Written Representation 86

Name: Myla V. Pilao & Ryan Flores
Director, Core Technology Marketing & Senior Manager, Forward-Looking Threat Research Team

Received: 28 Feb 2018

Dear Committee Heads,

Please find the attached submission on the topic of Fake News from Trend Micro.

We would be happy to share more technical information and deeper insights based on our research and findings upon request.

We hope that this will support your ongoing initiatives to identify possible measures to counter this disruptive practice of spreading falsehood online.

Thank you

Myla Pilao

THE MOTIVATIONS, ECONOMY, AND DIGITAL PLATFORMS THAT FUEL CYBERPROPAGANDA

Myla V. Pilao (Director, Core Technology)
and
Ryan Flores (Senior Manager, Forward-Looking Threat Research Team)

CONTENTS

CHAPTER | 1

INTRODUCTION

Fake news (or deliberate online falsehoods) have been likened to disinformation campaigns, cyberpropaganda, cognitive hacking, and information warfare.[1] But these are just a facet of the bigger problem: manipulating public opinion to affect the real world aided by connectivity and digital platforms, transcending physical borders and constraints presented by time and distance.

Fake news refer to false stories that appear to be news, spread on the internet or using other media, usually created to influence political views or as a joke.[2]

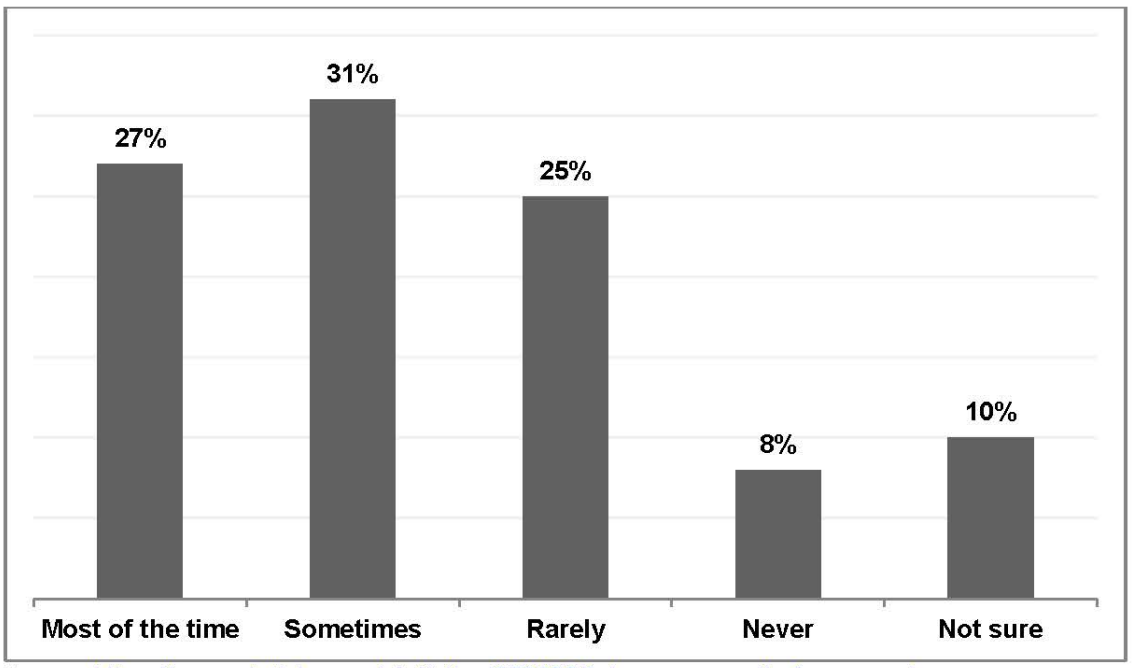
Though the term "fake news" only gained notoriety in 2016, the concept behind the phenomenon dates back millennia. Along with technological improvements (the invention of the printing press, etc.) came advancements in fake news proliferation.

In 2017, more than half (58 percent) of the respondents to a U.S. survey believed that even mainstream media spread fake news.

---

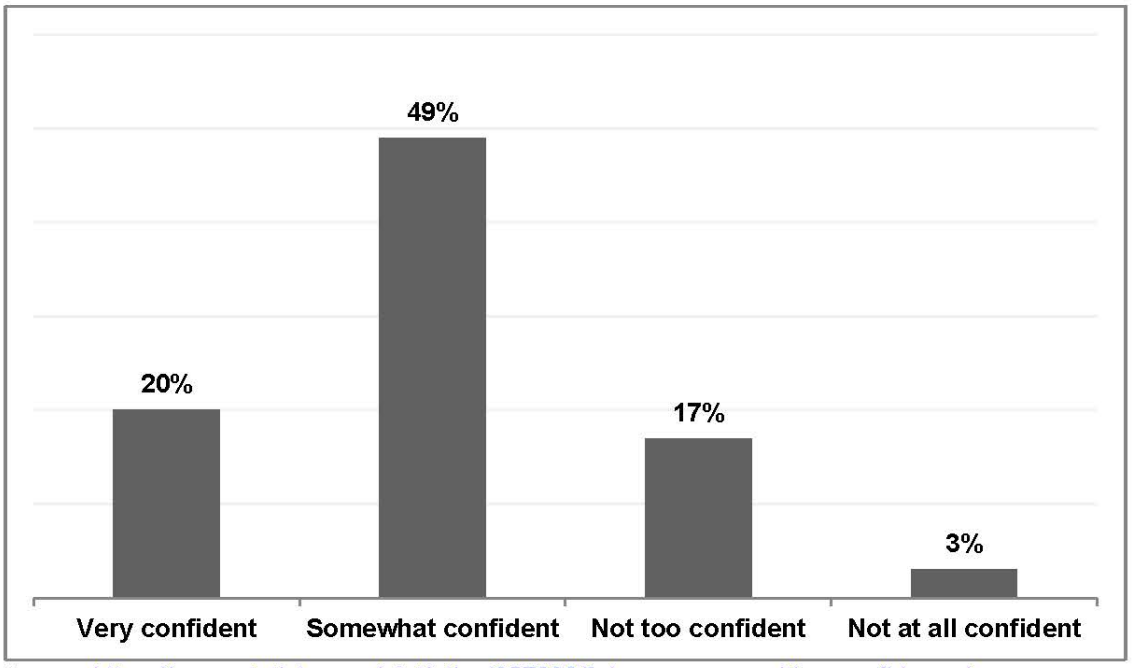
1 Lion Gu, Vladimir Kropotov, and Fyodor Yarochkin. (13 June 2017). *Trend Micro Security News*. "Fake News and Cyberpropaganda: The Use and Abuse of Social Media." Available at https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/fake-news-cyber-propaganda-the-abuse-of-social-media.

2 Cambridge University Press. (2018). *Cambridge Dictionary*. "Fake news." Available at https://dictionary.cambridge.org/us/dictionary/english/fake-news.



