Computer and Information Science; Vol. 14, No. 3; 2021
ISSN 1913-8989 E-ISSN 1913-8997
Published by Canadian Center of Science and Education

Targeting Reputation: A New Vector for Attacks to Critical Infrastructures

Giampiero Giacomello[1], & Oltion Preka[1]

[1] Department of Political and Social Sciences, University of Bologna, Bologna, Italy

Correspondence: Giampiero Giacomello, Department of Political and Social Sciences (DSPS), Strada Maggiore 45, 40125 Bologna, Italy.

Received: June 9, 2021 Accepted: July 8, 2021 Online Published: July 28, 2021

doi:10.5539/cis.v14n3p63 URL: https://doi.org/10.5539/cis.v14n3p63

Abstract

A substantial portion of critical information infrastructures in advanced economies comprises former public utilities, which in the 1980s/90s were fully or partially privatized, a change justified mainly on economic efficiency grounds. This entailed that these utility companies had to compete in the free market, thus being exposed to the same risks/opportunities as private companies. Much like businesses in other industrial sectors, utility companies have increasingly joined social media over the last decade, as 'digital' visibility through social networking platforms, such as Facebook, Twitter, and Instagram has become fundamental. The new (privatized) utilities have relied on marketing and ad campaigns to promote their business and generate revenues. Trust and reputation for companies are primary resources to attract new customers and/or keep old ones, especially for companies with a wide customer base. Trust and reputation are difficult assets to preserve on social media, as they can be subject to negative attacks, including fake campaigns. This paper is a *probe* that explores a potential attack vector to critical infrastructures via weakening customer and investor trust in (the now private) utilities by blemishing CII-utilities' reputation on social media. More specifically, the paper considers the possibility of attacks that have the potential to undermine the stability and reliability of critical infrastructures and advances a preliminary justification of why that may happen. We do this by looking at cases in which negative social media campaigns with fake content have been successfully implemented via digital tools.

Keywords: critical information infrastructures, digital tool, fake news, hacktivism, information operations, protest campaigns, social media

1. Introduction

Critical infrastructures are the 'arteries and veins' of complex, advanced societies, without which, it would be quite impossible for them to function and their economies to thrive. Essentially, this is the reason why they are defined as critical (Cohen, 2010). Adding a further layer of complexity, these systems and assets are now operated, managed and/or controlled via computer networks and information flows. Therefore, they have become critical *information* infrastructures (CII) (like adding the 'nerves' to the 'arteries and veins') and for this reason, we now talk of 'cyber-physical systems'.

Public utilities, i.e., the production and distribution of energy, water, gas, much like banking, emergency services, transportation and the like, are now fully managed and remotely controlled via CII. As large and complex systems, CII are also prone to catastrophic effects if they break down (Metzger, 2004). Any major disruption of the CII-utilities would indeed have serious consequences on the well-being and wealth of the people affected. Power outages or flight delays are moderate manifestations of such an outcome, which could be aggravated by several orders of magnitude. Moreover, a failure in any of the CII-utilities would likely send negative 'ripples' to other systems, thus creating a cascading disaster (see for example Sanger, Krauss and Perlroth, (2021)).

In the mid-1970s, the wisdom of retaining state-owned companies began to be questioned, and economists and policymakers alike looked for possible alternatives. The answer was 'privatization', that is, the ceding of state functions and/or assets, in full or in part, to private actors (Brendan, 1993; Donahue, 1989). U.S. Telecom companies were the first to change. Since then, there have been many organizational variants in privatization, but management through market mechanisms and a commoditization of services have been the common denominators (Almklov & Antonsen, 2010). In the ultimate 'corporatization of the public sector' (Sheil, 2000), even traditionally 'boring' utility companies had to become profit-making assets, with shareholders, board of

directors, market value and even corporate reputation. Business models, including brand management, 'social commerce', strategic communications and customers' relations, had to be applied even within the utility industry as they were now fully part of the market, and in the contemporary era, no place is more important for such activities than social media: Facebook, Twitter, Instagram, TikTok and the like.

Research on cybercrime has shown that cyber-attacks damage companies not only directly from data and time loss, but also from losses in market value and reputation (K.T. Smith, M. Smith, & L.J. Smith, 2011). This outcome, one such studies concludes (K.T. Smith, A. Jones, L. Johnson, & L.M. Smith, 2019), 'is a serious concern to company managers, financial analysts, investors and creditors.' If the targeted companies of such attacks are in the utility industry, it could become a concern for users who may start doubting the safety and the wisdom of relying on such a company (e.g., Cedergren, Lidell & Lidell, 2019).

This work explores the potential of a novel *attack vector* against the utility industry. The rest of this paper is organized as follows: after Section number 2 on the method adopted, in Section number 3and 4 we discuss the importance of corporate reputation on social media for CII-utilities and why the latter can be attacked on social media as part of strategic information operations (IO). In Section number 5 we provide some examples and data of campaigns aimed at damaging companies and why they matter. Finally, in Section number 6 we focus on how these attacks could become tools of a broader strategy to weaken national CII-utilities.

2. Method

As anticipated above, this is a *probe* into the dynamics of why utility companies' cyber-physical infrastructures may be vulnerable to orchestrated, adverse campaigns via social media. Today, for public utilities, much like other businesses:

a) corporate reputation has become a valuable asset for the utilities' shareholders (including governments);

b) social media has become central to promote their corporate image and reputation;

c) for this centrality, social media are often exploited by hacktivists and competitors, for various socio-economic reasons, to stain the name and reputation of companies;

d) if such attacks via social media were to be integrated into 'strategic' information operations (IO) campaigns (as for example Russia has repeatedly done) by states or non-state actors, they could damage CII-utilities' standing, financial resources and even customer bases, thus leading to a comprehensive weakening of critical infrastructures.

In this phase, we rely on case-based evidence to identify a preliminary (explanatory) hypothesis, which will have to be tested in further research. For hypothesis-generating purpose, this is an established method, as indicated in Baxter and Jack (2008) and George and Bennett (2005). The causal mechanism of our preliminary hypothesis is summarized in Figure 1.

