*, Harlow, Longman.

Fitzgerald, D. (2012), *Corporate News: Yahoo Passwords Stolen in Latest Data Breach*, «The Wall Street Journal», 13 July, https://www.wsj.com/articles/BL-AMB-3347.

Foucault, M. (1972), *The Archaeology of Knowledge*, New York, Pantheon Books.

Foucault, M. (1980), *Power/Knowledge: Selected Interviews and Other Writings 1972–1977*, New York, Pantheon Books.

Foucault, M. (1978), *The History of Sexuality: Volume I*, New York, Random House.

Gellman, B. (2013), *Edward Snowden, After Months of Nsa Revelations, Says His Mission's Accomplished*, in «The Washington Post», 23 December, https://www.washingtonpost.com/world/national-security/edward-snowden-after-months-of-nsa-revelations-says-his-missions-accomplished/2013/12/23/49fc36de-6c1c-11e3-a523-fe73f0ff6b8d_story.html.

Gidaris, C. (2019), *Surveillance Capitalism, Datafication, and Unwaged Labour: The Rise of Wearable Fitness Devices and Wearable Life Insurance*, in «Surveillance & Society», 17(1-2), doi: 10.24908/ss.v17i1/2.12913.

Gill, R. (2000), *Discourse Analysis*, in M. Bauer and G. Gaskell (eds), *Qualitative Researching with Text, Image and Sound: A Practical Handbook*, London, Sage, pp.172-190.

Gjesvik, L. and Szulecki, K. (2022), *Interpreting Cyber-Energy-Security Events: Experts, Social Imaginaries, and Policy Discourses around the 2016 Ukraine Blackout*, in «European Security», doi: 10.1080/09662839.2022.2082838.

Goel, V. and Perlroth, N. (2016), *Hacked Yahoo Data is for Sale on Dark Web*, «The New York Times», 15 December, https://www.nytimes.com/2016/12/15/technology/hacked-yahoo-data-for-sale-dark-web.html.

Greenwald, G., Macaskill, E. and Poitras, L. (2013), *Edward Snowden: The Whistleblower behind the Nsa*, The Guardian, 11 June, https://www.theguardian.com/world/2013/jun/09/edward-snowden-nsa-whistleblower-surveillance.

Guerra, L. (2021), *Security as White Privilege: Racializing Whiteness in Critical Security Studies*, in «Security Dialogue», 52(1_suppl), pp. 28-37.

Helmreich, S. (2000), *Flexible Infections: Computer Viruses, Human Bodies*, Nation-States, Evolutionary Capitalism, in «Science, Technology, & Human Values», 25(4), pp. 472-491.

Hansen, L. and Nissenbaum, H. (2009), *Digital Disaster, Cybersecurity, and the Copenhagen School*, in «International Studies Quarterly», 53, pp. 1155-1175.

Hoffman, A.J. (2012), *Climate Science as Culture War*, in «Stanford Social Innovation Review», 10(4), pp. 30-37.

Hswen, Y., Xu, X., Hing, A., Hawkins, J.B., Brownstein, J.S. and Gee, G.C.(2021), *Association of «#Covid19» versus «#Chinesevirus» with Anti-Asian Sentiments on Twitter: March 9-23, 2020*, in «American Journal of Public Health», 111(5), pp. 956-964.

Hwang, T. and Levy, K. (2015), *«The Cloud» and Other Dangerous Metaphors,* in «The Atlantic», 20 April, https://www.theatlantic.com/technology/archive/2015/01/the-cloud-and-other-dangerous-metaphors/384518.

Jancsary, D., Höllerer, M. and Meyer, R. (2016), *Critical Analysis of Visual and Multimodal Texts*, in R. Wodak and M. Meyer (eds), *Methods of Critical Discourse Studies*, London, Sage, pp. 180-204.

Jiwani, Y. and Richardson, J. (2011), *Discourse, Ethnicity and Racism*, In T.A. Van Dijk (ed), D*iscourse Studies: A Multidisciplinary Introduction*, London, Sage, pp. 241-262.

Kilpatrick, H. (2018), *150 million MyFitnessPal Accounts Compromised by a Massive Data Breach*, Cso, 9 April, https://www2.cso.com.au/article/635866/150-million-myfitnesspal-accounts-compromised-by-massive-data-breach.

Kitchin, R. (2014b), *The Data Revolution: Big Data, Open Data, Data Infrastructures & Their Consequence*, London, Sage.

Kumar, D. and Kundnani, A. (2015), *Race, Surveillance, and Empire, in «International Socialist Review»*, https://isreview.org/issue/96/race-surveillance-and-empire/index.html (last accessed on 14th December 2022).

Lapointe, A. (2011), *When Good Metaphors Go Bad: The Metaphoric «Branding» of Cyberspace. Center for Strategic and International Studies*, http://csis.org/publication/when-good-metaphors-go-bad-metaphoric-branding- cyberspace (last accessed on 14th December 2022).

Lawson, S. (2013), *Beyond Cyber-Doom: Assessing the Limits of Hypothetical Scenarios in the Framing of Cyber-Threats*, in «Journal of Information Technology & Politics», 10(1), pp. 86-103.