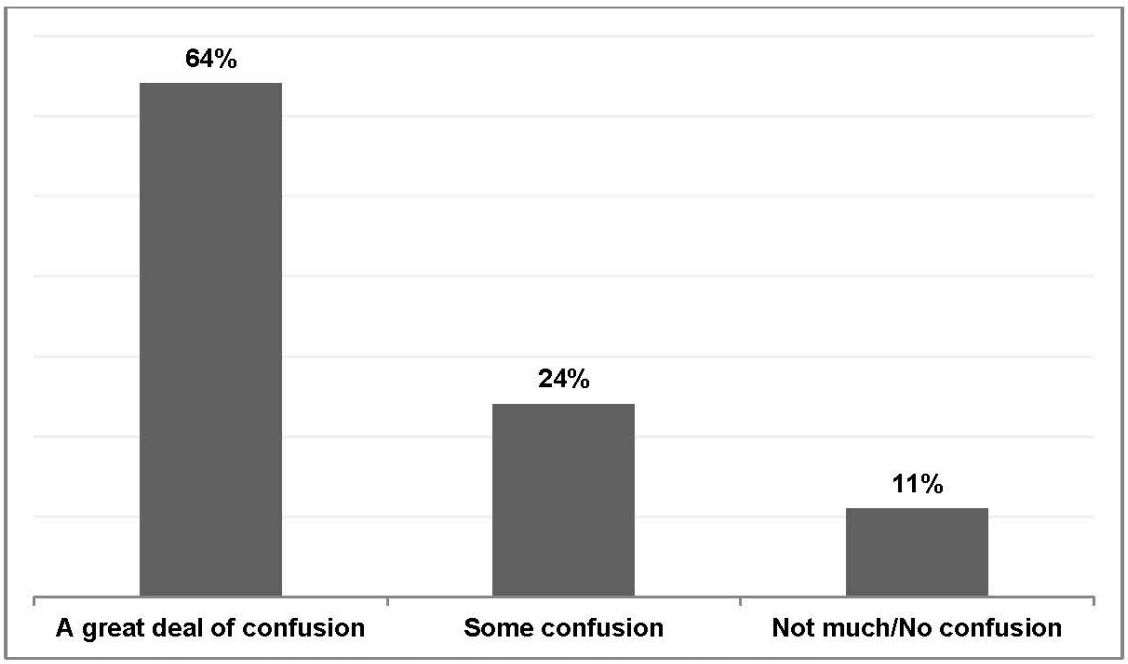
Source: https://www.statista.com/statistics/678000/fake-news-media-frequency/

Even more worrying, however, was the fact that as much as 20 percent of the respondents to a 2017 U.S. survey did not feel confident about discerning what was fake from what was real news.



Source: https://www.statista.com/statistics/657090/fake-news-recogition-confidence/

And even if readers could tell fake from real news, confusion was still sown on the part of the majority (88 percent) of the respondents to a U.S. survey.



Source: https://www.statista.com/statistics/657037/fake-news-confusion-level/

The dangers that fake news bring are real. Belief in and acting on fake news can destabilize governments, influence the outcome of elections, cause the demise of businesses, and discredit target individuals and groups, among others.

The following table shows samples of the some of the biggest fake news stories in 2017.

Fake News	The Truth
Hurricane Irma, a category 6 storm	No such thing as a category 6 storm
Manchester Arena attack	Pictures that circulated were fake (taken a long time before the bombing took place)
London Bridge attack	Supposed suspect was actually actor Sam Hyde
Greenfell Tower fire	Death toll did not reach the hundreds as shared millions of times on social media
Canadian imam closed its mosque doors to Christian victims of Storm Harvey	False claim
Miami Airport video during Hurricane Irma	Video was actually of the wrong storm
Frida Sofia, an earthquake victim in Mexico	Frida never even existed
Boy securing food for a friend after an earthquake in the Iran-Iraq border	Video was not filmed after said earthquake

Source: http://www.bbc.com/news/world-42487425

The verdict is in: the proliferation of fake news is a global problem. In fact, this year we expect to see refined cyberpropaganda campaigns using tried-and-tested techniques from successful spam campaigns.[3]

Cyberpropaganda campaigns will use do-it-yourself (DIY) kits to automatically spam social media users. Even blackhat search engine optimization (SEO) will be adapted to optimize social media posting to reach hundreds of thousands of readers across platforms. Spear-phishing emails may also be used to discredit authorities with dubious content.

---

[3] Trend Micro Incorporated. (5 December 2017). *Trend Micro Security News*. "Paradigm Shifts: Security Predictions for 2018." Available at https://www.trendmicro.com/vinfo/us/security/research-and-analysis/predictions/2018.

These campaigns are likely to target several countries set to have their presidential elections within 2018, including but are not limited to:

Africa	Asia	Europe	North America	South America
Cameroon	Cambodia	Czech Republic	Cuba	Paraguay
Madagascar	Maldives	Cyprus	Mexico	Venezuela
Mali	Pakistan	Finland	United States	
Mauritania	Turkmenistan	Georgia		
Sierra Leone		Italy		
South Sudan		Montenegro		
		Russia		
		Sweden		

Sources: http://www.electionguide.org/elections/upcoming/; https://www.thelocal.se/20170911/what-you-need-to-know-about-swedens-party-leaders-2018-election; https://www.usatoday.com/story/news/politics/2017/09/07/2018-midterm-elections-senate-races-to-watch/597965001/

Manipulated political campaigns will continue to mount smear tactics and deliberately shift public perception, aided by tools and services readily available in underground markets.

Even businesses can end up in a bad light using altercated audio and video files that render realistic-looking footage. A company can, for instance, spread false negative comments about a competitor to rake in more business. Cases of this have been found in New Zealand.[4] But probably the biggest business hoax had to do with an individual tricking people into believing his shed is a top-rated restaurant on TripAdvisor.[5] This turned out to be a social experiment done by someone who used to write fake restaurant reviews for a fee.

---

[4] Cherie Howie. (9 December 2017). *Nez Zealand Herald*. "Kiwi businesses most likely target for fake news attacks - Massey University Business School senior lecturer Jenny Hou." Available at http://www.nzherald.co.nz/business/news/article.cfm?c_id=3&objectid=11955189.

[5] Oobah Butler. (6 December 2017). *Vice*. "I Made My Shed the Top Rated Restaurant On TripAdvisor." Available at https://www.vice.com/en_uk/article/434gqw/i-made-my-shed-the-top-rated-restaurant-on-tripadvisor.

Each time fake news is posted and reposted, readers of the same content grow familiar with it and take it as truth. Distinguishing fake from real news is tough, as cyberpropagandists use proven and reliable techniques each time. The more times fake news is posted and reposted, the more chances it will be taken as truth.

Fake news and cyberpropaganda will press on due to the absence of a dependable way to detect or block manipulated content. Even the social media crackdown on bogus stories has had little impact so far. That said, the final screening will depend on news readers. As long as readers remain uneducated in flagging false news, it will continue to permeate online and be consumed by the unsuspecting and undiscerning.

CHAPTER | 2

THE FAKE NEWS TRIANGLE

To succeed, a fake news campaign relies on what we call the "fake news triangle," which comprises motivations, tools and services, and social media. Lack of any one of these components can make spreading fake news difficult, if not impossible to pull off.

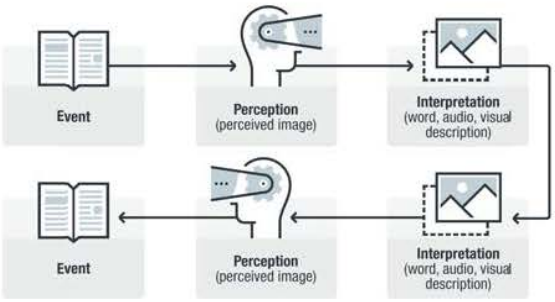
Motivations

Trend Micro research revealed three major factors for fake news' notoriety, namely:

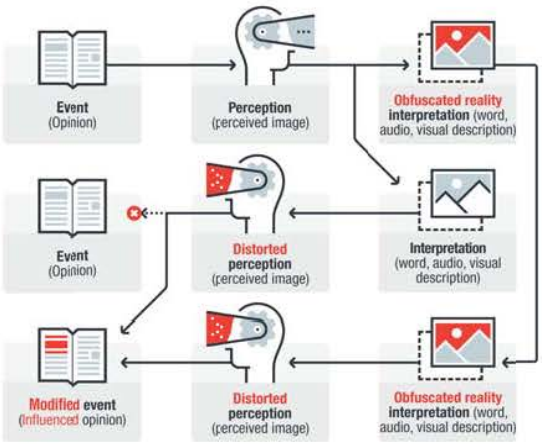
- **Cost:** To obtain the same reach, spreading fake news costs significantly less than posting legitimate advertisements or paid content. This is very important to interested parties without much funding.
- **Anonymity:** It is much easier to hide the origin of a fake news story compared with its legitimate counterparts.
- **Credibility:** News sources (legitimate or otherwise) prefer "viral" stories over paid ads or content.