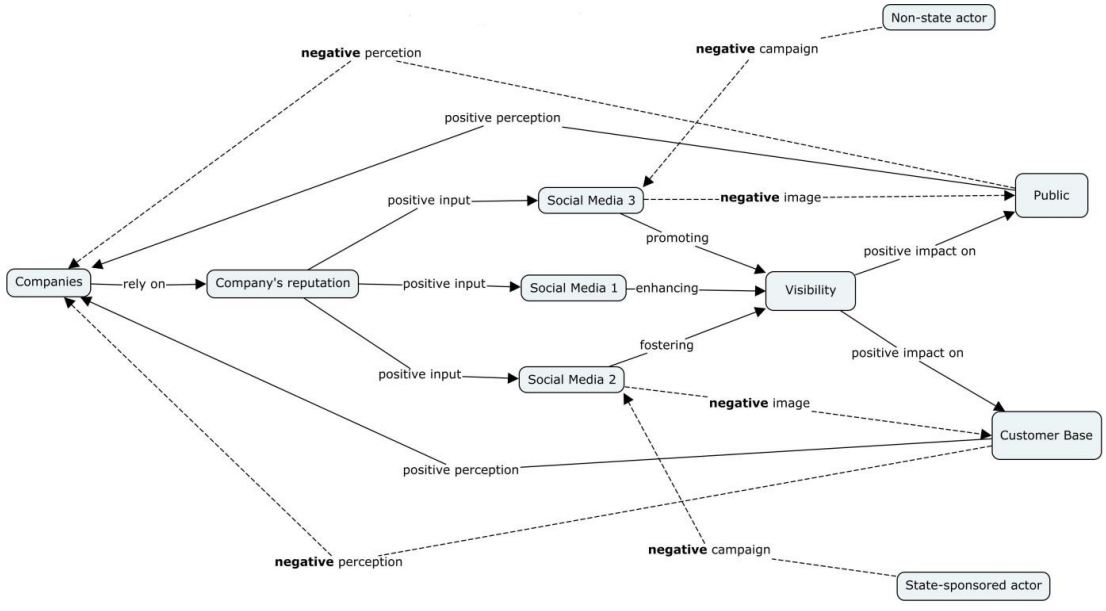

Figure 1. Hypothetical Attack Vector Mechanism

3. Corporate Reputation and Social Media

Intuitively, similar to personal reputation, corporate reputation has always been a strategic, vital asset for any business. Problems arose with the definition and identification of what corporate reputation is, making it either too narrow or too broad to be useful for businesses themselves. It is essentially, a company's identity translated into an image in the eyes of its various stakeholders (e.g., customers, retailers, suppliers, joint venture partners, financial institutions, shareholders, government regulatory agencies, social action organizations, the general public and employees) through a variety of communication mechanisms and channels (Gray & Balmer, 1998). Evaluating online retailers, Caruana and Ewing (2010) observe, 'Corporate credibility may, for example, impact customer loyalty directly or indirectly via corporate reputation.'

Today corporate reputation is a full-fledged scholarly topic, with many research articles and even its own journal (*Corporate Reputation Review* by Springer). Research shows that reputation is a very valuable resource for a contemporary enterprise because it may create its long-term competitive advantage and market value, and while it may take many years to build a strong, positive reputation, this can be damaged *relatively quickly* (Szwajca, 2018). Moreover, research reveals that the degree of customer loyalty has a tendency to be higher when perceptions of both corporate reputation and corporate image are strongly favorable (Nguyen & Leblanc, 2001). Referring specifically to the telecom industry, Shamma and Hassan (2009) note that:

> General public […] drive perceptions about corporations mainly from media sources. The mass media is the main source by which the general public forms perceptions about corporate reputation […]. The relatively strong relationship between knowledge from media and corporate reputation further supports the importance of media as an important source for building a company's reputation.

Social media, which allows for unmediated contact with many of the above-mentioned stakeholders, is now the most important communication platform to enhance and protect corporate reputation. At some point, all companies face complaints, and such complaints are now most likely to be publicly posted on social media accounts. In fact, experiments show that image restoration for a company works very well when crisis management is correctly applied in social media (Nazione & Perrault, 2019). Furthermore, 'the emergence of social media has dramatically influenced marketing practices', diminishing at the same time the relevance and role of traditional marketing (Habibi, Laroche, & Richard, 2014).

Many businesses have facilitated and even fed the development of 'brand communities' for like-minded followers on social media. Only ten years ago, no one would have thought of making a living as an 'influencer'. Utilities could hardly inspire such 'devotion' among users (few would get excited about who runs the power grid), but much like other market players, utility companies could not afford to be cavalier about their 'social persona' (i.e., their image and perception on social media). In fact, evidence shows that ultimately, trust in the internet and trust in firms may significantly influence consumers' conviction and ultimately their intention to engage in social commerce (Sharma, Menard & Mutchler, 2019; Dijkmans, Kerkhof, & Beukeboomb, 2015).

In addition to being a favored channel for strategic corporate communications, social media with their 'unmediated' linking to the company stakeholders and the general public expand the spectrum of reputation risks and may have notable effects on corporate-level strategic endeavors (Aula, 2010). In other words, corporate communications via social media with stakeholders and customers is a double-edged sword, with opportunities as well as threats, and this is the case for all companies, those in the utility industry included.

4. Utilities as Critical Infrastructure Today

The utility industry is one of the most important industries in the world, since, without utilities, modern existence would be quite different. Utilities involve some of the basic necessities that societies require and utility companies provide sewerage, water, gas and electricity services to the public.[i] Governments used to be the (sole) owners of that industry and this condition long remained unaltered. With the privatization 'wave' of the 1980s and 1990s, however, most national governments conformed to the business logic of greater 'economic efficiency' in producing and providing goods and services (often through 'public-private partnership' - PPP) and open to long-term contractual agreements between private and public actors to build/manage critical infrastructures or provide services for public utilities.

Energy, money, information and other goods and services are accurately distributed thanks to the cyber-physical, critical infrastructures, hence it is hardly surprising that cyber-attacks, of various types and for different purposes, have been on the rise.[ii] At the same time, the literature on cases of privatized utilities not responding well and efficiently to critical emergencies is now large and established (e.g., Sheil, 2000; Palm, 2008; Newlove-Eriksson, Giacomello & Eriksson 2018). Moreover, literature reviews show that cyber-attacks have a negative impact on

the market value of companies (Modi, Sachin, Wiles, & Mishra 2015; Berkman et al., 2018), which then have to invest greater money into their security. This conclusion is particularly stern for 'privatized' public utilities that manage a large array of cyber-physical assets. CII-public utilities cannot be simply considered as 'profit-maximizers' because security concerns must be taken into consideration. Dixon, Dogan, & Kouzmin (2003) warn that governments should become 'smarter' about when and where to cede their authority to the private sector especially in the area in which such care should probably be exercised the most, namely that of protection of CII-utilities.

The U.S. National Institute of Standards and Technology (NIST) defines critical infrastructures as the 'system and assets, whether physical or virtual, so vital to the U.S. that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters (Kissel, 2013). Likewise, the European Commission describes critical infrastructures as 'physical and information technology facilities, networks, services and assets that, if disrupted or destroyed, would have a serious impact on the health, safety, security or economic well-being of citizens or the effective functioning of governments in EU States.'[iii] Control mechanisms of various types connect infrastructures at multiple points, creating a bidirectional relationship between each given pair of infrastructures. Not only are infrastructures linked to one another by this close relationship, but they are also tied to one another across countries.