Leonidou, L.C., Leonidou, C.N., Palihawadana, D. and Hultman, M. (2011), *Evaluating the Green Advertising Practices of International Firms: A Trend Analysis*, in «International Marketing Review», 28(1), pp. 6-33.

Liebetrau, T. and Christensen, K.K. (2020), *The Ontological Politics of Cybersecurity: Emerging Agencies, Actors, Sites, and Spaces*, in «European Journal of International Security», 6(1), pp. 25-43.

Lupton, D. (1994), *Panic Computing: The Viral Metaphor and Computer Technology*, in «Cultural Studies», 8(3), pp. 556-568.

Mckinney, C. and Mulvin, D. (2019), *Bugs: Rethinking the History of Computing*, in «Communication, Culture and Critique», 12(4), pp. 476-49.

Mirza, S. (2018), *MyFitnessPal Apparently Has Some Foes; Under Armour Reacts Quickly to Massive Data Breach*, Mondaq Business Briefing, 11 April, https://www.mondaq.com/unitedstates/data-protection/690440/myfitnesspal-apparently-has-some-foes-under-armour-reacts-quickly-to-massive-data-breach.

Mendick, R. and Hymas, C. (2018), *Environmental Protestors Suspected of Orchestrating Gatwick Drone Chaos*, «The Telegraph», 21 December, https://www.telegraph.co.uk/news/2018/12/20/environmental-protests-suspected-orchestrating-gatwick-drone.

Myers, J. and Whiting, K. (2019), *These Are the Biggest Risks Facing Our World in 2019*, World Economic Forum, https://www.weforum.org/agenda/2019/01/these-are-the-biggest-risks-facing-our-world-in-2019 (last accessed on 14th December 2022).

Nardi, B.A. and O'day, V.L. (1999), *A Matter of Metaphor: Technology as Tool*, Text, System, Ecology, in B.A. Nardi and V. O'day, *Information Ecologies: Using Technology with Heart*, Cambridge (Ma), Mit Press, pp. 25-48.

National Public Radio (2007), *Marketplace Report: Tjx Data Breach*, Day to Day, 29 March, https://www.npr.org/templates/story/story.php?storyId=9209541.

New Vision (2016), *Yahoo Hack Shows Data's Use for Information Warfare*, New Vision, 16 December, https://www.newvision.co.ug/new_vision/news/1442179/yahoo-hack-datas-information-warfare.

Nissembaum, H. (2005), *When Computer Security Meets National Security*, in «Ethics in Information Technology», 7, pp. 61-73.

Office Of The Privacy Commissioner Of Canada (2007), *Inadequate Security Safeguards Led to Tjx Breach, Commissioners Say*, 25 September, https://www.priv.gc.ca/en/opc-news/news-and-announcements/2007/nr-c_070925 (last accessed on 14th December 2022).

Parent, M. (2019), *Growth in data breaches shows need for government regulations*, The Conversation, 4 December, https://theconversation.com/growth-in-data-breaches-shows-need-for-government-regulations-127600 (last accessed on 14th December 2022).

Parrika, J. (2005), *Digital Monsters, Binary Aliens–Computer Viruses, Capitalism and the Flow of Information*, in «Fibreculture Journal», https://four.fibreculturejournal.org/fcj-019-digital-monsters-binary-aliens-%E2%80%93-computer-viruses-capitalism-and-the-flow-of-information (last accessed on 14th December 2022).

Perlroth, N. (2017), *All 3 Billion Yahoo Accounts Were Affected by 2013 Attack*, «The New York Times», 3 October, https://www.nytimes.com/2017/10/03/technology/yahoo-hack-3-billion-users.html.

Puschmann, C. and Burgess, J. (2014), *Big Data, Big Questions: Metaphors of Big Data*, in «International Journal of Communication», 8(20), pp. 1690-1709.

Reed, L. (2000), *Domesticating the Personal Computer: The Mainstreaming of a New Technology and the Cultural Management of a Widespread Technophobia*, in «Critical Studies in Media Communication», 17(2), pp. 159-185.

Reisinger, D. (2012), *Worldwide Smartphone User Base Hits 1 Billion*. CNet, 17 October, https://www.cnet.com/news/worldwide-smartphone-user-base-hits-1-billion.

Roderick, I. (2016), *Critical Discourse Studies and Technology: A Multimodal Approach to Analysing Technoculture*, London, Bloomsbury.

Ropek, L. (2020), *Bad Actors Have Adapted Well to the Pandemic Crisis*, Government Technology, 30 April, https://www.govtech.com/security/Bad-actors-Have-Adapted-Well-to-the-Pandemic-Crisis.html.

Ross, A. (1991), *Hacking Away at the Counterculture*, in C. Penley and A. Ross (eds), *Technoculture*, Minneapolis (Mn), University of Minnesota Press, pp. 107–34.

Rushkoff, D. (1994), *Media Virus! Hidden Agendas in Popular Culture*, New York, Ballantine.

