VOL 2 (2018) ISSUE 2

EUROPEAN CYBERSECURITY MARKET

RESEARCH, INNOVATION, INVESTMENT

THE KOSCIUSZKO INSTITUTE

EUROPEAN CYBERSECURITY MARKET

RESEARCH, INNOVATION, INVESTMENT

European Cybersecurity Market is a new publication designed to promote innovative solutions and tools in the field of cybersecurity. In order to raise awareness and increase cooperation in the developing digital economy, this periodical will be openly distributed to all interested parties and stakeholders.

EDITORIAL BOARD

Chief Editor: Robert Siudak
CYBERSEC HUB Project Manager and Research Fellow of the Kosciuszko Institute, Poland

Deputy Editor: Dr Joanna Świątkowska
CYBERSEC Programme Director and Senior Research Fellow of the Kosciuszko Institute, Poland

Executive Editors: Marta Przywała and Barbara Sztokfisz

Designer / DTP: Joanna Kaczor

Proofreading: Justyna Kruk and Agata Ostrowska

ISSN: 2543-7259

European Cybersecurity Market is a quarterly publication.

Published by:
The Kosciuszko Institute
ul. Feldmana 4/9-10
31-130 Kraków, Poland

Phone: 00 48 12 632 97 24
E-mail: robert.siudak@ik.org.pl

www.ik.org.pl
www.cybersechub.eu

CO-FINANCED BY

European Funds Regional Programme

KRAKÓW REGION MAŁOPOLSKA

European Union
European Regional Development Fund

Disclaimer: The views expressed in articles are the authors' and not necessarily those of the Kosciuszko Institute. Authors may have consulting or other business relationships with the companies they discuss.

© 2018 The Kosciuszko Institute
All rights reserved. The publication, in whole or in part, may not be copied, reproduced, nor transmitted in any way without the written permission of the publisher.

FOREWORD

ROBERT SIUDAK
Chief Editor of European Cybersecurity Market
CYBERSEC HUB Project Manager
Research Fellow of the Kosciuszko Institute, Poland

According to the newest study by the Massachusetts Institute of Technology, false news spreads in the cyberspace roughly six time faster than the truth. The problem is systemic and based not only on technological factors, but also on our cognitive biases. Clickbait prone algorithms, fuelled by our behavioural attraction to novelty, are only part of the problem that we are slowly starting to apprehend. From democratic processes, through social communication, to business operations, almost all spheres are threatened by potential disinformation and fake news campaigns.

There is no silver bullet that will help us to face this multilevel challenge. Currently, numerous attitudes and possible countermeasures are developed simultaneously around the world. This edition of the ECM provides readers with the European perspective on these phenomena. First and foremost, is the perspective involves a deeply interdisciplinary and multi-stakeholder approach. You will find contributions from journalists, public policy analyst and startup representatives, with references to technological, social and legal layers of the issue. From the market perspective, disinformation is yet another customer-problem-solution opportunity that fosters the development of new technological and public relation products and services. From the societal point of view, disinformation disrupts mass communication and divides communities. The role of media literacy and the need for new models of journalism are amongst the main proposals for addressing these issues. Finally, from the public policy viewpoint, disinformation may threaten the stability of the state and harm trust between citizens and elected representatives. Unfortunately, there are still no clear solutions that could help to challenge this phenomenon on the national and international level.

Cyberspace is changing the way we consume information. While we do not yet fully understand this revolution, digitisation is reshaping not only the industry, military or leisure, but also the way we communicate with the world. I personally believe that the innovative effort, which we widely discuss in the ECM, should be focused not only on boosting profitability or revenues but also on facing such great modern challenges as disinformation.

Robert Siudak

CONTENTS

5 **FAKE NEWS AND POPULISM: A CONVERGENCE OF INTERESTS**
Vassilis Nedos

10 **FAKE NEWS IN REAL BUSINESS**
Michał Fedorowicz

16 **PUBLIC POLICY VS DISINFORMATION: DEVELOPING EUROPEAN UNION'S APPROACH**
Barbara Sztokfisz

22 **TRUTHNEST: A SERVICE ASSISTING USERS ASSESS THE TRUSTWORTHINESS OF INFORMATION FOUND ONLINE**
Nikos Sarris

30 **NO FAKE NEWS IS GOOD NEWS – DEALING WITH DISINFORMATION AT CYBERSEC – BRUSSELS LEADERS' FORESIGHT**
Ziemowit Jóźwik

FAKE NEWS AND POPULISM: A CONVERGENCE OF INTERESTS

BY VASSILIS NEDOS

"Today's populist Zeitgeist likewise encourages the public to privilege its own take on the past without deferring to expert views. Postmodernists preach that historians like all of us are partial, selective, above the fray; we should mistrust self-interested professionals all the more for claiming expertise. But students taught "that every historical source is biased… often dismiss all sources as unreliable and give up on the possibility of knowing anything about the past". But if all pasts are dubious, they are also equally deserving of attention. Your past, my past, so-and-so's past all differ, but each has the high populist merit of being someone's past"[1].

Historians of course have a different duty than journalists and media professionals in general. Nonetheless the aforementioned excerpt, just a tiny bit from the magnificent work of David Lowenthal on how we treat the past, and how it eventually shapes us collectively and individually, really underlines the very essence of the landslide success that fake news and disinformation campaigns achieve. In our contemporaneity, where through the search tool of Google and online encyclopedia's like Wikipedia, anyone can feel like an expert, the only condition that needs to be met, is a reliable internet connection or a 3G/4G network. The bottom line is that without populism fake news would be inconceivable. Disinformation campaigns would make no sense. Yet again this is not about reinventing the wheel.

In our contemporaneity, where through the search tool of Google and online encyclopedia's like Wikipedia, anyone can feel like an expert, the only condition that needs to be met, is a reliable internet connection or a 3G/4G network.

[1] Lowenthal D., The Past is a Foreign Country, Cambridge, 2015, p. 350.

In terms of the fake news phenomenon per se there already exists a vast literature, a fact that features on one hand the general interest on the topic, and points out on the other, the practical absence of any real answer on how blunt lies can be tackled out of the public debate. In global scale the American presidential elections of 2016 remain, most likely, the most debatable in terms of a possible political outcome that may have been influenced by the spread of fake news, especially with the help of the multiplying effect that social media have on the dissemination of any information whatsoever. Some researchers have shown that the actual impact on the voters final choice per se wasn't so important[2], even though it is quite clear that several actors did make a considerable effort to indirectly influence the elections, through fake news and disinformation campaigns[3].

In global scale the American presidential elections of 2016 remain, most likely, the most debatable in terms of a possible political outcome that may have been influenced by the spread of fake news.

Nonetheless, what is more important is that "fake news" is a phenomenon that is quite probably here to stay. Mainly because the spread of disinformation is not something completely new. What changes in comparison to "old school" propaganda or similar accustomed deliberate, well designed disinformation campaigns, is that through social media the impact of it, really becomes enormous.

The political discourse in Greece has been the victim of fake news and disinformation campaigns mainly through media outlets (mostly online) but also social media enhancers. The two main political events of 2015, elections of January 25st and the Referendum of July 6th, all had the creation of strong sentiments as the core element of the disinformation campaign[4]. At that time disinformation campaigns were mainly focused on accusations against what was perceived generally as the "status quo" political parties. With the change of government and the seizure of power from the current ruling party (SYRIZA), the then main branch of criticism against "status quo parties" one would expect that this tendency would diminish. Nonetheless it hasn't. It has only changed form and it looks a lot more like more traditional disinformation campaigns. This time it is connected to the information burbling up now and then about the negotiations between governments in Greece and Balkan countries to its north (Albania, but first and foremost about the Former Yugoslav Republic of Macedonia). On February 20th a series of Greek media (mostly online) shared what seemed to be an interview of the Greek Minister of Foreign Affairs to a Czech TV Station (Radio Slobodna Evropa). The information wasn't incorrect, but the interview was given to Reuters some 20 days ago[5]. On February 5th, a series of webpages also reproduced statements of the Turkish President Recep Tayyip Erdogan allegedly supporting fervently Skopje in its diplomatic quarrel with Athens. And as true as it may seem given the usually very bad relations between Greece and Turkey, these statements were made by Erdogan, but in reality almost 4 years ago, on May 12th 2014. That was a "trans-balkan" fake news campaign. It started from the webpage of a Skopje based webpage titled "TV Nova" and in a few hours it was uploaded on Greek (protothema.gr, iefimerida.gr) but also Bulgarian (topnovini.bg) online outlets[6]. This is a very clear indication that, even though Greece and FYR Macedonia are still heavily entangled in a 25 year long diplomatic dispute, even though in terms of fake news and disinformation, people on both sides of the border cooperate quite effectively.

[2] Allcott Hunt, Gentzkow Matt., "Social Media and Fake News in the 2016 Election" in *Journal of Economic Perspectives* 31, 2, 2017, p. 211-236.

[3] One of the most recent accusations came from the U.S. national security adviser Lt. Gen. H. R. McMaster, that said during the Munich Security conference that the indictment provided "really incontrovertible" evidence that Russia interfered in the last presidential elections. "Now that this is in the arena of a law-enforcement investigation, it will be very apparent to everyone," he added. From, Julian E. Barnes, U.S., Russian officials spar at Security Conference over election meddling, *Wall Street Journal*, 18.2.2018.

[4] Antonakaki D, Spiliotopoulos D, V. Samaras C, Pratikakis P, Ioannidis S, Fragopoulou P (2017) Social media analysis during political turbulence. PLoS ONE 12(10): e0186836. https://doi.org/10.1371/journal.pone.0186836.

[5] https://www.reuters.com/article/us-greece-macedonia-foreignminister/greece-sees-breakthrough-soon-in-macedonia-name-impasse-idUSKBN1FL5V3

[6] In almost every case the old news remained online for a good 5-6 hours before it withdrew.

Mainstream media role

But what about the reputation of the traditional media, what used to be labeled as "mainstream"? According to a recent survey from Poynter Media Trust, 44% of Americans are convinced that media fabricate fake stories about the US President Donald Trump "more than once in a while". Another 24% believe that this happens "about half of the time", 14% "most of the time" and a 6% of the people surveyed believe that Media fabricate stories about Trump "all of the time"[7]. This comes as a confirmation of the bad reputation "traditional" Mass media have in the eyes of their audiences and readers. And of course the U.S. is far from being the worse in that regard. Greece has the lowest score of trust in both news media and satisfaction that government will do what's best for the country[8]. The data aren't too good for the rest of the countries of the so called Western world (North America-European Union). In the cases of Hungary, Italy, Poland and Spain the percentage of trust is lower than 40%, still dwarfing the less than 20% of trust in media and politics at Greece. This combination of lack of trust in the government, flow of information from official sources or professionals and the breakdown of trust on expertise[9] draws a very bleak image of the future, where populists and people equipped with nothing else but the will of power, will be able to claim more seats in national parliaments and, why not, the top political institutions themselves. So we are also talking about how to prevent the crisis of western democracies, a crisis of institutional delegitimization that influences the very core of our representative political systems, be it North America or European Union.