Three essential features are central to protect CII in general and CII in the utility industry in particular, namely, reliability, resilience and redundancy:

a) *Reliability* is the ability of an apparatus, machine, or system to consistently perform its intended or required function or mission, on demand and without degradation or failure, as well as the probability of failure-free performance:[iv] the higher, the better of course. The capability of CII to withstand aggressions and keep functioning or quickly recover ('bouncing-back') is called resilience.

b) *Resilience*, according to the *Oxford Dictionary of Current English*, is the 'quality or property of quickly recovering the original shape or condition, after being pulled, pressed, crushed, etc.' (or attacked, for that matter). Resilience can be fostered through various means, both technical and organizational (and for humans, psychological).

c) One such (technical) means is to replicate control systems one or more times, so that if the main one fails, there is a second or even a third backup. This is called *redundancy*, which is a type of resilience, although the two are distinct. The latter is broader and more comprehensive than the former. Clearly, the more critical a system – think of the computers aboard a passenger airplane – the greater redundancy is desirable. Redundancy, however, as *duplication*, can also be considered, from certain viewpoints, as wastage and/or inefficiency, if the main system works fine, never failing. This is an unresolved problem when it comes to CII and one that presents an interesting puzzle in the three events reviewed in this article.

Guaranteeing reliability and resilience, via redundancy, is vital to protect cyber-physical infrastrutures and utility companies may use these features as positive assets in promoting the quality of service they offer to investors and users. Indeed, 'safety and reliability' are themes that resonate rather well with shareholders since they may increase the overall market value of the company (and this predisposition will only grow in the future). Likewise, market value has become the most important indicator of the performance of utility companies worldwide. Interestingly, the ranking of global utility companies listed in Table 1 shows that still a state-owned company, State Grid Corporation of China, with an estimated value of $347bn, is above the rest of other utility companies included in Table 1.

Table 1. Major Global Utility Companies (2019 data)

Ranking	Company	Total revenue (mln USD)	Total assets (mln USD)	Total employees	Country of origins
1	State Grid	383,906	596,616	907,677	China
2	Electricité de France	80,278	340,406	161,522	France
3	Enel	89,907	192,409	68,253	Italy
4	China Southern Power Grid	81,978	134,036	283,639	China
5	Iberdrola	40,783	137,437	34,306	Spain
6	Exelon	34,438	124,977	124,977	United States
7	Korea Electric Power	50,257	170,888	47,452	South Korea
8	CFE	29,869	115,748	90,621	Mexico
9	China Huadian	33,808	118,038	94,790	China
10	Tokyo Electric Power	57,407	110,649	37,892	Japan

Sources: InsiderMonkey: Largest 10 Utility Companies in the World, December 2020 (at https://www.insidermonkey.com/blog/15-largest-utility-companies-in-the-world-910928/).

Data from Table 1 indicates how valuable this industrial sector is and, if it is valuable, it is also a coveted target for criminals looking for profits (e.g., Sanger, Krauss, & Perlroth, 2021) as well as state and non-state actors searching for economic and geopolitical advantages. In the past, threatening to destroy or even disrupting physical infrastructures required substantial resources and energies. Today, if some of the control and monitoring nodes of cyber-physical infrastructures could be put out of order, possibly via computer attack vectors, the resulting cascading effects could bring down a large portion of the CII system. It would really be akin to cutting the nerves, so that the adversary collapses. Could effective results also be obtained via 'cheaper' yet efficient means, relying on fake news, negative advertisement campaigns or disinformation?

5. The Impact of Information Operations

Information operations (IO) (a.k.a. 'information warfare', IW) is a U. S. military term referring to a complex and evolving field in which, for example, an 'information' campaign is 'dedicated to obtaining a decisive advantage in the information environment' (Fecteau, 2019). A more technical U.S. Department of Defense document (Joint Chiefs of Staff 2012) identifies IO as the use of information-related capabilities with other lines of operation 'to influence, disrupt, corrupt, or usurp the decision making of adversaries and potential adversaries while protecting our own'. The concept of IO was approximately born in the First Gulf War, where Coalition forces had a clearly superior edge in managing information for attacks and defense, and it has come to include integrated employment of electronic warfare (EW), computer network operations (CNO), psychological operations (PSYOP), military deception (MILDEC), and operations security (OPSEC).

Russia has made information warfare the centerpiece of its strategy of restoring its status as a global power like the United States and China. While Russia does not have the economic basis to compete with either of them on an equal basis, and actually because of this, Russia has perfected an integrated, quite effective strategy of subterfuge, cyber-sabotage and disinformation aimed at crippling the West without crossing into an open, armed conflict (Thomas, 2014; Sanger, 2018).

Against the United States and the E.U., Russia has exploited social media for disinformation and smearing campaigns (Ajir & Vaillant, 2018), especially to undermine the public trust in elections and elected officials (Inkster, 2016; Sauerbrey, 2017) and thus reaching remarkably large numbers of people. Moreover, part of its information operations, Russia has continued to target U.S. infrastructures like the nation's electric grid via 'traditional' malware (Perlroth & Sanger, 2018).

It is not only Russia, as China too has developed its strategic thinking along the same lines (Barrett, 2005). It was actually China that launched the idea of 'unrestricted warfare' in 1999 (Liang & Wang, 1999) as a way to offset the United States' technological dominance. This form of warfare 'with no rules' includes 'computer hacking, subversion of the banking system, markets and currency manipulation (financial war), terrorism, media

disinformation and urban warfare' (Wither, 2016).

Russia, and to a lesser extent China, have had more than a decade of experience of quite successful *disinformacjia* campaigns against the United States, Europe and other Western countries. Albeit with less resources and skills, hacktivists (hacktivism comes from the 'marriage of hack and activism', in Denning (2001)) have repeatedly shown how 'naming and shaming' multiplied by social media is an effective tool for political campaigns as we report in the next section. Hacktivists too, although less efficiently, may use the same techniques to undermine consumer trust in CII-utilities for political goals.

All in all, cyber-sabotage and disinformation are already quite efficiently used against policymakers and businesses. As noted by Borek, Woodall, Gosden, & Parlikad (2011) 'Information quality is a key issue for a majority of utility companies […]. Poor quality information is generating more costs, higher risks and fewer revenues.' As 'quality information' is so essential for business to prosper, with little effort, non-state and state actors could transform the techniques described above into a novel way of undermining even the utility industry, as we observe in this paper.

6. Social Media Cases and Discussion

Almost everyone today is familiar with the notion of social media. In addition to the most famous social networks, such as Facebook, Twitter, Instagram, LinkedIn, the Chinese Baidu or the rapidly growing TikTok, there are hundreds of social media platforms of different types.[v] They offer a broad range of functionality, from photo sharing services, discussion groups, and blogs, to social networking, text messaging, streaming videos or podcasts, just to name a few. Social media has been defined as 'a group of Internet-based applications that build on the ideological and technological foundations of Web 2.0, and that allow the creation and exchange of user-generated content' (Kaplan & Haenlein, 2010, p. 61). This definition embodies two main dimensions, content creation and network effects.

Traditional sources of information, such as radio, TV and print media, are designed for a one-way model of communication (Lyon & Montgomery, 2013). In the system of mass media, the ordinary citizen is seen as a passive recipient of information, with no or little control over the information flow. Deephouse & Suchman (2008) note that traditional broadcasting channels filter out the relevant information for the audience. Such a communication model has benefitted companies by allowing them to convey their messages to the masses without any contradiction.