In 2017, we saw two major types of fake news campaigns according to motivation—political and financial.

Political propaganda campaigns are generally designed to get people to change their political beliefs or opinions. These may aim to destabilize target countries or discredit personalities that oppose the perpetrators' intended outcomes. In essence, fake news operators aim to change reader perception.



Ideal opinion-formation process



Opinion formation process affected by cyberpropaganda

A particular country, for one, has been accused of using social media to divide Americans in the months leading up to and immediately after the 2016 presidential elections.[6] In such campaigns, character assassination and leaking data are usual tactics to discredit people running for office or their staunch supporters. To date, 2017's Macron Leaks would probably be the biggest politically charged data leakage incident recorded.[7]

On the other end of the spectrum, some individuals or groups suffer public shaming just so fake news writers can line their pockets.[8] How? Every click on a fake news site translates to revenue earned for the operator.

---

6 Tom McCarthy. (14 October 2017). *The Observer*. "How Russia used social media to divide Americans." Available at https://www.theguardian.com/us-news/2017/oct/14/russia-us-politics-social-media-facebook.

7 Meghan Mohan. (9 May 2017). *BBC News*. "Macron Leaks: the anatomy of a hack." Available at http://www.bbc.com/news/blogs-trending-39845105.

8 Abby Ohlheiser. (18 November 2016). *The Washington Post*. "This is how Facebook's fake-news writers make money." Available at https://www.washingtonpost.com/news/the-intersect/wp/2016/11/18/this-is-how-the-internets-fake-news-writers-make-money/?utm_term=.5815cd812d30.

Politicians and celebrities are not the only possible victims of fake news though. Even businesses are at risk of damage to their corporate reputation.[9] All it takes to discredit a reigning competitor, for instance, is to launch a viral smear campaign against its owner or its flagship product or service.

The reasons for spreading fake news range far and wide. Though most truly believe in their cause and wish to convince the rest of the world to take it up as well; some are just after committing mischief by sowing confusion.[10] Still others are just after gaining popularity (or in this case, notoriety) by widening their social media follower base.

Tools and Services

To spread fake news, campaign operators use various tools and services commonly found in underground or even gray markets. These include but are not limited to the tools and services described in more detail below.

CONTENT MARKETING SERVICES

For as little as US$15–30, fake news operators can obtain 500–1,500-word articles from content marketing service providers.

---

[9] John P. David. (9 December 2016). *Huffpost*. "Fake News Can Damage Your Corporate Reputation." Available at https://www.huffingtonpost.com/john-p-david/fake-news-can-damage-your_b_13513496.html.

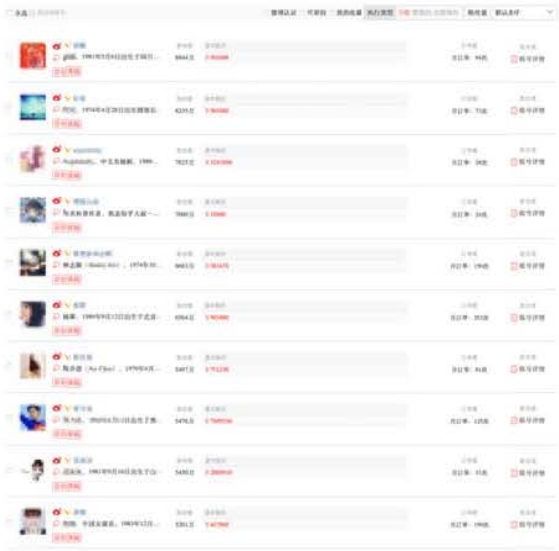
[10] Rachael Kelly. (8 January 2018). *The Southland Times*. "Southland's H&J Smith department store target of 'fake news' scam video." Available at https://www.stuff.co.nz/southland-times/business/100391452/southlands-hj-smith-target-of-scam-video.

ANALYTICS SERVICES

Sites also offer "public-opinion-monitoring systems" that can survey, research on, and influence opinions in prominent forums and social media for US$1,850–4,175, depending on the number of keywords identified.

SOCIAL MEDIA PROMOTION SERVICES

These services bank on the popularity of the social media account used to trigger a word-of-mouth effect among the posters' followers. They cost between US$0.16 and US$180,000, depending on how many followers the account used has.



CONTENT TAKEDOWN SERVICES

Some fake news operators opt to take down content that spout the opposite of their desired effect.

In 2012, Yage Times (a content takedown service provider), was nabbed by the police. The group reportedly earned US$7.9 million from a single operation in 2011 alone.

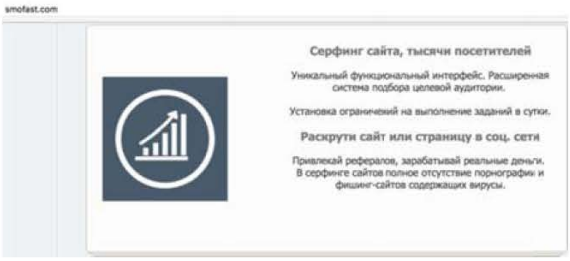
VOTE MANIPULATION AND CLICK FARM SERVICES

Fake news operators who wish to influence the outcome of polls or elections rely on these for US$4,925–14,524.

A click farm commits click fraud through a large number of low-paid workers who click paid ad links for the click farm master or simply click farmer.

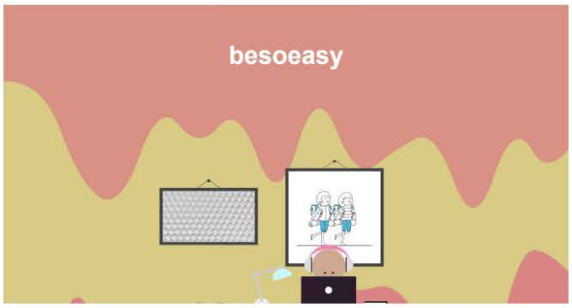
CROWDSOURCING SERVICES

These are available in Russian underground forums for as little as US$1. Fake news operators can crowdsource for either likes or dislikes, depending on their desired outcome.



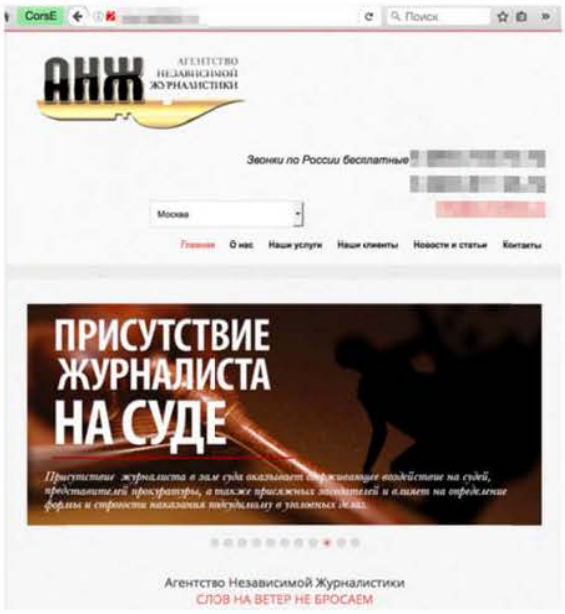
AUTOMATION BOTS

Some underground markets offer automation bots that can amplify the popularity of a fake news story should the operator wish to use his own "account" (typically also fake, of course).