This combination of lack of trust in the government, flow of information from official sources or professionals and the breakdown of trust on expertise draws a very bleak image of the future.

[7] The Pointer Institute for Media Studies, "You 're fake news", *The 2017 Poynter Media Survey*, Saint Petersburg FL, November 2017.

[8] Pew Research Center, Spring 2017 Global Attitudes Survey, Q4 and Q42a-d.

[9] The most recent example is the outbreak of measles in European countries fourfold between 2016 and 2017. This is not only due to the increase of refugee flows, but also on the widespread – apparently false -notion that vaccination is causing more problems than the ones it solves. WHO, Press Release 19.2.2018 http://www.euro.who.int/en/media-centre/sections/press-releases/2018/europe-observes-a-4-fold-increase-in-measles-cases-in-2017-compared-to-previous-year

CONCLUSIONS

In the end it all comes to one very evident question: How fake news and disinformation campaigns can be tackled? There's one thing that must certainly be done. The main players must be summoned in one way or another, and participate in addressing this challenge. Otherwise, maybe regulation would be a harsh, but quite probably necessary and unavoidable choice. The walls are already closing in for "big boys" like Facebook, especially in terms of its failure to safeguard the platform against Russian malign influence. Even though Facebook is declaring that its 25.000 personnel had done everything not to jeopardize the integrity of the platform and keeping possible propaganda out, it seems that a little more than 100 hackers had actually pushed Russian propaganda through the most popular social medium of the world[10].

The main players must be summoned in one way or another, and participate in addressing this challenge.

Despite their sophisticated algorithms, Facebook and Google actually failed to recognize fake news and disinformation on a lot of categories of cases.

One of the most characteristic such examples, is the one of popular images that were doctored to provoke strong emotions[11]. And that was simply another case of suspected Russian trolling and indirect disinformation. Regulation is an ugly word, even more when it is uttered in countries with tradition in civic societies like U.S. Nonetheless, regulation is a much more tolerable, if not desired tool of dealing with market deficiencies (in this case it looks more like a security problem too) in the European subcontinent. And of course it isn't only about some market malfunction or quality of content, but about a hardcore security issue. This convergence of threats, against the function of a market (credibility is not only about news and information, but also trade and other types of more... tangible products) but also against the security of countries through hybrid warfare (fake news and disinformation campaign is regarded as such), may in the end speed up the developments in the direction of some kind of a consistent regulation that would impose limitations on all major players that disseminate information and, right now, are quite global and quite out of control. The future is already here, let's see if we can do something about it. ■

ABOUT THE AUTHOR:

Vassilis Nedos is the diplomatic and defense correspondent of the leading Greek newspaper "Kathimerini", author and curator of the kathimerini.gr "Security Bulletin" blog. He has been working during the last 17 years as a reporter and a political editor. He has appeared on several tv shows as a diplomatic analyst and presenter. He studied European History (BA, MPhil) and has taken part in research teams and historical conferences.

[10] Georgia Wells, Robert Macmillan, "Facebook battles new criticism after U.S. indictment against Russians", *Wall Street Journal*, 17.2.2018.

[11] Georgia Wells, Shelby Holliday and Deepa Seetharaman, "The Big Loophole that helped Russia Exploit Facebook: Doctored Photos", *Wall Street Journal*, 22.2.2018.

CYBERSEC

EUROPEAN
CYBERSECURITY FORUM

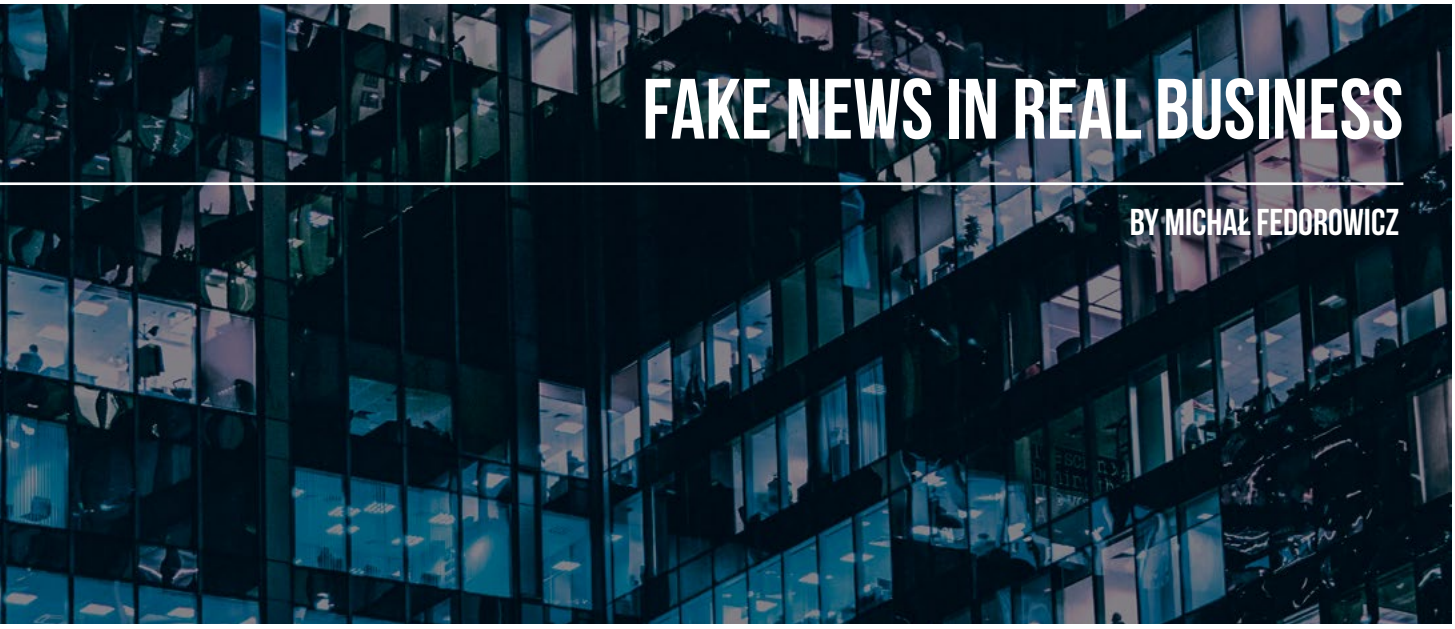
DON'T MISS THE 4TH EDITION

SAVE THE DATE 8–9 OCTOBER 2018

FOLLOW US ON:

#CSEU18

WWW.CYBERSECFORUM.EU



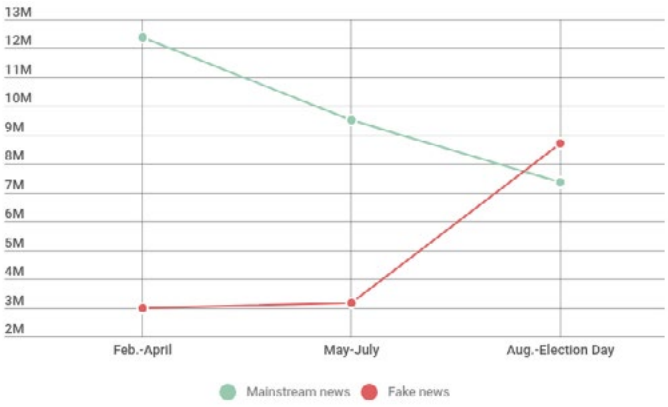
FAKE NEWS IN REAL BUSINESS

BY MICHAŁ FEDOROWICZ

According to the Collins Dictionary, fake news became the word of the 2017. Nowadays, it is a very popular term that made a world carrier through its presence in politics. Examples are many, such as the Brexit referendary campaign in 2016 or the 2016 presidential election in the U.S. The obvious link between misinformation, politics and social emotions provoked by this kind of activity is blotting out a much more complicated issue. While most national agencies try to fight this problem, identifying and punishing fake news creators, business representatives (corporate agents as well as small, family companies) from all around the world have to deal with this burden by themselves[1].

It is worth noting that fake news spreads not only through social media – the phenomenon grows in the traditional media, as well. According to research conducted by BuzzFeed during the presidential elections in the U.S., fake news is expanding its reach and drawing bigger broadcasts than real information. In most cases, fake news is just a tool aimed at financial and political benefits; however, it is also created by Internet haters and trolls. For media agencies, traditional and social alike (alongside all of the related branches), fake news is an escalating problem that causes the loss of social trust. Combating this phenomenon is very difficult – forged news is hard to distinguish from real information, especially in the era of quick and casual consumption of media content. This is hardly surprising, considering that this is the most popular way amongst Internet users[2].