The advent of social media has been a paradigm shift in communication, because it enables ordinary people to be an active part in the communication process. Social media sites offer virtual platforms where users can publicly communicate their ideas, opinions, preferences and emotions directly to their network, without asking for permission from gatekeepers of information. As noted by various studies (Gillmor, 2004; Benkler 2006), this has led to an empowerment of users that are now active players in content creation and spread of information, almost following in a two-way communication model.

As for the networking dimension of social media, Hensen, Shneiderman, & Smith (2011, p.3) note that 'billions of people create trillions of connections through social media each day'. These platforms enable even a single user to potentially reach tens of millions of people across the globe (Dijkmans, Kerkhof, & Beukeboomb, 2015).

Depending on the platform, social media allows for various types of active engagement. The more common ones consist of 'liking' a picture, a video, or a status, and include more active forms such as 'sharing' a link to another webpage or post written by other users, or 'posting' your own status or 'leaving comment(s)' to others' content.

This ease of engagement has significantly lowered the cost of mobilizing supporters (Earl & Kimport, 2011) not only in monetary terms, but also in terms of intangible resources like time and transport, making them affordable even for small online groups. Traditional forms of protesting require that citizens go out of home, often commute, and gather in a given place, at a specific time. Importantly, they involve the exposure of the protesters who may fear repercussions of some kind. Instead, the effort required for citizens to participate in the internet-based campaigns is minimal and usually preserves the user's anonymity, as social media accounts do not verify their real user identity.

In this way, ordinary citizens, activists or consumers can participate in social campaigns virtually, with the ease of a click on the keyboard of a PC or a touch on the screen of a smartphone. This action triggers a 'like', a 'post' or a 'share' of content written by somebody else, and this can easily be done from the comfort of the home couch, while sunbathing, or going for a hike.

Apart from how ordinary citizens interact with each other, the rapid growth of social networking has transformed

the communication between enterprises and customers (Hanna, Rohm, & Crittenden , 2011; Kietzmann, Hermkens, McCarthy, & Silvestre, 2011). Activists and consumers actively participate in the media process. Indeed, Hanna et al. (2011) recognize the ability of internet-based platforms to influence consumer decisions. On the other hand, Aula (2010) points out that social platforms allow for "uncontrolled arenas for participation", which may pose a risk of reputation damage for companies.

6.1 The Potential of Social Campaigns

The literature on social media provides many cases of how the social media ecosystem has been successfully utilized to launch negative campaigns against specific companies in various sectors. By raising people's awareness, such campaigns usually put pressure on privately owned companies demanding them to change operational decisions, practices, or behaviors mainly based on ethical considerations. In addition to local or national companies, Internet-based campaigns can also target global companies operating in hundreds of countries by engaging a worldwide audience.

Greenpeace, one of the most well-known NGOs worldwide, was among the first organizations to initially use the Web 1.0 (mainly webpages, blog), and later social networking sites (so-called Web 2.0), for its environmental campaigns as an additional instrument to various forms of offline activism (Lester & Hutchins, 2009; Castells, 2009).

Over the years, Greenpeace has launched several online protest campaigns against some of the major companies at a global level, including Coca-Cola, Apple, and Facebook. Back in 2000, Coca-Cola was targeted for contributing to greenhouse gas emissions through its refrigerators, which released high levels of hydro fluorocarbons (HFC) (Warkentin, 2001). Some years later, in 2006, Greenpeace started a campaign against Apple because of the supposed use of toxic chemicals in its products.

As the Internet has evolved from version 1.0 to the more interactive Web 2.0 with the introduction and diffusion of social networking platforms, so did Greenpeace with its campaign tactics. In early 2010, it posted a video against Nestlé on YouTube, which went viral; whereas the first campaign launched via a Facebook page, ironically, was directed against Facebook, the social network *par excellence*. The Unfriend Coal campaign asked Facebook to switch to renewable energy sources for its data centers.

All three of the campaigns listed above achieved their respective goals within a year or so, as companies embraced the campaigns' requests. While the first two combined online with offline actions, the Unfriend Coal campaign was entirely online based. While these kinds of campaigns call on both activists and internet users to raise their voice about private companies' decisions that are deemed to be unethical or unfair, a more effective way of online activism involves consumers through boycotting campaigns (Friedman, 1999).

As the name suggests, they explicitly invite consumers to stop buying products or services of a company with the end goal of causing economic damage to it. An example is provided by the case of Rimi Baltic, an International supermarket chain in Estonia. After announcing that Rimi Baltic was no longer selling local meat products in their shops, it became the target of a boycott campaign launched by local activists (P. Tampere, K. Tampere, & Abe, 2016). In this case, the rapid diffusion of the campaign convinced the company to take a step back in its decision, in addition to issuing public apologies. Other examples of campaigns via digital tools include McDonald's, Burger King, Sony, etc. The Greenpeace campaigns provide vivid examples of how social media can be used to mobilize activists and citizens online and gain successful campaign outcomes.

In addition to organized campaigns, the full potential of social networks as a key tool to share material quickly within a global audience appears evident through viral content. This means a spontaneous post going viral across one or more networking platforms, and so reaching millions of people across the Web in a very short time frame, especially if posts contain a negative sentiment like anger, fury or outrage.

Unlike designed campaigns, the mechanism behind content that becomes viral works roughly in the following way. All begin with either a single social media user, or several but uncoordinated social media users, usually complaining in a post about a product or service provided by a company, like millions of posts being published every day. However, once published, other users, prevalently part of the network, resonate with the post and engage with it in various ways, mainly through likes, shares, comments and posts. As a result, the post now reaches a larger number of users, who, in turn, decide to further distribute it on the Internet. This process will perpetuate up to the point where the original post of even a single user spreads so rapidly across the Web that it becomes viral. This pattern is similar to how a virus spreads among the population, hence the name. Finally, the cycle is closed with traditional media reporting the story.

There are many cases of user content going viral, and we will describe two of them. On the 14th of February

2007 (Valentine's Day), thousands of flights of JetBlue Airlines, a low-cost U.S. company, were canceled due to an ice storm. As expected, this caused anger among customers, who expressed their outrage online by writing about this experience on platforms like Twitter and Facebook. These events had a negative impact not only on the online reputation of JetBlue, but also on its offline reputation. Due to this online negative exposure, Busines Week magazine removed JetBlue from the list of the four U.S companies with the best customer service, as it had been previously recognized (Kaplan & Haenlein, 2011).

In another case, while flying back home from their deployment in Afghanistan with Delta Air Lines, two U.S. soldiers posted a video on YouTube expressing their indignation for being charged $2800 in extra baggage fees. Almost immediately, the video went viral, and as a result a disgruntled sentiment against the company grew rapidly for what was perceived as an unfair practice by the public, both customers and non-customers. Faced with such an unexpected outrage, Delta Air Lines reacted immediately: apart from apologizing publicly, they reviewed their policy on extra baggage fees for returning soldiers by extending free baggage from three to four bags (Jacquette, 2011).