CONTENT DISTRIBUTION SERVICES

In Russia, bogus and even legitimate news outfits can serve as platforms for fake news. Making fake content appear on legitimate news sites without appearing as advertorials, however, costs a premium (more than US$20,000).



The following table sums up all of the tools and services that can be used and/or abused for fake news campaigns found in underground and gray markets.

Tool/Service	Price (US$)
Vote that bypasses an IP address check, a Captcha, or simple authentication	0.02–0.03
1 social media like	0.04
Vote that bypasses social media authentication	0.04–0.05
Vote that bypasses detailed online registration	0.05–0.07
Vote that bypasses SMS confirmation/more complex authentication	0.09
40 WeChat article views	0.16
1K WeChat likes	0.19
like4u crowdsourcing service (5 minutes–24 hours)	0.20–80
100 Instagram subscribers, friends, likes, or video views	0.23–0.40
100 VK group subscribers	0.30
10K video views on Youku, LeTV, Sohu, Tencent, or iQiYi	0.32–3
100 Twitter followers, likes, or retweets	0.34
100 YouTube subscribers	0.66
1K video views	0.89–4
100 YouTube video dislikes	2
100 YouTube likes/video views/full video views	2/0.30/0.23
500 retweets	2–130
100 YouTube video comments/10 comments/1K YouTube views	3
1K Instagram subscribers	3–15

Tool/Service	Price (US$)
VTope (with 2M users) crowdsourcing coupon worth 10K points	8–21
1K group joins	11
VK user spamming (1K personal messages) service	14
500–800-word fake news article	15
500 WeChat followers	16
10K site visitors	17
1K high-quality fan page likes	17–31
1M Instagram likes	18
500 Instagram followers/1 month Facebook auto-like service subscription	25
1–1.5K-word fake news article	30
1 month Twitter promotion service subscription	30–150
1K votes on Weibo	32
8 comments per day for 1 month	45
1K high-quality channel subscribers/"Fake" content takedown service	50
5K votes on Weibo	55
VTope (with 2M users) crowdsourcing coupon worth 50K points	62
5K Weibo followers	66
Content distribution on a provincial news site	72
Content distribution on a national news site/ site on the Baidu news feed	116

Tool/Service	Price (US$)
5K WeChat followers	103–158
Social media VIP service	106–124
Content distribution on a real-estate/financial/business site	131
2.2K Facebook auto-likes/1K comments per month	150
Content distribution on an IT news/fashion/entertainment site	174
Content distribution on a healthcare site	189
Make a video trend for a certain search query service	222–266
Content distribution on dubious publication/a newspaper's classifieds section	266
10K WeChat followers	315
Content takedown service	394
Content takedown service on Tianya or mop.com	394–630
YouTube main page video appearance for 2 minutes	621
10K Facebook auto-likes per month	800
PR distribution to news outlets	802
1M YouTube views	999
10K votes/petition signatures	1,065
Public-opinion-monitoring service for 10 keywords	1,850
25K votes/petition signatures	2,664
Premium YouTube package (1M high-quality views and 50K likes)	3,150
Public-opinion-monitoring service for 20 keywords	4,175
Click farm service (1 server with remote control capacity for 30 phones	4,925
Content (with 4–6K characters) distribution on commercial news sites	5,328–9,768
Click farm service (1 server with remote control capacity for 50 phones)	7,815
YouTube main page appearance of 20 videos for 2–6 minutes	7,992
Click farm (1 server with remote control capacity for 100 phones)	14,524
Content (not marked as advertorial/paid) distribution	21,641
WeChat celebrity (with 10.7M followers) promotion	69,500
Weibo celebrity (with 78.3M followers) promotion	180,000

Note: The tools and services in the table above are arranged from cheapest to most expensive.

Social Networks

Social media use is now ubiquitous. Out of the 7.5 billion people worldwide as of 2017,[11] 3.5 billion are internet users,[12] and 3.03 billion are social media users.[13]

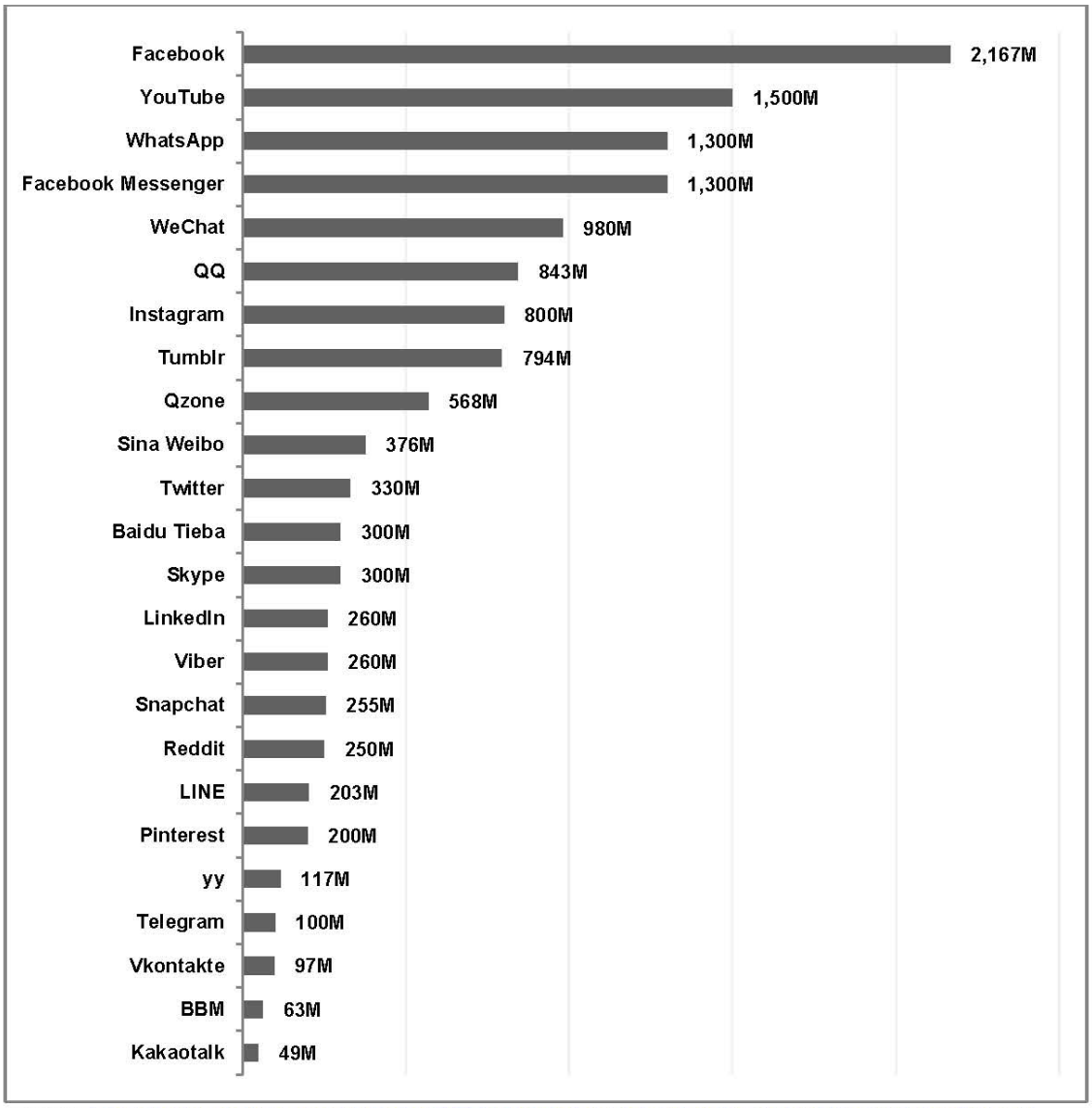
Among the world's social networks, Facebook has the highest number of active users (2.2 billion) as of January 2018, making it the most likely platform of choice to launch fake news campaigns.