Figure 1. Total Facebook Engagements for Top 20 Election Stories



Opinion's influence on business

We can find hundreds of millions of consumer reviews on the Internet. These are usually the recommendations of and comments about products, companies and their services. Since 88% of users trust the opinions they find online in the same way they trust personal recommendations, and 67% trust every review they see, it would seem that we should only

[1] http://www.independent.co.uk/news/uk/home-news/fake-news-word-of-the-year-2017-collins-dictionary-donald-trump-kellyanne-conway-anti-fa-corbynmania-a8032751.html

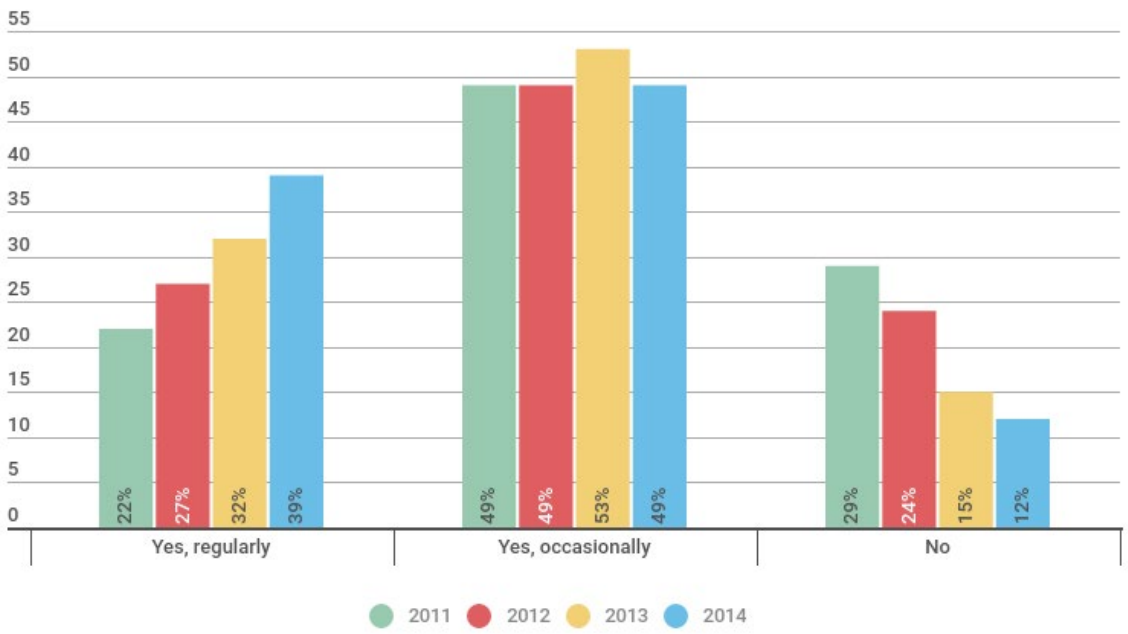
[2] https://www.buzzfeed.com/craigsilverman/viral-fake-election-news-outperformed-real-news-on-facebook?utm_term=.gvAZ07DQve#.yn91wrqB6o

find reliable opinions on the Internet[3]. Nothing farther from the truth. A report by the British CMA analysing the origin of online reviews shows how serious the influence of fake opinions actually is, on both decision-making and buying.

UK consumer spending after reading online opinions is estimated at around GBP 23.3 bln. These data show the importance of reviews.

There is a serious obstacle associated with online opinions – there are only two methods to supervise them:

Figure 2. Do you read online customer reviews to determine whether a local business is a good business?



Online review costs

CMA's report shows that 54% of adult Britons decide to buy a product after checking its online reviews. Furthermore, 6% of them browse blogs and videos before making their mind. If consider the overall consumer spending on products or services bought after checking posts on the Internet, we can see why the fake reviews market is so lucrative.

Expenses of UK Internet users (overall spending after reading opinions online):

- GBP 14.4 bln – travelling and hotels;
- GBP 360 mln – books;
- GBP 500 mln – CDs, DVDs and music;
- GBP 3.1 bln – electronics;
- GBP 3.9 bln– home improvement (furniture, detail work etc.).
- Providing an ideal product or service – 100% satisfied customers will not generate any negative feedback;
- Successful defusing of real negative reviews and their further conversion for the benefit of new customers.

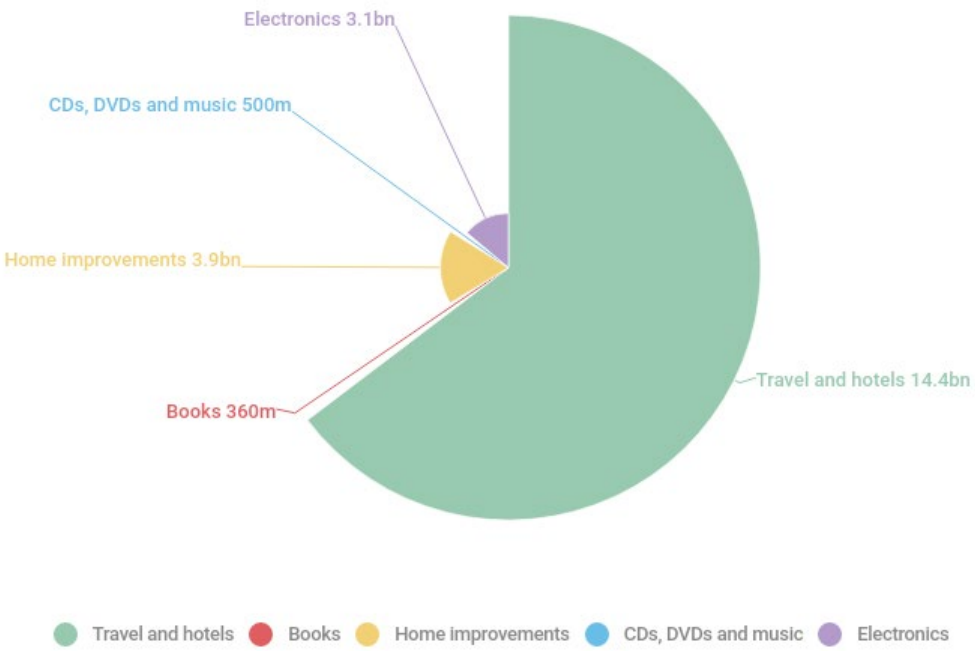
All of the above assumptions are quite obvious. Unfortunately, we live in the era of post-truth, where fake reviews sculpt our perception.

According to the CMA, the Internet is full of false opinions. Based on data from 2015, 15% to 30% of all comments on the web are fakes, and this value continues to increase. Some experts are positive that 45% of reviews are, in fact, lies[4].

[3] https://searchengineland.com/88-consumers-trust-online-reviews-much-personal-recommendations-195803

[4] http://www.inboundsystems.com/contractor-marketing-articles/fake-online-reviews-its-worse-than-we-thought/

Figure 3. Customer spending after reading online reviews



What kinds of posts are likely to be fakes?

In the opinion of CMA's experts, typical fake posts hide behind a mask of the promotion or review of a given brand, service or product. False opinions also include image vandalism performed on the competition.

The common traits of fake reviews are:

- They are commissioned – paid reviews are meant to glorify a product;
- False opinions attack the competition without any good reason and compare offers (glorifying a given product and criticising its competitors);
- 'Cherries on top' – reviews with a large number of likes (or other positive interactions);
- Fake reviews are often placed on anonymous sites, where it is difficult to post your own opinion[5].

Yelp.com, a popular U.S. review service reports that around 16% of all opinions posted in a year are actually fake.

False opinions demolish both a company's reputation and profits. According to research by Google, 70% of consumers will not buy a product after reading negative reviews (when most of them are fakes)[6].

It is worth noting that false opinions are very often the foundation for blackmailing a company. A common practice (also in Poland) is to post fake negative feedback on anonymous boards and demand a price in cryptocurrency for removing them.

How to spot a fake opinion?

- Online reviews describe the products/services of a company in a very similar style;
- A large number of comments about a product/service have been added in very short intervals (for example, every 60 seconds);
- False reviews are short and use expressions typical for advertisements (for example, 'the best', 'superb' or 'the one and only');
- Fake opinions are the most upvoted ones (in terms of the overall number of interactions);
- They are posted from the same IP address[7].

[5] Ibid.

[6] https://www.forbes.com/sites/investopedia/2013/01/25/can-you-be-sued-if-you-give-a-bad-review-on-yelp/#71d5eb4a1275

[7] http://www.inboundsystems.com/contractor-marketing-articles/fake-online-reviews-its-worse-than-we-thought/

Remember that fake reviews have to be removed as soon as possible. Leaving them online will result in a negative influence on business in the future.

However, statistical research does not take into account the thousands of small companies that become the victim of fake reviews every day. Corporations can try to deal with this issue with lawsuits and efficient PR actions, but small ventures are doomed to failure. Left alone without any help from government agencies, they fall into a deep crisis (or even go bankrupt) after a successful attack.

According to the latest data from the IPSOS analytical agency, the trust placed in information from the Internet is visibly dropping. This can be considered as a success in fighting against the political fake news[8]. However, this does not apply to the fake reviews of commercial products and services.

The travelling and hotel branch is a very common example. TripAdvisor's and PhoCusWright's research from 2014 shows that:

- 77% of travellers check reviews on the hotel they choose before making reservation;
- 80% of travellers read from 6 to 12 opinions of other guests;
- 73% of travellers look at photographs of the hotel before making a decision[9].

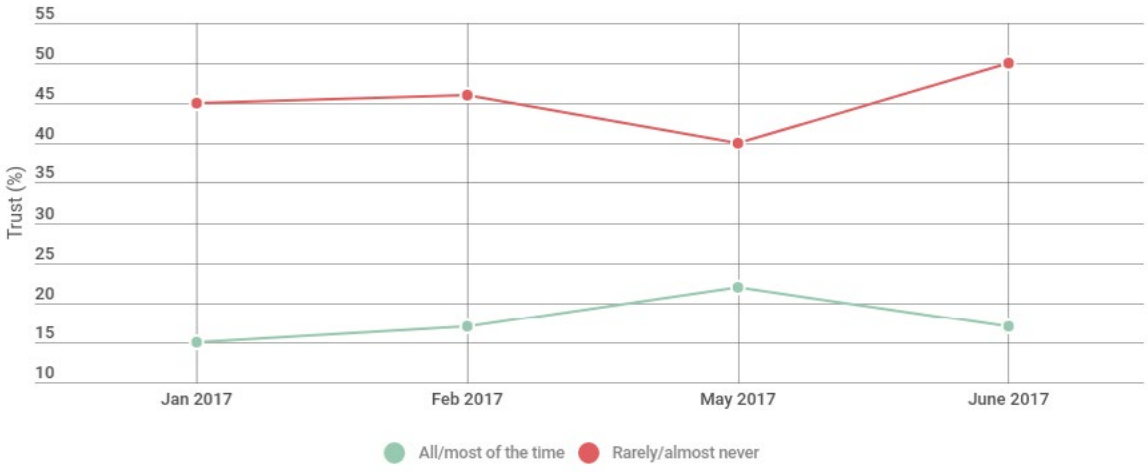
Guest reviews about a destination have always had a considerable impact on the entire branch, but the owners have realised how to deal with online opinions only recently.

Every single day, thousands of guests publish their opinions on hotels online, very often using websites such as TripAdvisor or the relevant message boards.

The largest research among hotel guests conducted by TripAdvisor in 2013 shows that more than 50% of 15,000 guests wrote an online opinion about the hotel they visited. More than 40% of them shared their opinion with their real-life friends through social media messengers or e-mails. According to the data, the online reviews of a given hotel spread on the Internet twice as fast as the traditional face-to-face opinions (which we trust the most).

93% of hoteliers claim that online reviews are the key to the future of their business. The dynamic growth of such travel portals leads to a quick spread of this kind of content. Ninety per cent of hotel owners say that online comments are one of the top three factors affecting their success[10].

Figure 4. I trust the news I read/hear on social media...