Other than viral content, there are other ways to gain traction in social media platforms. Topics can receive attention within a single platform, thus being viewed by relatively large audiences. Twitter, for example, among others has a feature called trending topics that shows the most diffused topics among platform users at any point in time. Similarly, another forum-based platform called Reddit uses the number of thumbs up received by discussion topics as the measure to rank them on their home page.

Though driven by harmless motivations, a notable example of arranged Twitter trending topics is provided by the case of superstar Taylor Swift: thousands of her fans coordinated online across many countries through Telegram channels, a text messaging social network, to tweeting posts containing Taylor Swift hashtags within a certain time frame so that it could become a trending topic among all Twitter users. This led to the term 'Taylor Swift' to be considered a trending topic by the Twitter algorithm. Similarly, many individuals can agree to simultaneously vote on a post on Reddit so that it will appear among the first posts to be viewed. Reddit became the center in another interesting incident.

Indeed, the power of ‘distributed’ or ‘crowdsourcing’ attacks has been demonstrated, quite convincingly, by the 2021 GameStop (GME) case, which has gained particular notoriety via media outlets. Over January 2021, GME stocks at NYSE suddenly rose sharply up to a maximum of about $347 from $17-18, thus gaining more than 2000%. There has been a large consensus among financial analysts that the price bump was attributed to retail investors organized collectively on Reddit. All started on WallStreetBets subreddit[vi], which now counts more than 10 million members, with several members spreading information on GME’s financial situation. The main idea was that the company was heavily shorted (some sustain up to 160% of total shares) by some of the main Wall Street speculative funds with the final aim to cause the company to go bust, albeit the company was coping well with the COVID-19 economic crisis that had hit the United States. Therefore, the stock price was not reflecting a fair evaluation of the company’s actual value, but rather, it was the result of pure financial speculation. Going further, WallStreetBets members suggested that given the healthy financial situation of GME, it was the perfect case to push for a so-called ‘short squeeze’. Therfore, they invited numerous small investors to buy huge amounts of stocks to drive the stock price up, so that, ultimately, speculators (who would buy back what they had sold) could lose a lot of money. And that is exactly what happened.

Apart from the technical specificity of the financial case, what the GME story has proved once again is that online crowds, especially if driven by a sense of justice and organized for a common goal, are strong enough to/capable of winning against what is perceived as the ‘evil’, in this case represented by Wall Street funds. IO experts could with ease turn around a ‘just cause’ and with proper dressing elicit a massive disruptive response, as in the GameStop example, with serious consequences even for actors with a firm reputation of being normally quite powerful (such as Wall Street investment funds).

6.2 Risks

Social networking platforms offer an unparalleled digital tool to share content among ordinary citizens and, if needed, engage them in ethical, social, or any other type of causes. However, the spread of these digital media tools is associated with drawbacks as well. Among others, one of the main downsides of enabling even a single user to spread viral content is the ease with which improper information or fake content can be propagated on the Web.

There is no surprise, therefore, that networking tools are utilized to influence consumer behavior. Marketing agencies, for example, try to favor the creation of viral content mainly by giving the false perception that topics

related to products or services they want to promote are gaining traction online. Indeed, cases involving McDonald's (Thomases, 2012) and Sony (Kaplan & Haenlein, 2011) demonstrate that viral campaigns are hard to replicate as with lab experimentation given that the interminable ways in which humans interact with each other in the virtual world are very hard, if not impossible, to predict.

However, the algorithms underlying digital tools can be played by organized online communities, mostly trolls. The most common techniques combine the use of trolls with specific software known as bots. In our context, bots are programmed to perform automated tasks that mimic human actions in social media. Bots can be designed to create fake accounts first and then like, share or post a status, just like humans. Recently, the spread of fake accounts is increasingly becoming a worrying issue for social media providers as well. To provide a better idea of the gravity of this phenomenon, while more than 70 million fake or suspicious accounts were removed by Twitter between May and June 2018, Facebook detected and canceled 3.9 billion fake accounts during a period of only 6-months (October, 2018 - March, 2019)[vii].

Bots and fake content can therefore be used in an inappropriate way by spreading fake news aimed at damaging the reputation of a specific company. Although hard to uncover, various cases have been identified of bots being used to alter the perception of reality related to specific topics in the social media world. The interference of Russian trolls in the US presidential elections is perhaps the most notable one. Recently, apart from demonstrating the direct involvement of the Russian Internet Research Agency (IRA) in discussions on Twitter regarding vaccines in the US between 2015 and 2017, Walter, Ophir, & Jamieson, (2020) argue that the content promoted by IRA accounts was functional in fostering the polarization of positions about vaccines instead of providing a scientific contribution to the topic.

In another case, digital tools were used to launch a fake campaign against the Metro Bank in the United Kingdom (UK), causing the shares of the company to drop by about 11 percent[viii]. More specifically, false rumors about the bank going bankrupt and inviting customers to empty their accounts were spread via WhatsApp groups first and on Twitter later. In addition, pictures of panicked customers in Harrow (UK) standing in line while waiting to withdraw their money were posted on Twitter[ix]. As a result, some hedge funds shorted about 12.5 percent of the company's shares, according to Wired[x]. Luckily, Metro Bank managed to react immediately, avoiding irreversible damage.

As illustrated by the cases described above, social platforms can easily be manipulated. While Twitter algorithms are not able to distinguish between spontaneous trending topics and artificially created ones, organized users on Reddit can agree to simultaneously vote a discussion topic so that it can appear among the top ones on the homepage. More sophisticated strategies that combine bots with organized online communities with specific goals can give rise to the manipulative use of social media platforms with the purpose of spreading fake content.

Although the cases reported so far regard companies not operating in the utility industry, they nonetheless demonstrate that social media can play a crucial role in damaging a company's reputation in various sectors, which would be quite a novel attack vector. In light of these cases, therefore, it is reasonable to sustain that companies operating in sectors related to CII are not immune to threats related to protest, complaints or fake campaigns that leverage digital media.

Companies in the utility industry, especially those involved in the energy sector, are more vulnerable to negative campaigns than other sectors because of their questionable reputation they may have in terms of the environment. Energy companies are often perceived as polluters at least by a part of the public particularly sensitive to the environment, but such conclusion can be a concern for companies in water distribution or sewage. It is plausible that hacktivists could utilize such controversial situations and exploit them to their own social/political advantage.

This state of affairs should raise serious concerns about what could happen if CII-utilities were to be targeted by fake social campaigns. To what extent can the trust of companies' stakeholders be affected by a crisis started by either unjustified protests or a fake news campaign via social media? What would be the impact on a company's reputational value deriving from the partial loss of consumer confidence or that of stakeholders in general? Would this in turn affect the value of the company and, if yes, to what extent? And finally, could this eventually trigger a domino effect to the point that it compromises the company's ability to provide critical services, thus creating widespread disturbance to large masses of users?