---

[11] Population Reference Bureau. (2018). *PRB*. "2017 World Population Data Sheet." Available at http://www.prb.org/Publications/Datasheets/2017/2017-world-population-data-sheet.aspx.

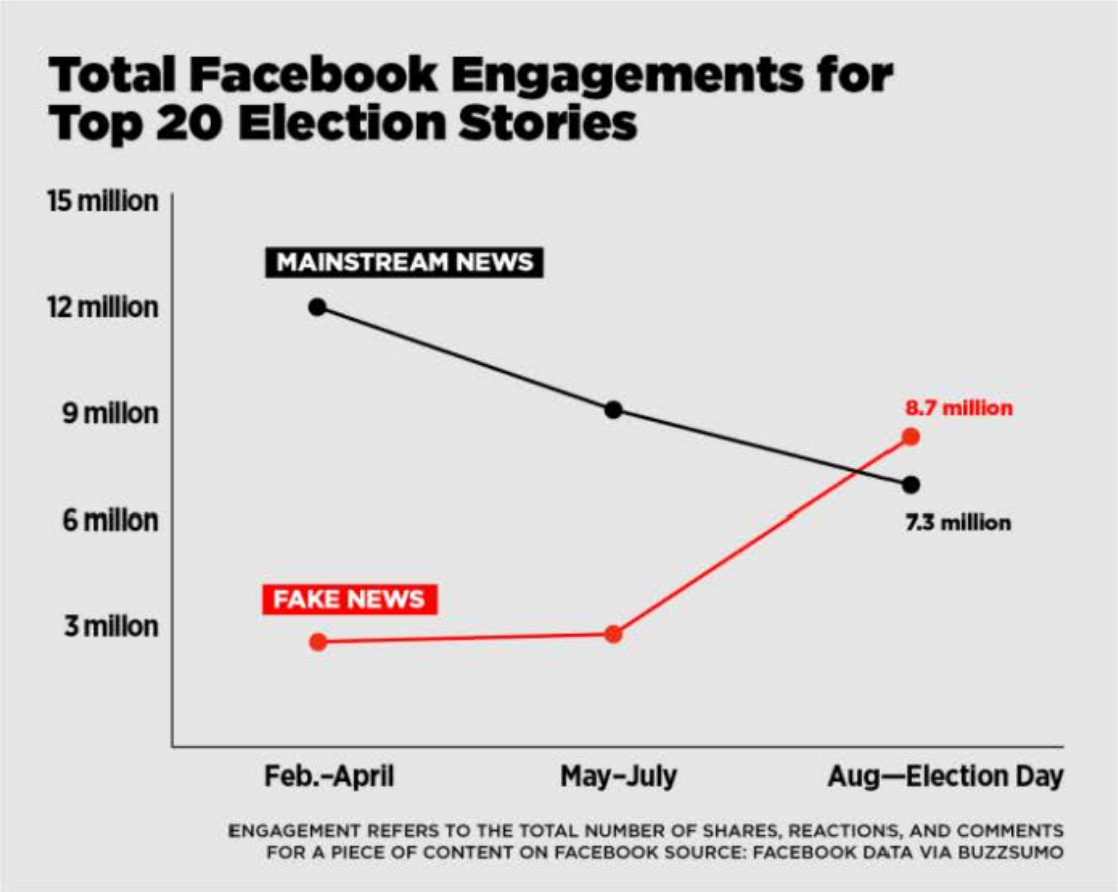
[12] Kit Smith. (18 November 2017). *Brandwatch*. "Marketing: 105 Amazing Social Media Statistics and Facts." Available at https://www.brandwatch.com/blog/96-amazing-social-media-statistics-and-facts-for-2016/.

[13] Simon Kemp. (7 August 2017). *LinkedIn*. "Global Digital Statshot Q3 2017." Available at https://www.slideshare.net/wearesocialsg/global-digital-statshot-q3-2017.



Source: https://www.statista.com/statistics/272014/global-social-networks-ranked-by-number-of-users/

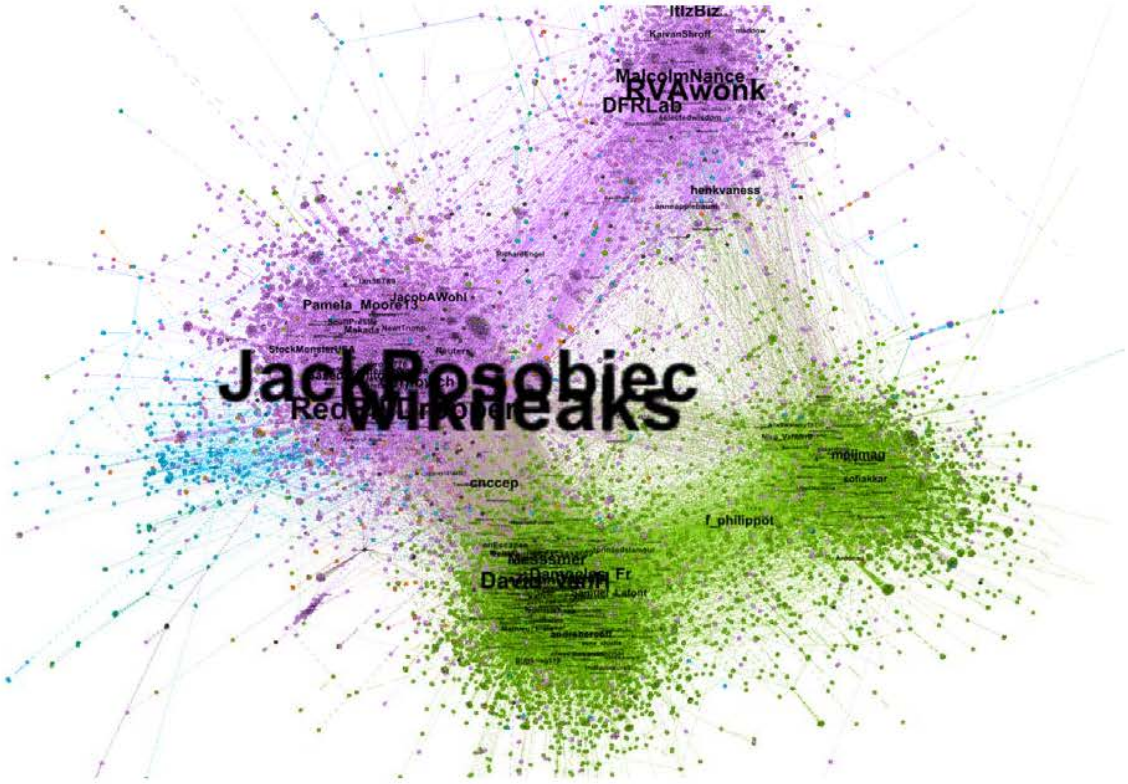
It was not surprising then that in the months leading up to the 2016 U.S. presidential elections, "viral fake election news stories outperformed real news on Facebook."