[8] https://www.ipsos.com/sites/default/files/2017-07/Trust%20in%20News%20Wave%204-Topline-2017-07-11.pdf

[9] https://www.tnooz.com/article/tripadvisor-online-review-insights-phocuswright-study/

[10] https://www.reviewpro.com/blog/tripadvisor-survey-shows-why-hotel-reviews-matter/

How does fake news spread so quickly?

Despite their cleverness and great performance, social media algorithms (which are very similar to each other in terms of mechanics) cannot control how quickly lies spread among all Internet users. This kind of infections always works in the same way – with more interactions (likes, comments, shares) comes the higher chance to spread this informational virus.

In the world of a constant fight against fake news, the human mind still holds the greatest power. Facebook and Google are hiring thousands of workers to read and verify content published on their pages. Governments are encouraging social media providers to cooperate with local watchdogs, foundations and journalist think-tanks. Furthermore, some countries have introduced special buttons for reporting fake news to the portal administration[11].

Computers may still lack advanced algorithms that would let them fully comprehension the presented content, but they are doing very well in automatic linguistic analysis. For example, they can verify whether particular information is actually fake news. Social media content with the word/hashtag/phrase 'fake news' were published in 2017 and analysed with the Natural Language Processing (the popular NLP).

Between January to December 2017, there were 115,000 posts that mentioned fake news. Most of them (73%) were published on Twitter. The successfulness and efficiency of fake news is always a combination of two factors: the trust gained by the distributor of the information (for example, the social media profile that shares a post) or the headline/title/first words of the news[12].

How much does fake news cost?

According to research by Trend Micro, a specialised content marketing agency charges USD 30 for writing a piece of fake news. A full malign campaign against a journalist costs around USD 50,000.

Trend Micro, as a cybersecurity company, analysed the costs of conducting informational campaigns for many different marketing subjects that offer their services in Chinese, English, Russian and other languages. A content marketer offers an entire range of options. At the Chinese market, creating a real-looking account on the local social media platform Baidu (the equivalent of Google) costs USD 2,600. A single piece of fake news costs only USD 30. A short YouTube movie costs a potential client around USD 620. There are also packages of more complicated services: defaming chosen journalists, provoking social turbulences or putting pressure on a political party. For example, destroying the image of a journalist costs around USD 50,000, which includes publishing fake news, spamming their Twitter account or posting hateful comments on their Facebook profile[13].

Trend Micro's experts revealed the price list of a Chinese company supporting the local propaganda industry, Xiezoubang. They charge USD 15 (100 renminbi – Chinese currency) for writing a fake article of 600 to 800 words. An article of 1000 to 1500 words costs USD 30. Prices depend on the preferable theme of the platform they are published on. Placing fabricated news on ten common websites displayed in the Baidu search engine costs USD 116 (800 renminbi). The cost for a specialised platform – such as an IT or entertainment platform – is around USD 174. Fake news in the local media costs only USD 72[14].

On the Russian market, there are multiple companies which offer services using propaganda mechanics, such as SMOService. Their price list starts with products for only USD 2. A hundred dislikes on YouTube costs USD 1.70 (100 roubles). A hundred negative comments on the same platform costs USD 2.60 (150 roubles). Ten thousand fake page views costs USD 17 (1,000 roubles). A single piece of fake news costs USD 802 (45,200 roubles). There are also much more expensive services. Preparing 20 short videos to appear on YouTube's homepage for 2 minutes costs almost USD 8,000 (45,0000 roubles). A single video

[11] https://www.theguardian.com/technology/2016/nov/14/facebook-fake-news-us-election-news-feed-algorithm

[12] https://medium.com/@Genyunus/detecting-fake-news-with-nlp-c893ec31dee8

[13] http://www.bbc.com/news/technology-40287399

[14] http://www.wirtualnemedia.pl/artykul/ile-kosztuje-fake-news-jak-to-zrobic

costs USD 621 (35,000 roubles). Preparing and running a VIP social media account costs from USD 106 to USD 124 (5,990 to 6,990 roubles)[15].

In addition to describing the mechanics of disinformation, the authors of the report also give advice on how to recognise fake news portals. Users should pay attention to: clickbait headlines, suspicious site addresses resembling real ones (for example, misspelled site names), mistakes in publications and homepages that raise doubts. Users should also look out for: irregular publication periods, absence of the author's name or references to sources. There exists no method for proving the authenticity of online news. Lies apparently spread much quicker than the truth on the Internet – especially if they appeal to the lowest instincts[16].

CONCLUSIONS

Taking into consideration the efficiency of fake news, we can assume that, as with political issues, without systemwide solutions many companies are forced to deal with this threat by themselves or with support from specialised PR agencies.

Here are some internal actions that every company should take:

- Permanent monitoring of comments and news published on their business;
- Designing procedures to fight with attacks and fake news;
- Clearing false opinions about their business from the Internet.

Actions that governments and business agencies can perform to fight with fake reviews include:

- Designing a website certification system that will check if a website verifies their users and their opinions (for example, with the requirement of adding the reservation number from a hotel or providing a bill from a given destination);
- Screening out company sources of fake news;
- Helping enterprises that fell victim to false negative reviews. ■

All the charts used in the article are taken from: http://politykawsieci.pl/

POLITYKA W SIECI

ABOUT THE AUTHOR:

Michał Fedorowicz is expert of management and protection of image rights on the Internet. He is founder and co-owner of the biggest networking agency Apostołowie Opinii which deals with protection of image rights, controls and scans online reviews, prepares e-image audits and optimizes image searches in search engines.
Monthly, 180 companies are serviced by Apostołowie Opinii.

[15] Ibid.

[16] https://blog.trendmicro.com/trendlabs-security-intelligence/online-economy-fake-news/

PUBLIC POLICY VS DISINFORMATION: DEVELOPING EUROPEAN UNION'S APPROACH

BY BARBARA SZTOKFISZ

Under the framework of the Digital Single Market policies, the European Commission is analysing the problem of disinformation and fake news together with platforms, news media, research and civil society organisations. Specific solutions must embody fundamental values of democratic societies and respect the freedom of expression, guarantee media pluralism and the right of citizens to diversified and reliable information. The complexity of the problem as well as its strong relation to the principles highly valued by western societies make specific responses and solutions extremely difficult to define. The role of the Commission is to support the multi-stakeholder process aiming to find right and coherent policy responses to address the spread of disinformation[1]. One of the Commission's steps within this framework was setting up in January 2018 the High Level Expert Group (the HLEG) on Fake News and Online Disinformation[2]. The HLEG's mission is to define the scope of the phenomenon and to advise on European policy strategy to counter disinformation spread online. The main result of the HLEG's work is a report containing best practices, recommendations, responsibilities of stake-holders and suitable responses, all in the light of fundamental principles.

DEFINITIONAL ASPECT

The report focuses mainly on problems related to the disinformation defining it as *false, inaccurate, or misleading information designed, presented and promoted to intentionally cause public harm or for profit*. The public harm includes mainly threats to democratic political processes and sectors such as health,

[1] https://ec.europa.eu/digital-single-market/en/fake-news, access date: 15.03.2018.

[2] The HLEG consists of 39 members and is chaired by Prof. Dr. Madeleine de Cock Buning.

education and finance. Activities operating for profit, in turn, aim to promote disinformation for economic gains, political or ideological goals.

In the opinion of experts, the term 'fake news' (often used interchangeably with the term 'disinformation') may be restrictive and inadequate in describing this phenomenon. 'Fake news' include wide spectrum of activities, from relatively low-risk forms (such as honest mistakes made by reporters) to high-risk forms (such as malicious fabrications or automated amplification techniques). The term 'fake news' is also inadequate because the content of 'disinformation' is not always completely 'fake' and is more concentrated on the circulation of disinformation (networks of fake followers, targeted marketing, organized trolling, and much more) and less on the production of disinformation. 'Fake news' may be also misleading because of its wide use by politicians who use the term to disagree with the content they find unfavourable.

DISINFORMATION IN THE EUROPEAN UNION

Problem of disinformation is multi-facetted and involves the ecosystem of political, social, civic, and media actors. Although many specific forms of disinformation have been developed by digital tools, some fundamental issues predate the move to digital media. Experts from the HLEG highlight four main aspects of this phenomenon in the European Union. (1) Political actors (foreign governments or domestic groups) may be involved in the process of disinformation in order to determine the integrity of the political processes. The level of respect for media freedom and independency vary across European political actors. (2) Standards of professionalism are not the same for news media. Some of them contribute to disinformation problems, weaken the overall trust and undermine democratic processes. (3) The civil society plays an important role in both fact-checking and verification as well as in circulating false and misleading content. Highly polarized societies are particularly vulnerable for sharing ideologically motivated disinformation. (4) The role of large social media platforms is not yet well understood. Their growing power should come with growing responsibilities.

RESPONDING TO DISINFORMATION

The understanding of the scale, scope and nature of the disinformation phenomena is crucial to design appropriate and tailor-made responses. They should take into account the complexity of the problem and form the so-called multi-dimensional approach. The report lists some of the already taken measures by various stakeholders[3] and good practices which respect fundamental values like freedom of expression. They should be distinguished from bad and simplistic practices like censorship and online surveillance. According to the HLEG, good practices fall into three major groups – (1) transparency, (2) trust-enhancement, and (3) media and information literacy. The first category contains initiatives influencing "findability", privileging credible content in algorithm rankings, identifying and removing disinformation sources (illegitimate accounts) and ensuring the proper environment for news media and journalism. The second category is strongly connected with measures based on artificial intelligence and machine learning algorithms aiming to define specific features of the disinformation as well as ranking news and therefore enabling the exposure of fact-checked information. However, there is no consensus on the level of transparency of algorithms. Some platforms warn that an excessive level of transparency may lead to misuses of the system. The third category of best practices aim to foster responsible social media use and critical thinking on propaganda. Civil society organisations are very active in this area and develop programmes on media literacy and conscious behaviour in the digital ecosystems.

INTERVENTION AREAS

The HLEG focused on five major intervention areas in order to create specific responses and recommendations for both public and private stakeholders:

A. Transparency

The transparent ecosystem is the key element in building appropriate responses to digital disinformation and supporting users' ability to critically distinguish between quality content and disinformation.

[3] Governmental measures are not analysed.

It helps to understand the motivations, dissemination process, and sources of information so that its recipients could better evaluate the credibility of the news they access. In this respect, following actions are recommended:

- Platforms should provide information whether the popularity of the specific content is the result of artificial amplification techniques or is supported by targeted investments. Political advertising should be clearly labelled as paid and sponsored content during a campaign.
- Transparency Indicators (based on professional codes of conduct and users' expectations) should be created so that fact-checked and quality news are easily findable on the Internet.
- Media platforms should reduce the risk of mistakes to the minimum (by training journalists, creating fact-checking teams) and should provide the system allowing to report the appearance of false information on their platforms.
- Platforms should provide the information on the functioning of algorithms responsible for selecting and displaying information in order to help to understand the information dissemination patterns. This step should be, however, made with caution.
- European Commission and Member States should foster the cooperation between various stakeholders (media organisations, professional newsrooms, platforms, academic researchers, fact-checkers, advertising industry and civil society organisations) and therefore develop innovative and transparent fact-checking methods[4].