Within this context, how can companies be protected from campaigns aiming to undermine their reputation by utilizing digital tools of communication? Like other kinds of risks (i.e., financial, seismic), it is impossible to prevent risks associated with social platforms. However, risks can be mitigated to a certain extent. To achieve

this, companies should first raise awareness about various threats related to the spread of social media. Secondly, being prepared to quickly handle negative news or campaigns is key to mitigating the impacts of such attacks before they turn into a serious reputational crisis with devasting effects.

From a practical perspective, companies need to put in place specific procedures and practices to protect their reputation, brand image, and ultimately, their company value. In particular, they should take advantage and use the same channels to communicate what they do, what their strengths are and potentially even to be transparent about their weak points (Dijkmans, Kerkhof, & Beukeboomb, 2015).

7. Conclusions

This paper is a probe into the future, with case-based evidence for hypothesis-generating purposes. The attack vector considered in this paper is based on relevant literature and present examples and could be considered likely if integrated into a larger strategy aimed at weakening the infrastructures of potential adversaries. The basis on which we constructed our argument for a potential attack vector in this paper can be summarized as follows:

a. Corporate reputation is an extremely valuable asset for companies; cyber-attacks may undermine a company's market value and, likewise, damage customer trust in a company's services and products.

b. Public utility companies that were privatized during the 1980s and 1990s now have to 'behave' like other companies in the market and pay attention to the same opportunities and risks, including the protection of their corporate reputation and market value; however, CII utilities are *not* like other businesses as their services to the public are essential for the 'normal' functioning of societies and economies and failure or collapse of the utility industry would have profound repercussions.

c. Russia, and to a lesser extent China and other countries, have shown the effectiveness of using 'information operations' (what was called 'propaganda' but more sophisticated) to destabilize public trust in democratic elections, political parties or national governments, in order to gain political advantage. Moreover, businesses can be subject to the same outcomes, but they are rarely targeted by state-actors; companies in the utility industry, however, could be considered worthwhile targets by governments interested in causing negative attitudes within the general public towards CII-utility companies.

d. Evidence from examples of negative social campaigns or even spontaneous complaints against large companies in various sectors, through the use of Facebook, Twitter, YouTube and social media platforms in general, show that with relatively small investments and resources hacktivists and other online groups can certainly damage a company's online reputation and have real effects on their operations; state-actors with superior expertise and resources than non-state actors could launch such 'negative' campaigns with relative ease and achieve considerable results.

Our generated hypothesis, on the case-based evidence, indicates that, like other companies, utility companies can be affected in their reputation by adverse social media campaigns, as summarized in Figure 1. The more their reputation is blemished, the more their operations will suffer (because of the loss of customer base and/or stakeholders), and the more their operational capacity is affected, the less utility companies will be able to safeguard their cyber-physical infrastructures. Another possible element of explanation, which should also be investigated in future research, is that the global utility industry, as shown in Table 1 is dominated by the continent of Europe, although East Asia- Pacific (specifically China, South Korea and Japan) has started catching up quickly, while the United States is mostly in rearguard. Thus, the US government is not overly concerned about the attack vector described in this paper, whereas continental Europe and East Asia should be devoting more attention to it.

Therefore, the key point is that, as the privatized utility industry, much like any other industrial sector, has to factor-in the centrality of corporate reputation that may be vulnerable via negative campaigns on social media, some non-state (hacktivists?) or state-actors (Russia?, China?, Iran?) may see integrating such discrediting methods in a larger information strategy as valuable assets. The trust of both shareholders and customers in the utility industry could be compromised and thus also their revenue and investment bases. Even if such effects were to be small (and they are unlikely to be so), the resources and technical investment demands on the attackers would be rather negligible, as the assets are already available and applied in other information operations; it would be a matter of extending their application and a bit more planning on the attackers' side and it could reap considerable long-term advantages against their adversaries by undermining their critical infrastructures. It is still hypothetical, but the potential impact and the effortlessness of execution should make

utility companies and those in charge of protecting CII duly take note and develop proper countermeasures. In a sense, negative campaigns on social media as a novel attack vector should already be a concern of the personnel in charge of information systems (IS) risk within public utility companies. A preliminary literature review (Amraoui, Elmaallam, Bensaid & Kriouile, 2019), however, shows that this is not yet the case. In fact, if information systems are, de facto, socio-technical systems, organizational overlapping should bring IS people to work more closely with marketing and social media managers. If one considers that even oil companies could prefer to become electricity providers (at least in Europe), because it is 'greener', socially more acceptable (Reed, 2020) and thus good for their reputation, it is plainly clear that the social media perception problem can only grow in importance.

Acknowledgments

Authors would like to express their greatest appreciation to Maria Krasilowez and Emma Michela Giacomello for their help with the editing of this article.

References

Ajir, M., & Vaillant, B. (2018). Russian information warfare: Implications for deterrence theory. *Strategic Studies Quarterly, 12*(3), 70-89. Retrieved from https://www.jstor.org/stable/10.2307/26481910

Almklov, P. G., & Antonsen, S. (2010). The commoditization of societal safety. *Journal of Contingencies and Crisis Management, 18*(3), 132-144. https://doi.org/10.1111/j.1468-5973.2010.00610.x

Amraoui, S., Elmaallam, M., Bensaid, H., & Kriouile, A. (2019). Information systems risk management: Literature review. *Computer and Information Science, 12*(3), 1-20.

Aula, P. (2010). Social media, reputation risk and ambient publicity management, *Strategy & Leadership, 38*(6), 43-49. https://doi.org/10.1108/10878571011088069

Barrett, B. M. (2005). Information warfare: China's response to US technological advantages. *International Journal of Intelligence and Counterintelligence, 18*(4), 682-706. https://doi.org/10.1080/08850600500177135

Baxter, P., & Jack, S. (2008). Qualitative case study methodology: Study design and implementation for novice researchers. *The Qualitative Report, 13*(4), 544-559. https://doi.org/10.46743/2160-3715/2008.1573

Benkler, Y. (2006). *The wealth of networks: How social production transforms markets and freedom*. London: Yale University Press. https://doi.org/10.1177/1084713807301373

Berkman, H., Jona, J., Lee, G., & Soderstrom, N. (2018). Cybersecurity awareness and market valuations. *Journal of Accounting and Public Policy, 37*(6), 508-526.

Borek, A., Woodall, P., Gosden, M., & Parlikad, A. K. (2011). Managing information risks in asset management experiences from an in-depth case study in the utility industry. IET and IAM Asset Management Conference 2011, 2011. Retrieved from https://digital-library.theiet.org/content/conferences/10.1049/cp.2011.0551

Brendan, M. (1993). *In the public interest: Privatization and public sector reform*. London: Zed Books Ltd.

Caruana, A., & Ewing, M. T. (2010). How corporate reputation, quality, and value influence online loyalty. *Journal of Business Research, 63*(9-10), 1103-1110.