Rothschild, E. (1995), *What is security?*, in «Daedalus», 124(3), pp. 52-98.

Sampson, T. (2007), *The Accidental Topology of Digital Culture: How the Network Becomes Viral*, Transformations: Online Journal of Region, Culture and Society, http://www.transformationsjournal.org/journal/issue_14/editorial.shtml.

Sandwell, B. (2006), *Monsters in Cyberspace Cyberphobia and Cultural Panic in the Information Age*, in «Information, Communication & Society», 9(1), pp. 39-61.

Satter, R. (2012), *2nd Update: Yahoo Confirms Theft of Passwords from Users*, 12 July, Yahoo Finance, https://finance.yahoo.com/news/yahoo-confirms-theft-450-000-users-passwords-182147150--finance.html.

Sobers, R. (2019), *107 must-know data breach statistics for 2020, Varonis*, 24 September, https://www.varonis.com/blog/data-breach-statistics.

Stark, L and Hoffmann, A L. (2019), *Data is the New What? Popular Metaphors and Professional Ethics in Emerging Data Culture*, in «Journal of Cultural Analytics», doi: 10.22148/16.036.

Stern, M. (2006), *«We» the subject: The power and failure of (in)security*, in «prio», 37(2), pp. 187-205.

Stevens, C. (2020), *Assembling Cybersecurity: The Politics and Materiality of Technical Malware Reports and the Case of Stuxnet*, in «Contemporary Security Policy», 41(1), pp. 129-152.

Swartz, J. (2007), *Tjx Data Breach May Involve 94 Million Credit Cards*, Abc, 25 October, https://abcnews.go.com/Technology/story?id=3773782&page=1.

Swinhoe, D. (2020), *The 15 Biggest Data Breaches of the 21st Century*, Cso, 17 April, https://www.csoonline.com/article/2130877/the-biggest-data-breaches-of-the-21st-century.html.

Thornborrow, J. (1993), *Metaphors of Security: A Comparison of Representation in Defence Discourse in Post-Cold-War France and Britain*, in «Discourse & Society», 4(1), pp. 99-119.

Threat Connect (2019), *Disrupting Adversary Infrastructure*, https://3hyr133hoba8cg1mqt4pktdd-wpengine.netdna-ssl.com/wp-content/uploads/ThreatConnect-Disrupting-Adversary-Infastructure-Whitepaper.pdf (last accessed on 14th December 2022).

United States Department Of Justice (2020), *Chinese Military Personnel Charged with Computer Fraud, Economic Espionage and Wire Fraud for Hacking into Credit Report Agency Equifax*, https://www.justice.gov/opa/pr/chinese-military-personnel-charged-computer-fraud-economic-espionage-and-wire-fraud-hacking (last accessed on 14th December 2022).

Van Dijck, J. (2014), *Datafication, Dataism and Dataveillance: Big Data Between Scientific Paradigm and Ideology*, in «Surveillance & Society», 12(2), doi: 10.24908/ss.v12i2.4776.

Van Dijk, T.A. (2011), *Discourse and Ideology*, in T.A. Van Dijk (ed.), *Discourse Studies: A Multidisciplinary Introduction*, London, Sage, pp. 379-407.

Vazquez, C. (2020), *The Basics of Threat Hunting,* https://www.linkedin.com/pulse/basics-threat-hunting-carlos-vazquez (last accessed on 14th December 2022).

Vijayan, K. (2007), *Tjx Data Breach: at 45.6M Card Numbers, it's the Biggest Ever*, Computer World, 29 March, https://www.computerworld.com/article/2544306/Tjx-data- breach--at-45-6m-card-numbers--it-s-the-biggest-ever.html.

Wall, D. S. (2008a), *Cybercrime and the Culture of Fear*, in «Information, Communication & Society», 11(6), pp. 861-884.

Wall, D. S. (2008b), *Cybercrime, Media and Insecurity: The Shaping of Public Perceptions of Cybercrime*, in «International Review of Law, Computers & Technology», 22(1-2), pp. 45-63.

Watson, S. (2016), *«Data is the New __»: On the Industrial Metaphors of Big Data*, Dis Magazine, http://dismagazine.com/discussion/73298/sara-m-watson-metaphors-of-big-data (last accessed on 14th December 2022).

Widger, D. (2007), *A Look Back at Green Marketing in 2007*, GreenBiz, 28 December, https://www.greenbiz.com/article/look-back-green-marketing-2007.

Yedioth Ahronoth (2018), *Cyber security lesson brief from the Under Armour Data Breach*, 6 April.

Yen, A. C. (2003), *Western Frontier or Feudal Society? Metaphors and Perceptions of Cyberspace*, in «Berkeley Technology Law Journal», 17(4), pp. 1207-1263.

Zuboff, S. (2019), *The Age of Surveillance Capitalism: the Fight for a Human Future at the New Frontier of Power*, New York, PublicAffairs.

Zeffiro, A. (2022), *Breach, Heliotrope*, https://www.heliotropejournal.net/helio/breach (last accessed on 14th December 2022).