B. Media and information literacy

Media and information literacy acquired strategic importance in the digital age and constitute basic educational competences. They help societies to keep the pace of the profound changes and enable critical thinking and good personal practices. Actions focused on the strengthening the media and information literacy are more preventive than reactive solutions. The HLEG proposes following activities for their improvement:

- Media and information literacy should be included to the list of "EU key competences for life-long learning" and should be the reference for future educational reforms.
- National governments should add them into school curricula.
- EU should support training for teachers (through Erasmus+ or similar schemes).
- Organisations involved in media literacy should elaborate best practices and constantly evaluate them in collaboration with various stakeholders.
- EU should support initiatives that take into account the specific needs of sub-regions (e.g. Eastern Europe).

C. Empowerment of users and journalists

Empowering both users of platforms and media professionals is crucial to boost the resilience of society to disinformation. This can be done by the increased users' control over the content they access online and by the journalists' knowledge of basic tools aiming to verify the content in order not to spread disinformation. Within this category, following actions could be addressed:

- Platforms should promote client-based interfaces, e.g. plug-ins or applications for browsers to give users the control over the access to the content.
- There should exist tools allowing users to report the false information and correct it. Such tools should be part of the competitive market and users should be able to select tools they consider the most suitable.
- Journalists should have access to trainings focusing on media literacy and the use of new technologies supporting the identification of false information.

[4] The HLEG supports the creation of European Centres for interdisciplinary and independent evidence-based research on problems of disinformation that could be run within national research organisations as well as the possibility to set up by the European Commission a Centre of Excellence, acting independently and in full autonomy.

- The EU should increase R&I funding dedicated to news media innovation (fact-checking tools, artificial intelligence, big data for media and more).

D. Diversity and sustainability of the news and media ecosystem

The fight against disinformation should not include any form of direct or indirect censorships. The media pluralism constitutes a cornerstone of democratic societies and is indispensable to offer high quality content to users. In the light of the above, the HLEG lists following actions:

- Public authorities should support the press freedom and media pluralism by creating the proper environment (both de facto and de jure) and ensuring the rights to free expression and diverse information.
- There should exist projects supporting quality journalism, including i.a. data literacy and data collection.
- The EU should (under the Horizon 2020 programme or its successor) include media-related calls.
- National public authorities should not have control over what can and cannot be accessed online. The censorship is neither justified nor efficient to counter disinformation.

E. Process and evaluation

In order to ensure that all the above actions are meaningful and effective, the process of implementation and consequent evaluation is indispensable. The HLEG propose therefore to create a general, European-wide Code of Practices that would reflect roles and responsibilities of online platforms, media organisations, fact-checking and research organisations. The establishment of Code of Practises should be then followed by the regulatory activities ensuring the implementation of the recommended actions. Ten guiding principles supported by the HLEG are the following:

1. Platforms should adapt advertising policies (including “follow-the-money” principle) to discourage dissemination of disinformation for profit.

2. Platforms should ensure transparency with regard to processing of users' data for advertisement placements.
3. Platforms should ensure that sponsored content is distinguished from other content.
4. Platforms should enable access to data for fact-checking and research activities.
5. Platforms should make available to users advanced settings and controls.
6. Platforms should take measures to improve the visibility of reliable news.
7. Trending news items should be accompanied by related news suggestions.
8. Platforms should provide tools to enable users to link up with trusted fact-checking sources and allow them to reply.
9. Platforms applying flagging and trust systems that rely on users should implement safeguards against their abuse.
10. Platforms should provide relevant data on the functioning of their services and information on algorithms.

CONCLUSIONS

Although the report is undoubtedly a good step in building strategic and common responses to counter disinformation in Europe, it is only a start of the process. The phenomena might be much more complex than described by the HLEG. Disinformation is also a challenge at the level of nation states, therefore, it is necessary to include, apart from technical and social tools (which are addressed in the report), tools specific for the foreign policy domain. Also, the main attention in the report is focused on media platforms and professional journalism sector, while the origins of the problem and the risk landscape are not at all highlighted. History has proven that Central and Eastern Europe is strongly exposed to a wide range of cyber operations aimed at people's perception and that this region is the first which experienced the information warfare consequences. The origin of disinformation as well as its foreign policy context cannot be ignored in building specific tailor-made solutions. ■

ABOUT THE AUTHOR:

Barbara Sztokfisz has worked in the Kosciuszko Institute since 2017 as Junior Research Fellow and Project Manager of the European Cybersecurity Forum – CYBERSEC. She holds a Master degree in International Economics and Bachelor Degrees in European Studies and French language and literature. She is also PhD candidate in Economics at the Cracow University of Economics. She studied International Economics at Université Paris 1 Panthéon-Sorbonne. Her interests encompass processes of economic change in the context of new technologies, economic growth and international security.

LOOKING INTO THE CYBERFUTURE THROUGH THE EYES OF **YOUNG LEADERS**

The Kosciuszko Institute is launching a new initiative addressed to young, ambitious and visionary students interested in strategic and interdisciplinary aspects of cybersecurity from most renowned academic institutions of the entire world. Our aim is to create a coalition of educational institutions that will patronize the quest for young leaders aware of high significance of cyber challenges and help them boost their careers in the domain.

WHAT?

We warmly invite MA and PhD students to take part in the CALL FOR PAPERS on challenges in cyberspace within such domains as international relations, economy, national security, defence, etc.

WHEN?

The IV European Cybersecurity Forum – CYBERSEC will be held on **8 - 9 OCTOBER 2018** in Krakow, Poland.

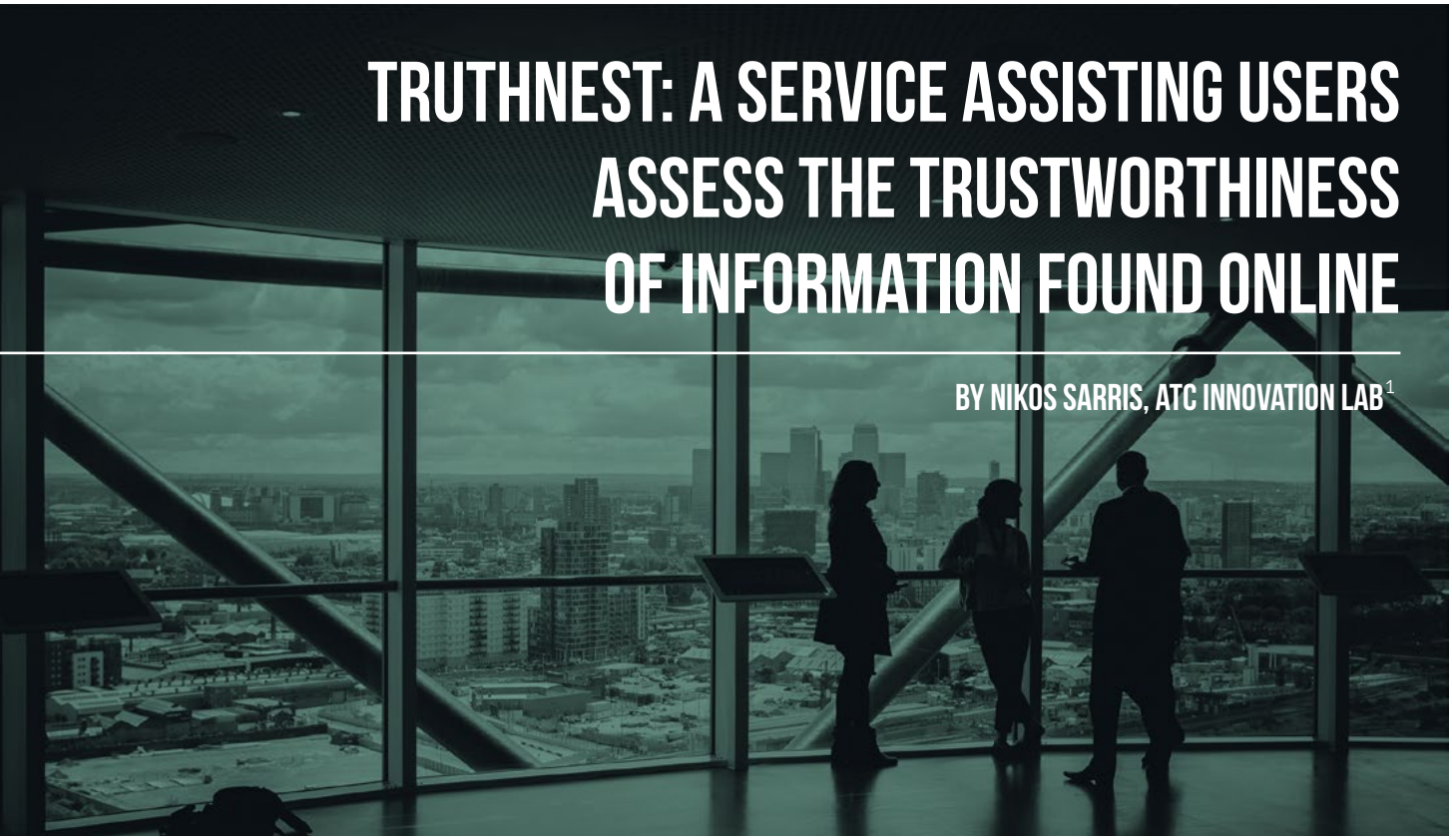
HOW?

The universities willing to take part in the consortium are responsible for sharing the information about the call for papers with their students. These universities' logos will be exposed while promoting the endeavour.
The papers shall be sent till the end of June to **editor@cybersecforum.eu**.
Please find publication guidelines attached.

WHY?