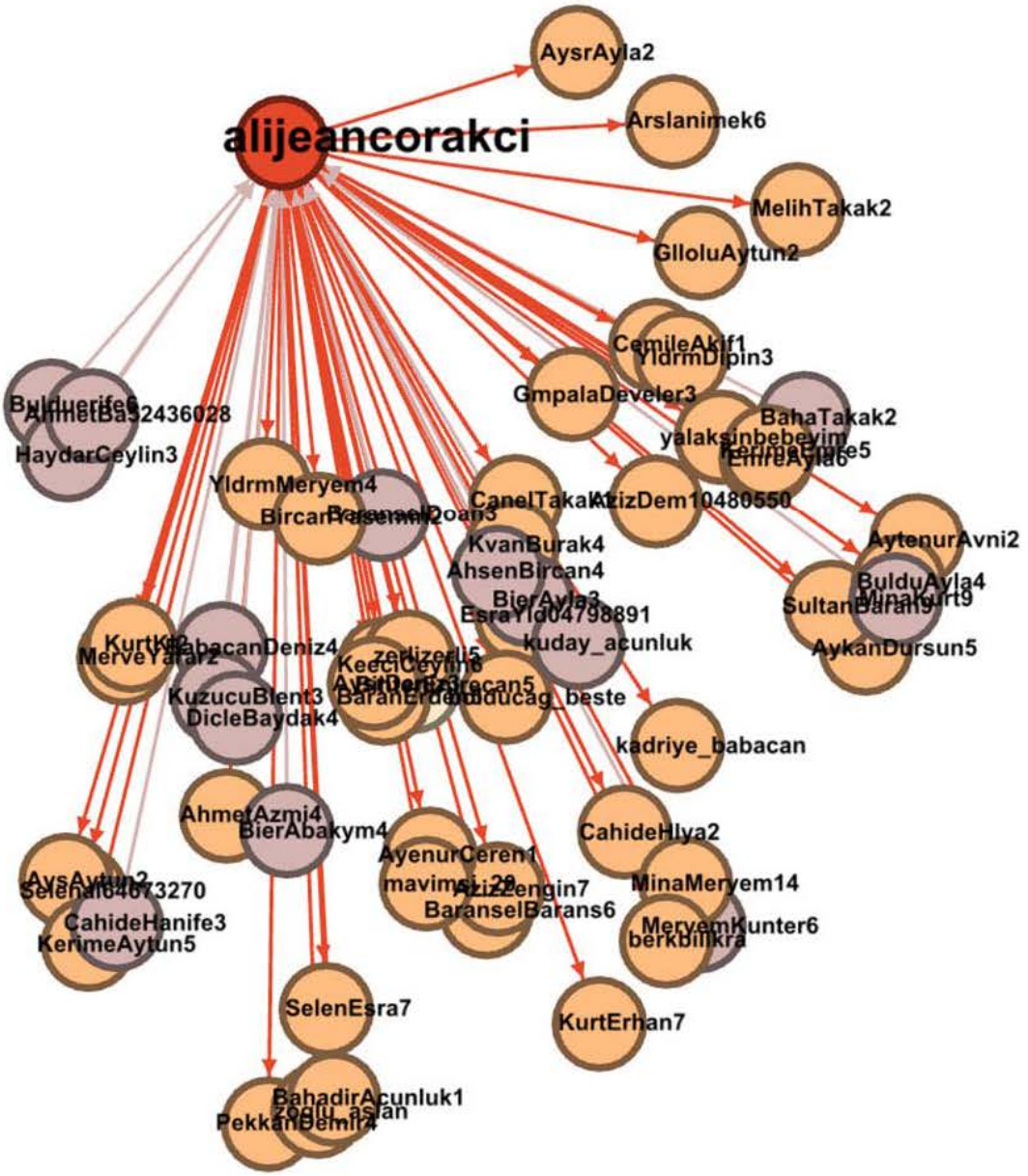
Source: https://www.buzzfeed.com/craigsilverman/viral-fake-election-news-outperformed-real-news-on-facebook?utm_term=.stmRqKdbO#.yuqjqlyJA

On Facebook, fake news headlines and photos are designed to quickly engage readers of a particular ideological orientation, but don't reveal the entire story. They serve as hooks to the fake articles that are linked to the posts. They use consistent branding and typically a fake site.

We looked at a Twitter network diagram for the #Macronleaks hashtag and found that two distinct communities (purple and green) were formed. But we were more interested in the small satellite communities that only interacted with one another, especially if they exhibited the same behavior across multiple social events, which could indicate misuse or abuse.



Twitter accounts can be categorized as “gurus” or “sect followers.” Gurus are often followed by a large number of users (or sect followers) who actively repost and retweet the original posters’ messages as shown in the following guru-sect follower structure.



In a fake news campaign, bot accounts retweet a single post at around the same time using the same hashtag. Each bot usually has the same group of followers as the other bots. Groups of bots usually follow and retweet the posts of the same gurus as well.

In the French presidential elections' case alone, we identified more than 5,400 suspicious accounts. Research indicates that the Manchester bombing saw similar suspicious activity. Twitter has, however, identified and suspended suspected follower accounts since.

CHAPTER | 3

THE FAKE NEWS TRIANGLE AT WORK

In essence, every cyberpropaganda campaign is launched with one primary goal in mind, to change the public's opinion on a chosen topic. Cyberpropagandists are likely to follow the Public Opinion Cycle below.

Note: This diagram was loosely based on Lockheed Martin's Cyber Kill Chain found at https://www.lockheedmartin.com/us/what-we-do/aerospace-defense/cyber/cyber-kill-chain.html.

To change the reigning public opinion, cyberpropagandists first need to gather information and analyze their target audience (*Reconnaissance*). They need to gauge the target's level of loyalty, acceptance, and knowledge maturity regarding the topic of interest. Only then can they actually prepare the key story or the version of facts they wish to spread aka fake news (*Weaponization*). They need to create background stories to support the key story, along with variations or "alternative versions" or "secondary" side stories to "plant" in case more informed readers do not fully buy the key story and decide to investigate. To see how well their key story did, they should also set success metrics depending on their expected reach.

Once the preparations are done, the key story is spread across traditional and social media (*Delivery*). This is where the tools and services discussed earlier can be used. As in real marketing campaigns, controlled targeted promotion (idea distribution) can be done among small but active groups of supporters (*Exploitation*). This is where social networks come in handy.

Cyberpropagandists need to maximize the visibility of their key story; they need to reach critical mass in terms of supporter volume (*Persistence*). Their target must be convinced to actively promote their key story on their own until it goes viral. They can engage supportive activist groups in this stage and make use of both positive and negative feedback. They then need to keep the story going while anticipating and reacting to changes in sentiment (*Sustainment*). Metrics can help with this as well.

Should the public sentiment change, the cyberpropagandists need to take the necessary steps to get back on track (*Taking Action*). Once they have accomplished their mission, they need to switch the public attention somewhere else (*Trace Removal*) so they will not fall under public scrutiny.

To better explain how the Public Opinion Cycle works, take a look at the following scenario that could have instigated a street protest in the U.S. (from "The Fake News Machine: How Propagandists Abuse the Internet and Manipulate the Public").