Castells, M. (2009). *Communication power*. Oxford: Oxford University Press. https://doi.org/10.1080/10584609.2010.517097

Cedergren, A., Lidell, K., & Lidell, K. (2019). Critical infrastructures and the tragedy of the commons dilemma: Implications from institutional restructuring on reliability and safety. *Journal of Contingencies and Crisis Management, 27*, 282-292.

Cohen, F. (2010). What makes critical infrastructures critical. *International Journal of Critical Infrastructures Protection, 3*(2), 53-54.

Denning, D. E. (2001). Activism, hacktivism, and cyberterrorism: The Internet as a tool for influencing foreign policy. In *Networks and netwars: The future of terror, crime, and militancy*, edited by John Arquilla and David Ronsfeld, Santa Monica, CA: RAND, 239-288.

Deephouse, D. L., & Suchman, M. (2008). Legitimacy in organizational institutionalism. In R. Greenwood, C. Oliver, R. Suddaby, K. Sahlin (Eds) *The Sage handbook of organizational institutionalism* (pp.49-77). London: SAGE Publications Ltd.

Dijkmans, C., Kerkhof, P., & Beukeboomb, C. J. (2015). A stage to engage: Social media use and corporate reputation**.** *Tourism Management, 47*, 58-67. https://doi.org/10.1016/j.tourman.2014.09.005

Dixon, J., Dogan, R., & Kouzmin, A. (2004). The dilemma of privatized public services: Philosophical frames in understanding failure and managing partnership terminations. *Public Organization Review, 4*(1), 25-46.

Donahue, J. D. (1989). *The privatization decision: Public ends, private means*. New York, NY: Basic Books.

Dunn-Cavelty, M., & Suter, M. (2009). Public–private partnerships are no silver bullet: An expanded governance model for critical infrastructure protection. *International Journal of Critical Infrastructure Protection*, *2*(4), 179-1987. https://doi.org/10.1016/j.ijcip.2009.08.006

Earl, J., & Kimport, K. (2011). *Digitally enabled social change: Activism in the internet age*. Cambridge, MA: The MIT Press. https://doi.org/10.7551/mitpress/9780262015103.001.0001

Eriksson-Love L., Giacomello, G., & Eriksson, J. (2018). The invisible hand? Critical information infrastructures, commercialisation and national security. *The International Spectator*, *53*(2), 124-140. https://doi.org/10.1080/03932729.2018.1458445

Fecteau, Matthew J. (2019). Understanding Information Operations & Information Warfare: The Muddled Meaning of IO (and IW), Global Security Review, Last updated Jun 7. Retrieved from https://globalsecurityreview.com/understanding-information-operations-information-warfare/

Friedman, M. (1999). *Consumer boycotts: Effecting change through the marketplace and the media*. New York, NY: Routledge. https://doi.org/10.4324/9780203900406

George, A. L., & Bennett, A. (2005). *Case studies and theory development in the social sciences*. Cambridge, MA: MIT Press. https://doi.org/10.1177/0276146707305480

Gillmor, D. (2004). *We the media: Grassroots journalism by the people, for the people*. Sebastopol, CA: O'Reilly.

Gray, E. R., & Balmer, J. M. (1998). Managing corporate image and corporate reputation. *Long Range Panning, 31*(5), 695-702. https://doi.org/10.1016/S0024-6301(98)00074-0

Habibi, M. R., Laroche, M., & Richard, MO. (2014). The roles of brand community and community engagement in building brand trust on social media. *Computers in Human Behavior, 37*, 152-161. https://doi.org/10.1016/j.chb.2014.04.016

Hanna, R., Rohm, A., & Crittenden, V. L. (2011). We're all connected: the power of the social media ecosystem. *Business Horizons, 54*(3), 265-273. https://doi.org/10.1016/j.bushor.2011.01.007

Henk, B., Jona, J., Lee, G., & Soderstrom, N. (2018). Cybersecurity awareness and market valuations. *Journal of Accounting and Public Policy, 37*(6), 508-526.https://doi.org/10.1016/j.jaccpubpol.2018.10.003

Hensen, D., Shneiderman, B. & Smith, M. A. (2011). *Analysing social media networks with NodeXL: Insights from a Connected World*. Boston, MA: Elsevier.

Inkster, N. (2016). Information warfare and the US presidential election. *Survival, 58*(5), 23-32. https://doi.org/10.1080/00396338.2016.1231527

Jacquette, R. (2011, June 8). Delta apologizes for charging returning troops $2,800 baggage fee. *New York Times*. Retrieved from http://atwar.blogs.nytimes.com/2011/06/08/delta-apologies-for-charging-returning-troops-2800-baggage-fee/

Joint Chiefs of Staff. (2012). JP 3-13, Information Operations, US Department of Defense, 27 November (updated 2014). Retrieved from https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_13.pdf

Kaplan, A. M., & Haenlein, M. (2010). Users of the world, unite! The challenges and opportunities of social media. *Business Horizons, 53*(1), 59-68. https://doi.org/10.1016/j.bushor.2009.09.003

Kaplan, A. M. & Haenlein, M. (2011). Two hearts in three-quarter time: How to waltz the social media/viral marketing dance. *Business Horizons, 54*(3), 253-263. https://doi.org/10.1016/j.bushor.2011.01.006

Kietzmann, J. H., Hermkens, K., McCarthy, I. P., & Silvestre, B. S. (2011). Social media? Get serious! Understanding the functional building blocks of social media. *Business Horizons, 54*(3), 241-251. https://doi.org/10.1016/j.bushor.2011.01.005

Kissel, R. (ed.) (2013). Glossary of Key Information Security Terms, NIST IR 7298 Revision 2, National

Institute of Standards and Technology (NIST), US Department of Commerce. Retrieved from http://csrc.nist.gov/publications. https://doi.org/10.6028/NIST.IR.7298r3

Lester, L., & Hutchins, B. (2009). Power games: Environmental protest, news media and the internet. *Media, Culture & Society, 31*(4), 579-595. https://doi.org/10.1177/0163443709335201

Liang, Q., & Wang, X. (1999). *Unrestricted Warfare*. Beijing: PLA Literature and Arts Publishing House, 1999. Retrieved from https://www.oodaloop.com/documents/unrestricted.pdf.https://doi.org/10.18278/gsis.5.1.2

Lyon, T. P., Montgomery, A. W. (2013). Tweetjacked: The impact of social media on corporate greenwash. *Journal of Business Ethics 118*, 747-757. https://doi.org/10.1007/s10551-013-1958-x

Metzger, J. (2004). The concept of critical infrastructure protection. In A. Bailes, and I. Frommelt (Eds), *Business and Security Public-Private Sector Relationships in a New Security Environment* (197-209), New York: Oxford University Press.

Modi, S. B., Wiles, M. A., & Mishra, S. (2015). Shareholder value implications of service failures in triads: The case of customer information security breaches. *Journal of Operations Management, 35*(1), 21-39. https://doi.org/10.1016/j.jom.2014.10.003

Nazione, S., & Perrault, E. K. (2019). An empirical test of image restoration theory and best practice suggestions within the context of social mediated crisis communication. *Corporate Reputation Review 22*, 134-143. https://doi.org/10.1057/s41299-019-00064-2

Newlove-Eriksson, L., Giacomello, G., & Eriksson, J. (2018). The invisible hand? Critical information infrastructures, commercialisation and national security. *The International Spectator 53*(2), 124-140, https://doi:10.1080/03932729.2018.1458445.