Once a year, the mesmerizing city of Krakow becomes the European centre for strategic discussions on cybersecurity, a place of inspiring debates, presentations and informal conversations.
Authors of 3 best papers will be invited to take part in the specially dedicated panel discussion entitled *Young Cybersecurity Leaders looking Ahead* during the IV European Cybersecurity Forum – CYBERSEC.
The panel will be held under the auspices of the overmentioned coalition of universities.
CYBERSEC is a public policy conference dedicated to the pivotal aspects of cyberspace and cybersecurity. CYBERSEC gathers more than 1,000 participants from around the world, including political decision-makers, diplomats, experts, business leaders and academic researchers.
Winners will be granted:
- VIP pass for the whole conference including travel & accommodation and unlimited networking opportunities,
- Invitation for afterhours events, e.g. CYBERSEC Banquet,
- Publication of their articles in the **European Cybersecurity Journal.**

CYBERSEC
YOUNG LEADERS



TRUTHNEST: A SERVICE ASSISTING USERS ASSESS THE TRUSTWORTHINESS OF INFORMATION FOUND ONLINE

BY NIKOS SARRIS, ATC INNOVATION LAB[1]

1. Introduction

We are currently experiencing a social web explosion, which is giving the power of speech back to the citizens who had been practically deprived of this since the gradual explosion of the population that made it impossible for news to travel via the old channel of the 'word-of-mouth'. We now live through the new phenomenon of the 'e-word-of-mouth', which is travelling in rapid paces and huge volumes through tweets, posts and blogs. This creates the opportunity for direct access to information coming from first hand sources, as it was happening centuries ago in small societies. The problem is that the scales are now very much different and all the sides have their say in this big bang of gossiping: truth and lies, positive and negative, genuine and fake. The truth is out there but can we discover it?

We now live through the new phenomenon of the 'e-word-of-mouth', which is travelling in rapid paces and huge volumes through tweets, posts and blogs.

TruthNest aims to provide journalists and the public with a tool to help filter reality from noise.

Social Networks not only provide a globally accessible real-time interface with primary sources of information, they also radically change mainstream content distribution and consumption. Established news brands continue playing an important role on that matter; however people tend to read all the more news shared by their friends or other social network relationships as objectivity of journalists, institutions, financial and other corporate entities is increasingly questioned.

TruthNest aims to provide journalists and the public with a tool to help filter reality from noise.

Equally importantly Social Networks enable users to share their views on topics, persons, brands and products, making them the vastest potential source for opinion-mining, sentiment analysis and trends prediction.

[1] http://ilab.atc.gr/

2. TruthNest Analysis

2.1. Overview

In our work, apart from trying to gather and organise information coming from Social Media, we are also trying to verify it. In this context we have developed 'TruthNest': a service attempting to assess the trustworthiness of information we find online.

We have organised this around what we call the 'triple-C': we are developing or adopting metrics that can help users assess the credibility of information under the following pillars:

Contributor – This involves all data relevant to the source of information, such as its history, its connections and interactions in the social circle and any other information that can assist in the profiling of any contributor of content.

Content – This includes all multimedia analysis methods that can provide clues about the meaning of the content, but also indicate possible manipulations and fraudulent use.

Context – Under this pillar we investigate all contextual co-occurrences which strengthen or weaken the confidence built around several concepts like credibility and suspicious behaviour.

We have organised this around what we call the 'triple-C': we are developing or adopting metrics that can help users assess the credibility of information.

The results from the above steps are weighted and combined together to provide a metric that will give a sense of truth to the user, while giving access to all the evidence that leads to this result, so that the user can also subjectively decide on how credible every piece of information is. Although this is work in progress, we have identified many methods and metrics that are already under development.

2.2. A wide range of metrics

We employ the most complete array of metrics to assess each modality. The obtained values are statistically processed in order to present the user with data that make sense and provide valuable insight as to the various modalities under examination.

The table below summarizes metrics that are partly or fully developed, or under research. Our implementation currently covers Twitter as the main source of information.

Contributor	**Reputation**	**What do people think of this source of information?** Analyse comments towards a given source of information in the course of time, in order to discover sentiments and opinions towards this source. Use crowdsourcing and gamification mechanisms to trigger higher participation for comments and opinion sharing.
	History	**What is the past activity of this source?** Information about how active a given source is, also combining it with validity information (when did this source appear, how frequently has it been posting, what is the validity of previous posts based on other members' opinions?).
	Popularity	**Who cares about this source?** Information about how many and what kind of people are following the activity of this source, and how many are reading or are recommending this activity to others.
	Influence	**What happens because of this source?** How much does this source trigger activities, such as re-posts, discussions or comments? Are things happening because of what this source is posting?
	Presence	**What kind of source is this?** Information about the type of source (e.g., individual, organization, officially verified account, etc.). Is the same source present on multiple social media platforms?

Content	**Reputation**	**What is the reputation of linked web content?** Do the linked web addresses lead to reputable sites? (e.g., in terms of domain reputation, page rank, or properties of the contributors to the content). What do other people think of this linked web content (does it have a high readership? Quality of destination? Can we find positive or negative comments?)
	Provenance	**What is the history of linked web content? Can we trace the original occurrence of the content and its whole path across sources, places and time?** Information about the origin, update rate and freshness (or age) of the linked content.
	Popularity	**Who is interested in this content?** Information about how many and what kind of people are following this content.
	Influence	**What happens because of this content?** Analyse if this content is triggering discussions in the social sphere and what actions are taking place after the posting of this content.
	Originality	**Has the same content been used in the past?** Check whether the content or parts thereof have been used in the past (e.g., reused text or images that have appeared in the past).
	Authenticity	**Has the content been tampered with?** Check whether the content has been changed with respect to its original state.
	Objectivity and Diversity	**Are views presented from all sides?** Does an article (in case of linked web content) present views from all involved sides? How different are the opinions found for people, content, or general entities?
Context	**Cross-check**	**Are there multiple similar reports?** Are there many different and independent reports / mentions etc. about the same thing?
	Coherence	**Is the content internally and externally coherent?** Information about the coherence relations between sentences inside the content, or between the content and tags, attached web-links, or attached multimedia.
	Proximity	**Has the report originated where and when it is claimed it originated / was produced?** Comparison of the geo-temporal positions of the report and the event it is referring to.

We currently research even more metrics to be included in the following development cycles. We feel that an extensive array of metrics like this, presented in a comprehensive and transparent way can significantly help journalists distinguish what is true and what is not in the first critical hours or minutes when news first emerge in the social media.

2.3. The "Truth" in TruthNest

Our intention, apart from consuming this analysis, is that TruthNest users are able to provide feedback as well. They should be able to flag as true or false another user's claim and also provide supporting material should they wish to do so. Human input is critical when trying to determine the truthfulness of a claim.

We should be able to infer the probability of a post being true in the first critical time when it emerges, given TruthNest's users assessment. As mentioned, TruthNest users will be able to vote on whether an emerging post is true or false, among other functionalities. Assuming that the truthfulness of a particular post can be verified a-posteriori, we can calculate the probability of an emerging post being true, depending on users' historical predictions. In addition,

we can assign credibility scores to each user, depending on their performance in predicting whether past emerging posts were true or false. The actual confirmation of the post's truthfulness can be done in various ways, at any point later. It is important to note that journalists state that they are very interested in being able to tell whether a post is true, during the very first minutes when it emerges. Therefore we assume that for an emerging post the reality is hidden when it emerges. TruthNest users can cast their opinion on the hidden reality, given the knowledge of the context, their own research during the first minutes and their activity on the social media (the so-called "human algorithm"). As stated, we also assume that the hidden reality is revealed at any point later in time. Participation and feedback can be reinforced by a gamified environment.

It is important to note that journalists state that they are very interested in being able to tell whether a post is true, during the very first minutes when it emerges.

2.4. Technology

A number of methods are involved in calculating the metrics presented, including:

- ***Social Network API calls:*** refers to data that are primarily available through the particular social network's web services (the network being Twitter, Facebook or any other source to which the particular metric applies). The data are retrieved by calling certain methods in the API of the social network under examination. The metric's computation (e.g. M2, M3, M4 etc.) may involve processing this data by the logic layer before presenting the user with the actual result. Similarly, in other metrics we use the Alexa API to get the ranking of a website and image analysis APIs to detect whether a posted picture has been tampered, if it has been used in the past etc.
- ***TruthNest data layer:*** Users will be able to verify or flag as false a user's announcement and also provide supporting material, through the user interface. Human input is critical and there is a number of metrics evaluated against "credible" users. "Credible" users are considered to be the ones performing over a certain threshold.
- ***Sentiment analysis*** refers to the technology of extracting sentiment by first performing natural language processing on given texts. Our sentiment analysis engine is medium-specific, tailored to each social network's dialect. We implement the best suiting analysis model -including sentiment lexicons and machine learning- depending on the source and will use regression for fine-grained sentiment evaluation to inform the user through the corresponding metrics. Entity extraction and sentiment analysis will be tailored to social networks parlance, i.e. abbreviations to meet Twitter's characters restriction, Facebook's "social steganography" etc.
- ***Entity extraction*** refers to the identification of certain entities inside the text, such as events, persons and topics. By examining the metadata of a picture (for example several sites and social networks allow geo-tagging of announcements and multimedia content) and extracting from the text the event to which it is associated, we can determine whether the content was announced close to the position and time that the event actually occurred.

3. Visualization

One of the most important aspects of a product is the ability to engage its users and create retention. To this aim we design and implement rich visualizations of the data which are also interactive. The described analysis is transparent and all data discussed previously are presented to the user interactively, at the desired level of granularity. No "magic numbers", no excess of information either: no confusion.

Visualization is a key feature but it is also important to identify that this may not be enough to create retention. To promote retention, users must be able to input information within the product, feel the compulsion to return to it and check their status and the status of the ecosystem and finaly support virality.

One of the most important aspects of a product is the ability to engage its users and create retention. To this aim we design and implement rich visualizations of the data which are also interactive.

The data loop requires that TruthNest users, should not simply analyze information. They should also be able to input data within TruthNest. Data might be information related to the posts they discover and analyze in TruthNest, evidence that the information is actually true or false. They might be able to sketch a story within TruthNest by piecing together information they have found and analyze from TruthNest, together with notes, attachements etc. They might be able to make this information public (i.e. share it in other social media), private or share it with particular users inside TruthNest. Finally, TruthNest may provide an API to allow integration of the "story sketches" or other services with external systems. Importantly, they will be able to insert streams from their social networks lists and create dynamic streams based on their own filters (location, keywords etc), from within the interface.

4. Domains of Application and Impact

The original TruthNest service was developed to support media and citizen journalists as well as news consumers verifying information emerging on the social media. The technology itself however is also applicable to other domains, subject to necessary modifications. In fact the more specific the domain is, the easiest it is to achieve higher accuracy; news in general is a rather broad and challenging application domain.

The technology itself however is also applicable to other domains, subject to necessary modifications. In fact the more specific the domain is, the easiest it is to achieve higher accuracy.