> In February, 2017, a doctored photo of burning teepees and a caption that sternly criticized the police for setting a protest group's camp on fire caused a misguided uproar over social media.[14] By May, boycotts from a number of students at a college in Minnesota were incited by a fake message.[15]

---

[14] Valerie Richardson. (5 February 2017). *The Washington Times*. "Burning teepees, floating buffalo and zombies: Dakota Access pipeline protest plagued by 'fake news.'" Available at https://www.washingtontimes.com/news/2017/feb/5/dakota-access-pipeline-protest-plagued-by-fake-new/.

[15] KARE Staff. (10 May 2017). *KARE*. "St. Olaf: Racist note that prompted protests was fake." Available at http://www.kare11.com/article/news/st-olaf-racist-note-that-prompted-protests-was-fake/438629694.

With the tools available in the underground and legitimate services that can be abused, manipulating public perception to provoke a protest can be a scalable campaign. Pulling it off, however, entails financial resources. The instigator can first create and populate social media groups that discuss sensitive topics and ideologies he wants to fuel with fake news (*Reconnaissance* and *Weaponization*). In the underground, populating 20 groups with 1,000 "high-quality" members would cost around US$40,000.

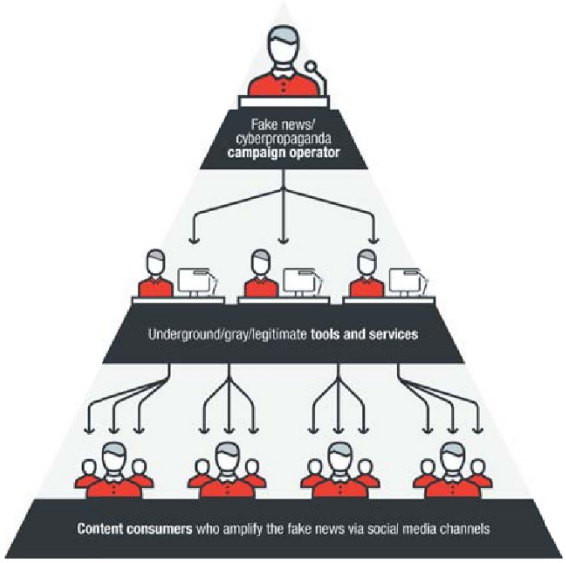
Promotional services for fake content that further incites the group's ideologies can also be bought in underground markets (*Delivery*). Maximizing the content's reach to the intended audience would cost US$6,000 (around 40,000 high-quality likes). Comments, which come in templates that a customer can choose from, cost US$5,000 (20,000 comments at US$250 per 1,000 comments). The instigator can further promote his "cause" by ordering at least 10 news stories promoted with 50,000 retweets and likes from 100,000 visitors for US$2,700 per story. Placements of at least 50 related videos on YouTube and making them go viral can further elevate the instigator's ulterior motive for US$2,500 for every five videos (*Exploitation* and *Sustainment*).

A service that can be misused to announce and promote a protest over social media can cost around US$10,000. Buying promotional services to propagandize it on a bigger venue would entail US$30,000. The instigator can then run the protest's upkeep with logistics, paraphernalia, medical support, and other provisions for around US$20,000. He will need a further US$10,000 for dispersing the protest after the instigator's objective has been accomplished (*Trace Removal*).

The overhead for this campaign would tally around US$200,000. But even a 1 percent turnout from a reached audience of around 2 million from a desired or targeted region, for instance, can still have an impact. Note, however, the key ingredient required to make the campaign a success: fake news fabricated as truth that panders to its audience's ideologies and promises an illusion of the future—enough to compel people to join an imagined cause.

The same or a similar attack scenario can be used in any target country. In Singapore's case, for instance, the same tactics, tools, and services can be used to instigate a public protest against announcements made concerning the 2018 budget that will affect households.[16] All it takes is a determined adversary with the financial resources to pull off an intended malicious action.

To make a fake news campaign work, all three components of the Fake News Triangle need to be present. In the scenario above, the campaign operator had a political agenda (motivation). For a fee (to buy the required tools and services) and by abusing the most widely used platform in the country (social network, in this case, Facebook), the perpetrator could launch a campaign that can affect even the country's policy implementation and possibly even economy.



[16] Charmaine Ng. (19 February 2018). *The Straits Times.* "Singapore Budget 2018: 9 things that will affect households and Singaporeans." Available at http://www.straitstimes.com/singapore/singapore-budget-2018-9-things-that-will-affect-households-and-singaporeans.

COUNTERMEASURES

Legislative authorities and international organizations the world over have started discussions (even if they have not yet implemented sanctions) to curb the growing fake news problem. Signing an anti-fake news or anti-hate speech bill into law is one way of addressing the growing problem. This works especially when social and mainstream media (among other partners) work hand in hand in said legislation's implementation.

The following table shows what other countries have done to tackle the fake news problem by way of legislation.

Country/Region	Legislative Countermeasure
U.S.	U.S. Congress proposed an anti-fake news bill since Obama's time that authorizes officials to combat propaganda and fake news and allows federal money to be used abroad where misinformation "threatens the country's national security"; a law, however, remains nonexistent.
European Union (EU)	Keeps a list of sites that publish disinformation while deciding on whether or not an anti-fake news bill should be signed into law; plans to set up a panel of experts to engage in discussions and running a public poll are also being considered
Russia	Ministry of Foreign Affairs keeps a list of sites known for spreading fake news
Italy	Antitrust chief recommended that the EU set up a network of independent agencies to tackle the problem
Brussels	Included fake news in its agenda for discussion
Germany	Signed an anti-hate speech law last year to thwart the fake news problem by fining social networks as much as €50M for failing to promptly remove fake content after it has been reported
France	Macron proposed an anti-fake news law that concerns social media platforms, especially during elections; this would deeply change the role of the country's media watchdog, the Conseil supérieur de l'audiovisuel (CSA); sites would be required to reveal who financed the distribution of particular content; sponsored content pricing would be capped; and in times of elections, emergency legal actions may allow French authorities to suppress content or even block access to a site
Brazil	Federal Police announced its plans to regulate, control, and censor political content assessed as "false" on the internet and "punish" those who disseminate it; this would cover social media posts and entire sites devoted to politics

Country/Region	Legislative Countermeasure
Ireland	"Online Advertising and Social Media (Transparency) Bill 2017" contains a number of measures that aim to expose those who professionally engage in "false flag" and deceptive advertising to disrupt the democratic process
U.K.	Ofcom, the media regulator, believes Google and Facebook should be classed as publishers instead of conduits for information, "raising the prospect that they could eventually face more regulation"; social media posters could also find themselves on the end of a defamation claim, but so far there's no specific law to tackle fake news
Czech Republic	Instituted the Department of Interior Ministry to tackle misinformation in cyberspace just this January; the department is tasked to forward findings to the police, the army, and the secret services; a part of it will specialize in detecting misinformation from open sources (including social networks) and reversing them
South Korea	Under the current law, spreading fake news to smear or ruin someone's reputation is illegal but information and communication service providers offering web platforms are not pressured enough to do more to tackle the growing issue of fake news; if the new legislation is passed, IT service providers (e.g., web portals) can delete news stories proven fake as part of the government's efforts to stop misinformation from spreading and manipulating public opinion
Association of Southeast Asian Nations (ASEAN)	Several countries are considering new legislations or expanding existing regulations to make publishing fake news an offense; "fake news" has entered the lexicon of ASEAN leaders who commended the work done by governments in countering its spread in a statement issued at the end of a November summit
Malaysia	Proposed new law against fake news is part of its effort to safeguard national interest, according to the Malaysian Communication and Multimedia Commission (MCMC)
Philippines	Signed Republic Act 10951 into law in August of last year; users who spread false news can be imprisoned for up to six months and fined up to ₱200,000