Nguyen, N., & Leblanc, G. (2001). Corporate image and corporate reputation in customers' retention decisions in services. *Journal of Retailing and Consumer Services*, *8*(4), 227-236. https://doi.org/10.1016/S0969-6989(00)00029-1

Palm, J. (2008). Emergency management in the Swedish electricity market: The need to challenge the responsibility gap. *Energy Policy*, *36*(2), 843-849.

Perlroth, N., & Sanger, D. E. (2018, March 15). Cyberattacks put Russian fingers on the switch at power plants, U.S. says. *The New York Times*, https://nyti.ms/2FMlo5o

Reed, S. (2020, Aug. 17) Europe's oil titans ramp up transition to cleaner energy. *The New York Times*, Section B, Page 1.

Shamma, H. M., & Hassan, S. S. (2009). Customer and non-customer perspectives for examining corporate reputation. *Journal of Product & Brand Management*, *18*(5), 326-337. https://doi.org/10.1108/10610420910981800

Sanger, D. E. (2018). *The perfect weapon: War, sabotage, and fear in the cyber age*. New York, NY: Crown Publishing.

Sanger, D. E., Krauss, C., & Perlroth, N. (2021, May 8). Cyberattack forces a shutdown of a top U.S. pipeline. *The New York Times.* Retrieved from https://www.nytimes.com/2021/05/08/us/politics/cyberattack-colonial-pipeline.html?smid=url-share

Sauerbrey, A. (2017, July 22). Will Russia try to hack Germany? *The New York Times*, p. A1.

Sethuraman, R. A. J., Tellis, G. J., & Briesch, R. (2011). How well does advertising work? Generalizations from a meta-analysis of brand advertising elasticity. *Marketing Science, 48*(3), 457-471. https://doi.org/10.1509/jmkr.48.3.457

Sharma, S., Menard, P., & Mutchler, L. A. (2019). Who to trust? Applying trust to social commerce. *Journal of Computer Information Systems*, *59*(1), 32-42.

Sheil, C. (2000). *Water's fall: Running the risks with economic rationalism*. Annadale, NSW: Pluto Press Australia.

Smith, K. T., Smith, M.， & Smith, L. J. (2011). Case studies of cybercrime and its impact on marketing activity and shareholder value. *Academy of Marketing Studies Journal*, *15*(2). Retrieved from https://ssrn.com/abstract=1724815

Smith, K. T., Jones, A., Johnson, L. & Smith, L. M. (2019). Examination of cybercrime and its effects on corporate stock value. *Journal of Information, Communication and Ethics in Society, 17*(1), 42-60. https://doi.org/10.1108/JICES-02-2018-0010

Szwajca, D. (2018). Dilemmas of reputation risk management: Theoretical study. *Corporate Reputation Review 21*, 165-178. https://doi.org/10.1057/s41299-018-0052-9

Tampere, P., Tampere, K., & Abe, S. (2016). Who defines the narrative of a crisis? The case of an Estonian online boycott campaign against an international supermarket chain. *Central European Journal of Communication, 16*(9), 57-72. https://doi.org/10.19195/1899-5101.9.1(16).4

Thomas, T. (2014). Russia's information warfare strategy: Can the nation cope in future conflicts? *The Journal of Slavic Military Studies, 27*(1), 101-130. https://doi.org/10.1080/13518046.2014.874845

Thomases, H. (2012, January 25). McDonald's twitter mess: What went wrong. *Inc. Magazine*. Retrieved from https://www.inc.com/hollis-thomases/mcdonalds-mcdstories-twitter-mess.html

Van Noort, G., & Willemsen, L. M. (2012). Online damage control: the effects of proactive versus reactive webcare interventions in consumer-generated and brand-generated platforms. *Journal of Interactive Marketing, 26*(3), 131-140. https://doi.org/10.1016/j.intmar.2011.07.001

Walter, D., Ophir, Y., & Jamieson, K. H. (2020). Russian Twitter accounts and the partisan polarization of vaccine discourse, 2015-2017. *American Journal of Public Health, 110*(5), 718-724. https://doi.org/10.2105/AJPH.2019.305564

Warkentin, C. (2001). *Reshaping world politics: NGOs, the internet, and global civil society*. Lanham, MD: Rowman & Littlefield.

Weinberg, B. D., & Pehlivan, E. (2011). Social spending: managing the social media mix. *Business Horizons, 54*(3), 275-282. https://doi.org/10.1016/j.bushor.2011.01.008

Wither, J. K. (2016). Making sense of hybrid warfare, *Connections: The Quarterly Journal, 15*(2), 73-87.

Endnotes

[i] Compiling a list of major utilities worldwide: Ty Haqqi "15 Largest Utility Companies in the World", InsiderMonkey, December 22, 2021, https://www.insidermonkey.com/blog/15-largest-utility-companies-in-the-world-2-910631/.

[ii] Evidence of this can be seen quite clearly even in real time on the web site operated by *Deutsche Telekom* (www.sicherheitstacho.eu/) or that by Akami (www.akamai.com/html/technology/dataviz1.html). From the latter is even possible to download the app to have a continuous update.

[iii] European Commission, DG Home Affairs, at http://ec.europa.eu/dgs/home-affairs/e-library/glossary/index_c_en.htm.

[iv] For more definitions, see www.businessdictionary.com/definition/reliability.html#ixzz3kUbxWtwTwill.

[v] Harris, R. (2009). Social media ecosystem mapped as a wiring diagram. http://www.twitterthoughts.com/social-media-news-analyses/2009/9/3/social-media-ecosystem-mapped-as-a-wiringdiagram. html?printerFriendly=true.

[vi] https://www.reddit.com/r/wallstreetbets/

[vii] Rosen, G. "An update on how we are doing at enforcing our community standards", (a blog onFaceBook), May 23, 2019, https://about.fb.com/news/2019/05/enforcing-our-community-standards-3

[viii] Megaw, N. & Hammond, G. "Metro Bank shares fall as it reaffirms capital raising", *Financial Times*, May 13, 2019, https://www.ft.com/content/0b1a50fe-754e-11e9-bbad-7c18c0ea0201

[ix] Katwaa, A. "The Metro Bank hoax shows the immense power of fake news on WhatsApp", *WIRED*, May 14, 2019, https://www.wired.co.uk/article/metro-bank-share-price-whats-app-hoax

[x] Timberg, C. & Dwoskin, E. "Twitter is sweeping out fake accounts like never before, putting user growth at risk", *Washington Post*, July 7, 2018,

https://www.washingtonpost.com/technology/2018/07/06/twitter-is-sweeping-out-fake-accounts-like-never-befor

e-putting-user-growth-risk/