Journalism and New Media – As previously mentioned, the first prototype was developed for promoting crowdsourcing citizens journalism and enable journalists verify the vast volume of information available on Social networks. Motivated by the increasing interest of the public to news emerging on the social networks both by primary sources as well as mainstream news brands and the conversation built around it, we aim to provide

journalists and the public a tool to help filter reality from noise. For this purpose we bring together all possible automatic controls and metrics into a transparent environment to help users:

- Locate possible credible sources of information efficiently in the critical interval between the first minutes after an event occurs and before the social media channels are flooded by noise.
- Verify authenticity of information posted during turmoil situations where information flow is blocked between contro lled media and social media polarization and even propaganda.

At the same time we continue to value and incorporate human input as one of the most important means of identifying what is true and what is not. As Twitter seems to have a special importance when it comes to news from primary sources, the first prototype was developed based on it. More social networks will be incorporated in subsequent phases.

Finance and marketing – Tracking collective sentiment about certain brands and products can be a valuable enhancement for informed financial and marketing decisions. Marketers can gain direct insight into the sentiments caused by their campaigns and the advertised products. Stockbrokers can gain intuition on the collective sentiment about certain companies and therefore the corresponding stocks.

Social media are also increasingly being used as campaign channels for marketers that look for cheaper alternatives. “Internet memes” and “guerilla marketing” techniques are employed to reach consumers with often impressive efficiency. Accurate social media analytics provides with impact insight and helps reaching the desired audiences more efficiently.

In the financial domain, a growing body of evidence shows that financial institutions of all kinds become gradually less trusted due to their perceived role in the ongoing financial crisis. TruthNest can add a social analysis dimension on websites providing comparison of financial products and services providing expert opinion for investment purposes.

TruthNest can also be applied in many other domains including product reviewing, public opinion analysis, political candidacies and more.

5. Conclusions

Our past and ongoing work on Truthnest has been described providing information to the level we can disclose due to the commercial status of this service. TruthNest has been available as a commercial online service since 2015, but is continuously enriched with new features and the latest information is always available under www.truthnest.com. Our work has been supported by two R&D projects co-funded by the European Commission: REVEAL (https://revealproject.eu/) and SocialSensor (http://www.socialsensor.eu/). ■

ABOUT THE AUTHOR:

Nikos Sarris is heading the Innovation Lab of ATC, a software development company based in Athens Greece. He has been working for more than 20 years in R&D projects as a researcher, project manager and coordinator of large multinational consortia. In the latest years, he has mainly been involved in media related projects focusing in the semantic analysis and ‘understanding’ of multimedia news content.

TECHMO

Techmo is a spinoff of AGH University of Science and Technology in Krakow, Poland. The company implements solutions in the field of audio, speech and language technologies. It was formed by qualified specialists from AGH UST. Techmo focuses on allowing voice control of devices to become more widespread. Currently, it is involved in providing technology for IVR (Interactive Voice Response) solutions for customers such as Energa or Fortum. Techmo cooperates also with Pacific Voice & Speech Foundation from San Francisco in order to build technologies for logopedic applications. Techmo is also conducting project "Integrated system for supporting the teaching process for the purposes of raising the efficiency of operations in KSRG domain" where is responsible for spatial audio simulation and physical effects simulation. The project aims at building a firefighters training simulator using Unity engine and Oculus Rift.

TECHMO - MAKING EVERY VOICE MATTER

Just think about how much easier life would be if we could control everything around us by voice. Talking is the natural way of communicating for most people in the world. Not clicking, not touching - simply speaking. Thanks to Techmo's solutions, voice can be used for various purposes, including electronic device control, speaker identification (biometrics), 3D sound simulation, and automatic speech recognition. Users no longer have to remember their PIN codes or passwords. It's enough that they speak in their own voice and they will access their accounts quickly and easily. It's safer than using fingerprint too! As a university spin-off, Techmo is run by some of the greatest minds in the field of voice technologies. Its technologies have been implemented in a few of the biggest Polish companies and now Techmo is reaching out to global customers. All you need is voice.

VOICE COLOR - SPEAKER VERIFICATION AND IDENTIFICATION

Widely used standard process of identification and verification using password or PIN code is not only uncomfortable for customers, but also expensive for a company. Every call to helpline is connected with necessity of finding or recalling PINs or password and then entering it to the system. It takes time of customers as well as Call Centre consultants.

Biometric voice identity verification with IVR system allows shortening of user identification time more than 4 times and rising the authorization security level at the same time. In contrary to the password, which can be stolen, our voice is our unique property similarly to fingerprints or iris. It is guaranteed that customers' data are properly secured and access to them is quick and comfortable.

The Voice Color allows remote authorization of access to services and resources offered through teleinformatics channels:

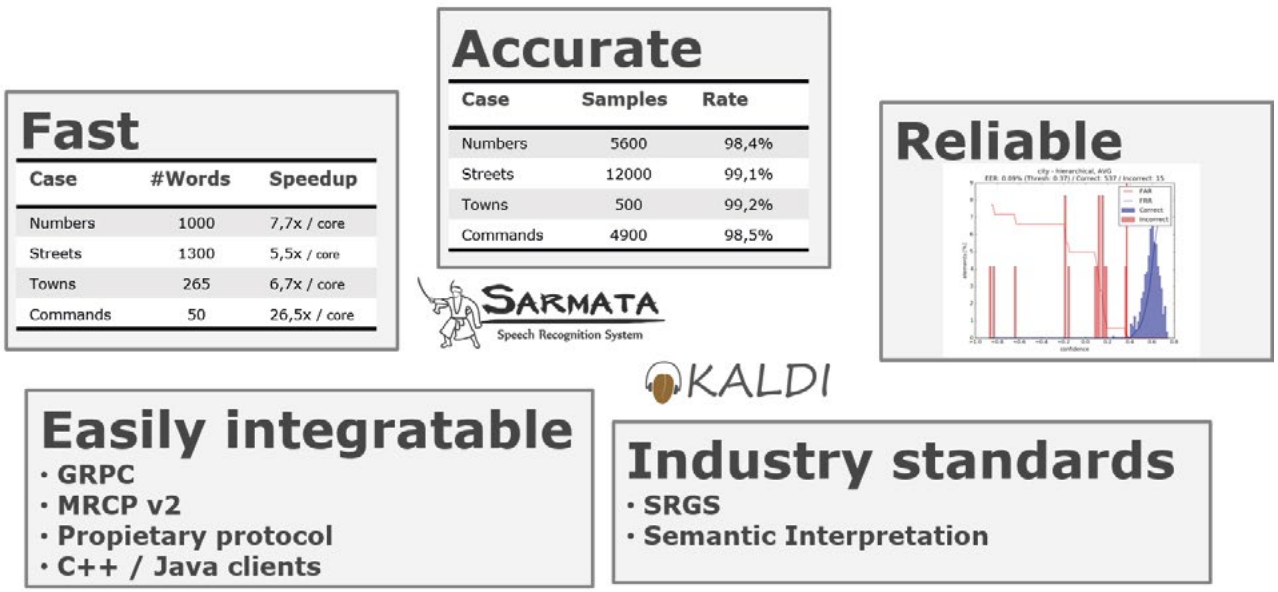
- phone calls (including GSM)
- VoIP internet telephony
- Internet
- mobile applications
- info-booths.

Identity verification does not require memorization of password or PIN - the password is a user's voice itself!

Registration for verification involves speaking 4 times a short phrase - biometric password, which will be used for verification. All users uses the same phrase, for example "I confirm my identity". It is possible to adjust the text of biometric password to the needs of particular deployment. In case of identification any content of the recording is allowed but it has to be longer.

SARMATA 2.0 AUTOMATIC POLISH LANGUAGE SPEECH RECOGNITION

Automatic Speech Recognition (ASR) systems are becoming increasingly more popular, even for languages with fewer native speakers (around 60 million worldwide for Polish). Our ASR system aims to work in a difficult environment. It is designed to recognize short phrases or single word commands in Interactive Voice Response (IVR) systems over telephone.
Our system supports context free grammars in form of Speech Recognition Grammar Specification (SRGS). It is a W3C standard, and is widely used in commercial systems. Decoding words with grammar allows the decoder to prune phrases that do not belong to a given formal language.



Biometry is the safest and the most convenient tool of authorization. This is how people recognize each other. Biometric features cannot be lend, stolen or forgotten and their falsification is practically impossible. Until now the barrier to the wider usage of voice biometry technology was high price of implementation and lack of solutions for fields other than telecommunication.

Both in Poland and in the whole world the market of Automatic Speech Recognition (ASR) technology and biometric voice verification (BVV/BVR) is a growing market. Current share of voice verification in the world market is little more than 4% amongst all biometry solutions. Not very high level of market penetration by speaker recognition and verification systems is affected by two basic factors: small number of efficient solutions and high price of licences for BVR/BVV modules. Helplines and voice systems market is a huge one, which is constantly open for new functionalities that increase customer satisfaction, improve security and lower the exploitation costs.

NO FAKE NEWS IS GOOD NEWS – DEALING WITH DISINFORMATION AT CYBERSEC – BRUSSELS LEADERS' FORESIGHT

BY ZIEMOWIT JÓŹWIK

Sir Julian King, Anna Fotyga, Prof. Alan Riley, Marietje Schaake and Andrei Soldatov at CYBERSEC Brussels 2018.

"As the current year is pivotal for shaping the European cybersecurity policy, it is crucial to deepen strategic transatlantic cooperation within the EU and NATO focused on cybersecurity." This is the key takeaway of CYBERSEC – Brussels' Leaders Foresight, a strategic debate held on 27 February. The opening panel discussion of the event concerned the challenges of counteracting disinformation and information warfare without infringing the core democratic values such as freedom of speech and pluralism. The debate chaired by Prof. Alan Riley, Senior Fellow at the Institute for Statecraft in London and Senior Non-Resident Fellow at the Atlantic Council, was attended by distinguished panellists including: Sir Julian King, European Commissioner for the Security Union, Andrei Soldatov, Russian investigative journalist and two Members of the European Parliament – Anna Fotyga and Marietje Schaake.

Fake news isn't new... but what is it actually?

As Sir Julian King, the European Commissioner for the Security Union stated, recently he saw a Victorian, over hundred years old cartoon that showed protesters with a banner saying "no to fake news". The problem isn't new and hasn't started along with the digital age – it's been there since societies started to communicate. What has changed are the ways that fake news are spreading. Therefore, as Marietje Schaake, the Member of the European Parliament advocated, the focus should be put on how disinformation is spreading, not on what is spread. In her view, paying too much attention to the content may in some cases lead to risks of interference with the freedom of speech. "Why technology is so disruptive on our democracies and economies?" – she highlighted – "if the phenomenon is so old, why is it such a hot topic

now?". We should avoid the situation in which "fake news" is appropriated and used misleadingly to dismiss coverage that is simply found disagreeable. "We need to approach fake news with precision and caution" – she said.