Sources: http://digitaledition.chicagotribune.com/tribune/article_popover.aspx?guid=e5824f23-fff8-4742-8479-0ee30aa2f881; https://eeas.europa.eu/headquarters/headquarters-homepage_en/9443/Disinformation%20Review; http://www.mid.ru/nedostovernie-publikacii; https://www.politico.eu/article/italy-joins-calls-for-fake-news-crackdown/?utm_content=bufferce55c&utm_medium=social&utm_source=twitter.com&utm_campaign=buffer; https://euobserver.com/justice/139850; https://www.cjr.org/watchdog/europe-fights-fake-news-facebook-twitter-google.php; http://www.independent.co.uk/news/world/europe/macron-fake-news-law-elections-facebook-social-media-a8140721.html; https://theintercept.com/2018/01/10/first-france-now-brazil-unveils-plans-to-empower-the-government-to-censure-the-internet-in-the-name-of-stopping-fake-news/; https://www.irishexaminer.com/breakingnews/ireland/new-bill-will-help-make-political-advertising-on-social-media-more-transparent--fianna-fail-817491.html; http://www.theweek.co.uk/90730/should-uk-adopt-european-style-fake-news-law; https://www.novinky.cz/domaci/424666-vnitro-se-brani-zemanovi-zadna-cenzura-jen-chceme-varovat-pred-bludy.html; http://koreabizwire.com/south-korean-lawmaker-proposes-anti-fake-news-bill/89762; http://www.aljazeera.com/news/2018/01/asian-leaders-riding-fake-news-mantra-180122090744078.html; https://www.malaysiakini.com/news/412592#xsV0IwEY5PwxPjza.99; http://newsinfo.inquirer.net/927055/president-rodrigo-duterte-treason-ra-10951#ixzz57jeeyEJ1

Government regulation is not the only answer, however. In fact, some have expressed fear that criminalizing fake news could be likened to curtailing freedom of speech.[17] What if these laws are abused? Would they not enable an incumbent government to step in during elections, for instance, and constrain the freedom of expression of its opponents, be they citizens writing on their blogs or accredited journalists writing for major publications.[18] Others believe a line should first be drawn between hate speech and fake news before actually considering the implementation of anti-fake news laws.[19] Still others believe that fake news publishers (including social networks) are not the problem because false information can be had from anywhere. The real problem lies in the ever-present cultural divide.[20]

---

[17] Jim Swift. (11 December 2017). *The Weekly Standard*. "Afternoon Links: Criminalizing 'Fake News', The End of Free Speech, and the Bridge to Nowhere." Available at http://www.weeklystandard.com/afternoon-links-criminalizing-fake-news-the-end-of-free-speech-and-the-bridge-to-nowhere/article/2010804.

[18] Alberto Alemanno. (7 January 2018). *Politico*. "Macron's fake news law will threaten democracy." Available at https://www.politico.eu/article/macron-fake-news-law-will-threaten-democracy/.

[19] Henri Mikael Koponen. (24 January 2018). *International Press Institute*. "Finland remains resistant to 'fake news,' disinformation." Available at https://ipi.media/finland-remains-resistant-to-fake-news-disinformation/.

[20] Miranda Katz. (6 December 2017). *Wired*. "The Fake News Culprit No One Wants to Identify: You." Available at https://www.wired.com/story/fake-news-social-media-danah-boyd/.

Countries that have yet to decide on the matter are not remaining idle, however. Prior to the U.K. elections, for instance, independent organizations formed teams of fact checkers to monitor and debunk fake news stories.[21] Mainstream media outfits left and right have been attempting to educate the public on how to spot real from fake news.[22] In the absence of laws, governments can actively engage the public to help fight the problem. They can launch awareness campaigns to educate the masses in identifying fake news and stay away from the sites that spread them. A simple list of fake news red flags like the one below may be helpful.

- Hyperbolic and "clickbaity" headlines
- Suspicious site domains spoofing legitimate news outfits
- Misspellings in content and awkwardly laid-out websites
- Doctored photos and images
- Absence of publishing timestamps
- Lack of author's name, sources, and data

How Technology Can Help

From a technical standpoint, the same problems linked to criminalizing fake news, may surface. Outright blocking of site domains known for publishing fake news may be prone to a lot of false positives. Site owners (bloggers and the like) may feel that they are being oppressed and this may lead to more problems than solutions.

---

[21] Robert Booth. (19 May 2017). *The Guardian*. "Truth seekers: inside the UK election's fake news war room." Available at https://www.theguardian.com/politics/2017/may/19/truth-seekers-inside-the-uk-elections-fake-news-war-room.

[22] James Titcomb and James Carson. (16 February 2018). *The Telegraph*. "Fake news: What exactly is it – and how can you spot it?" Available at http://www.telegraph.co.uk/technology/0/fake-news-exactly-has-really-had-influence/.

Reputation scores may be used instead. Organizations (whether public or private) can be formed to gauge the reputation of specific writers and sites and issue warnings to readers who wish to stay away from fake news. Instead of outright blocking, content publishers and/or sites can instead be accorded reputation scores that indicate the probability that the content they publish is fake.

Independent fact-checking sites such as https://www.snopes.com/, https://www.factcheck.org/issue/fake-news/, and others can also help individuals check the veracity of particular stories.

Machine learning and artificial intelligence (AI) technology can be applied to actual content as well. Computers can be programmed to watch out for sensational content (e.g., use of hyperbolic language, sensational headlines, misspellings, etc.) on sites or pages. They can then be compiled and analyzed to give stories, pages, or sites reputation scores that reflect the likelihood that their content can be considered fake news. A tool that works like this is Fakebox.[23]

Machine learning and AI are also being used to detect if certain social media posts were most likely spammed by bots. Some tools such as https://botcheck.me/, https://botometer.iuni.iu.edu/#!/faq, and others are available to help you check if a social media account is a bot or not. You can block suspicious posts and accounts on your own end with these. Suspicious posts and the accounts that spread fake news can also be reported to the respective platform owners so they can take action.

Machine learning and AI can also be used to avoid unrelated pictures, video, or audio files from being used to support false claims. A simple check of Exchangeable Image File (EXIF) data can be done to see if proof (a photo or a video) actually coincides with the date of an event it is being linked to or provided as evidence of.[24]

---

[23] Aaron Edell. (11 January 2018). *Towards Data Science*. "I trained fake news detection AI with >95% accuracy, and almost went crazy." Available at https://towardsdatascience.com/i-trained-fake-news-detection-ai-with-95-accuracy-and-almost-went-crazy-d10589aa57c.

[24] David Peterson. (2018). *Digital Photo Secrets*. "What is EXIF?" Available at http://www.digital-photo-secrets.com/tip/38/what-is-exif/.

Most of the tools cited above are not 100 percent foolproof but they are considered a promising start.[25] In fact, content platforms and advertising networks in the U.S. and Europe that don't want to be associated with false or potentially offensive stories use some of them.

The decision to implement an anti-fake news law or not requires careful consideration of all aspects of the problem. Though legislation helps, is it really necessary? Is encouraging a social media clampdown enough? Can technology partners be asked to help? Whatever path a government takes will depend on several factors, including but not limited to how effective legislature is in curtailing crime and similar acts from a historical perspective, how willing the platform and technology owners are to cooperate with the government, and what the nation's current social and cultural realities are.

---

[25] Jackie Snow. (13 December 2017). *MIT Technology Review*. "Can AI Win the War Against Fake News?" Available at https://www.technologyreview.com/s/609717/can-ai-win-the-war-against-fake-news/.