That's why M. Schaake would rather refer to another term "junk news" which is not subject to misleading interpretations in the public discourse such as "fake news". Against this backdrop it could be valuable to refer to the recent report of the European Commission High level Group on fake news and online disinformation that presented a shared understanding of disinformation (that actually goes beyond the term "fake news"). Disinformation has been defined as all forms of false, inaccurate, or misleading information designed, presented and promoted to intentionally cause public harm or for profit.

According to Andrei Soldatov, investigative journalist and Russian security services expert who author the best-selling *The Red Web*, the phenomenon of fake news, junk news and disinformation campaigns stems from the disruptions that have already been present in the Western societies. "Trolls and fake news agencies aren't capable of creating narratives, they're exploiting the problems that we already have". The decay of trust towards the institutions of democratic society is the primary reason here. "The first target of disinformation was the Russian society" – said Andrei Soldatov. Back then in the early 2000s, Russian society was persuaded that the democratic institutions such as the parliament, opposition parties or trade unions are corrupt, while media are used by "the West" or "Chechen terrorists" to wage information war against the regular people. The only instance that could be trusted was the president. "It's just Putin and the society – nothing between" – said A. Soldatov. Similarly, the fake news phenomenon has been triggered by the growing importance of social media that resulted from the shrinking credibility of traditional media. Following the Wikileaks, people tend to lose trust to journalists or outlets offering interpretation – "they wanted access to real, raw data, even though they weren't capable of understanding it themselves" – said A. Soldatov. This tendency has been used by the disinformation campaigns that on the one hand offer sensational stories, and on the other make us of the undermined trust towards traditional media, claiming that due to mainstream outlets' biased coverage, the story is only propagated via new media.

Shared understanding of disinformation

A multi-dimensional approach to disinformation report of the European Commission High level Group on fake news and online disinformation

All forms of false, inaccurate, or misleading information designed, presented and promoted to intentionally cause public harm or for profit.

It includes forms of speech that fall outside already illegal forms of speech, notably defamation, hate speech, incitement to violence, etc. but can nonetheless be harmful. It is a problem of actors — state or nonstate political actors, for-profit actors, citizens individually or in groups — as well as infrastructures of circulation and amplification through news media, platforms, and underlying networks, protocols and algorithms. In the near future, it will increasingly involve communication via private messaging applications, chat bots, and voice-operated systems, as well as augmented reality and virtual reality and content generated or manipulated by AI.

It does not cover issues arising from the creation and dissemination online of illegal content (notably defamation, hate speech, incitement to violence), which are subject to regulatory remedies under EU or national laws.

Nor does it cover other forms of deliberate but not misleading distortions of facts such a satire and parody.

The growing filter bubbles, that were discussed by Anna Fotyga, only reinforce the phenomenon. As long as the media audiences are isolated, they aren't able to communicate and verify the information feeds that are delivered. On the other hand, it facilitates the creation of tailor-made targeted communication. Each filter bubble could be simple served with adequate content in order to achieve a given goal within the information warfare.

How to tackle the problem – "a few words of caution"

"In building the resilience we need to remember the values that we're seeking to protect" – such a reservation provided by Sir J. King should be the core principle of dealing with the disinformation. This was complemented with M. Schaake's remark that in dealing with disinformation we should be "as specific as possible to define the problem that we're dealing with before we come up with solutions that could do more harm than good".

According to Anna Fotyga, the Member of the European Parliament and rapporteur of the *Report on EU strategic communication to counteract propaganda against it by third parties*, one of the main tools to increase the EU resilience to disinformation and fake news is to create new education programmes that will include media literacy and critical thinking skills. "Children should be provided with basic journalist's knowledge early at school" – she said. Being sceptical towards a soon triumph of quality media over clickbaits, she highlighted that "many media nowadays rely on fake news and there's no critical audience to change the attitude. That's a problem and as the public administration we cannot simply impose the solution from above". Therefore, she'd rather advocate a long-term measures that would provide a bottom-up solution such as education, awareness-raising and increasing media literacy.

"In building the resilience we need to remember the values that we're seeking to protect" – Sir J. King

Both M. Schaake and A. Soldatov supported A. Fotyga's view. "We need to be cautious when talking about quality journalism because this might be directly exploited by censors" – A. Soldatov highlighted. On the other hand, Sir J. King asserted that we shouldn't avoid "measures that might be exploited as an excuse against us; it cannot mean that our hands are completely tied, that we can't do anything because there's a risk that it'd be misrepresented or misused in another jurisdiction".

More EU-NATO cooperation

"Quite a lot of fake news that have apparently political objective is coming from Russia. We shouldn't be shy about that. No doubt that pro-Kremlin campaigns are orchestrated given the amount of disinformation that has been produced in different languages, in different channels and given the openness of some very senior figures in Russia" – said Sir J. King. Quite similarly, A. Fotyga claimed that "annexation of Crimea and Russian invasion on Eastern part of Ukraine was a real case study of disinformation". She cited NATO StratCom COE's report that illustrated the whole information campaign which was targeted at the Russian, Ukrainian and European societies that was initiated 12 years before the actual Russian aggression. On the other hand, Sir J. King referred to the EU StratCom East Task Force's analysis that identified 3500 examples of pro-Kremlin disinformation content contradicting publicly available facts.

This only shows the scale of the problem and the need to strengthen the EU response. Sir J. King welcomed the European Parliament's call to enhance the funding for the actions increasing the resilience to disinformation. Also, he mentioned the establishment

of independent High-Level Group on fake news and online disinformation by the European Commission. Also, he referred to the expected publication of the European Commission Communication on disinformation in Spring 2018. Finally, he highlighted the necessity to make sure "whether the laws of today are fit for purpose with the scale and pace of outside interference". In this context, legislation concerning hate speech, election, advertising, consumer and data protection, media transparency, political campaigns funding, media ethics were named as the crucial areas of consideration by M. Schaake and Sir J. King.

According to A. Fotyga, Transatlantic cooperation is critical here. "It's crucial, vital, the most important issue". For decades, the main purpose of Kremlin was to dismantle the Transatlantic alliance. She provided the example of initiatives bridging EU-NATO efforts – the European Centre of Excellence for Countering Hybrid Threats in Helsinki and called for more joint actions that might draw from the experience of NATO StratCom COE in Riga, NATO Cooperative Cyber Defence Centre of Excellence in Tallinn. "Most probably it's the best idea to enhance cooperation instead of building additional institutions". Finally, she underlined the necessity to "foresee how to be as close as possible to the UK after Brexit". In A. Fotyga's opinion the EU "can't make it well without this kind of cooperation", given "knowledge, tradition and the respected position of the services of this country".

Against this backdrop, M. Schaake warned against limiting disinformation problem to just one actor. "The problem is broader and deeper. It's not only Russia, also China, the Gulf States, Turkey or individuals with no political motives, doing it for a simple economic profit".

Striking a right public-private cooperation

Social media, digital platforms are crucial element of the rapidly changing media landscape that reinforced the spread of disinformation. "A large part of dealing with disinformation problem is the private sector's domain; we can address it if we strike a right public-private cooperation in the field" – said Sir J. King. M. Schaake expressed her concerns regarding the privatisation of law enforcement in the field of freedom of speech. "I'm worried that there's tendency, including the European Commission, to put more and more law enforcement on the shoulders of those companies. Who has the ultimate oversight is not always clear" – she said.

On the other hand, M. Schaake highlighted the growing impact of algorithms on society. "It's unsustainable that there're black boxes making enormously impactful decision without any oversight on behalf of the public interest. I'm thinking of companies like Facebook, Twitter and Google". She gave an example of the top trending video on YouTube of the week preceding the conference which claimed that protesters against gun violence after the recent Florida mass shooting were actors. "How come? We don't know because tech companies' algorithms are black boxes, we need transparency".

To conclude, an essential part of dealing with disinformation is to engage with digital platforms. As Sir J. King said "you're only going to be able to make progress if you construct a right public-private cooperation". ■

ABOUT THE AUTHOR:

Ziemowit Jóźwik is a graduate of law, Ukrainian Studies, post-graduate studies for translators of specialist texts from Ukrainian at the Jagiellonian University. He was in charge of projects related to border security and Ukraine as well as CYBERSEC - Brussels Leaders' Foresight. Co-editor of "Addressing Security Risks at the Ukrainian Border Through Best Practices on Good Governance" (NATO SPS Series) and "European Cybersecurity Market" magazine. His areas of interests include EU cybersecurity policy and legislation.

KRAKOW

THE PLACE WHERE CYBER MEETS SECURITY

THE KOSCIUSZKO INSTITUTE

WHAT **WE** DO?

In CYBERSEC HUB we believe that connecting means creating and that every network is more than the sum of its parts. That is why we launched our platform which brings together people from across boundaries. From the private to public sector, from the technical to political spectrum, we connect all those who want to forge a secure cyber future.

CYBERSEC HUB builds on the synergy between stakeholders from the Małopolska Region in Poland, with the city of Krakow as its strategic center. Krakow is one of the largest startup hubs in Europe with over two hundred ICT businesses, unparalleled investment opportunities, and access to talent, funding and the entire EU market. This unique environment is what attracts global IT companies to the area, many of whom have already moved their Research, Development and Security Operations Centres to Małopolska. Krakow also hosts the European Cybersecurity Forum CYBERSEC, one of the main public policy conferences on cybersecurity.

One of the initial projects run by our platform is CYBERSEC Accelerator which helps ICT and cybersecurity startups and SMEs from Małopolska to reach international markets. In the run-up to the project, an expert panel selected 7 of the most innovative businesses amongst the applicants. The Accelerator has been officially launched during the 2nd European Cybersecurity Forum CYBERSEC 2016. In this Innovation Book you will find unique products and services offered by CYBERSEC Accelerator participants.

The Kosciuszko Institute is a Polish think-tank founded in 2000. As an independent and non-profit organization, it gives itself the mission to contribute to the social and economic development of Poland in the European Union and as a partner of the Euro-Atlantic Alliance.

The experts of the Institute regularly cooperate with national and international organizations in the process of policy-making and initiating public debate on strategic issues.

Among its various areas of research, the Kosciuszko Institute leads its flagship projects in the field of cybersecurity, among them CYBERSEC HUB and the European Cybersecurity Forum – CYBERSEC.

We invite you to follow our initiatives and get involved.

Kraków, Poland.

www.ik.org.pl

THE KOSCIUSZKO INSTITUTE

is the publisher of

EUROPEAN CYBERSECURITY MARKET