Carter-Ruck

FAKE NEWS
AUTHENTIC VIEWS

A Carter-Ruck Report, 2018

The impact of mass disinformation campaigns on geopolitics, news media, corporate communications and the culture of democratic societies.

CONTENTS

FOREWORD

Nigel Tait
Head of Media Law, Carter-Ruck

Over recent months a growing number of our clients have encountered a set of intertwined issues arising from large-scale, deliberate, coordinated assaults on reputation, using modern communications techniques.

This nexus of problems is popularly referred to as Fake News, a term which is itself controversial. Many commentators argue that it conceals as much as it explains and that certain public figures are stretching its meaning through over-use. Others, including seasoned communications practitioners, point out with some justification that much of this phenomenon is not new at all and has been with us since the ancients.

But the phenomenon our clients are seeking to manage is very real. It is a complex combination of old problems – lies, intrusion, disinformation, inaccuracy and malicious communications – which present with greater intensity, from a far more distributed and often concealed set of sources, across a wider range of platforms than ever before.

We see this in our media law work, where individuals, businesses and institutions often struggle to manage sustained and often unfair criticism from consumers, those pretending to be consumers, pranksters and competitors.

We see it in our international law practice, in the form of inter-state conflicts and sponsored campaigns of subversion and manipulation of opinion. And we see it in commercial disputes, where misleading communications to shareholders and analysts are sadly deployed by unscrupulous people in pursuit of unearned competitive advantage.

That is why we felt Carter-Ruck could play a useful role in bringing together insights from leading thinkers who have been wrestling with the social pathology of Fake News. So in this publication, with eminent contributors from leading think tanks, universities and professional associations, we survey the origins and exponential growth of Fake News and ask:

- What is it, what are its dynamics and direction?
- What are its impacts on business, government and the management of reputation?
- What policy, regulatory and legal responses can contain or eliminate the threat…without undermining the culture of our society in the process?

We hope you find this an engaging and thought-provoking read. And we look forward to hearing your views on this most contemporary of topics over the months ahead.

nigel.tait@carter-ruck.com

THE GLOBAL CHALLENGE OF FAKE NEWS

Dr. Jonathan Eyal
Associate Director, Strategic Research Partnerships,
and International Director, Royal United Services Institute

A new battlefield

For decades, military strategists have argued that the next battlefield may be our brains, with informational war emerging as a key component of modern combat. That time may now have arrived, with many of the deception techniques fit for warfare spilling over into the civilian sphere.

This is a culmination of decades-long processes. Advertisers, psychologists and behavioural economists have been figuring out how to influence people by exploiting personal data harvested by consumer tech companies. Governments defending their informational infrastructure have realised the potential for asymmetrical information warfare by unleashing armies of online trolls. All of these efforts have now come together, and the battlefield is global.

From Macedonia to the mainstream

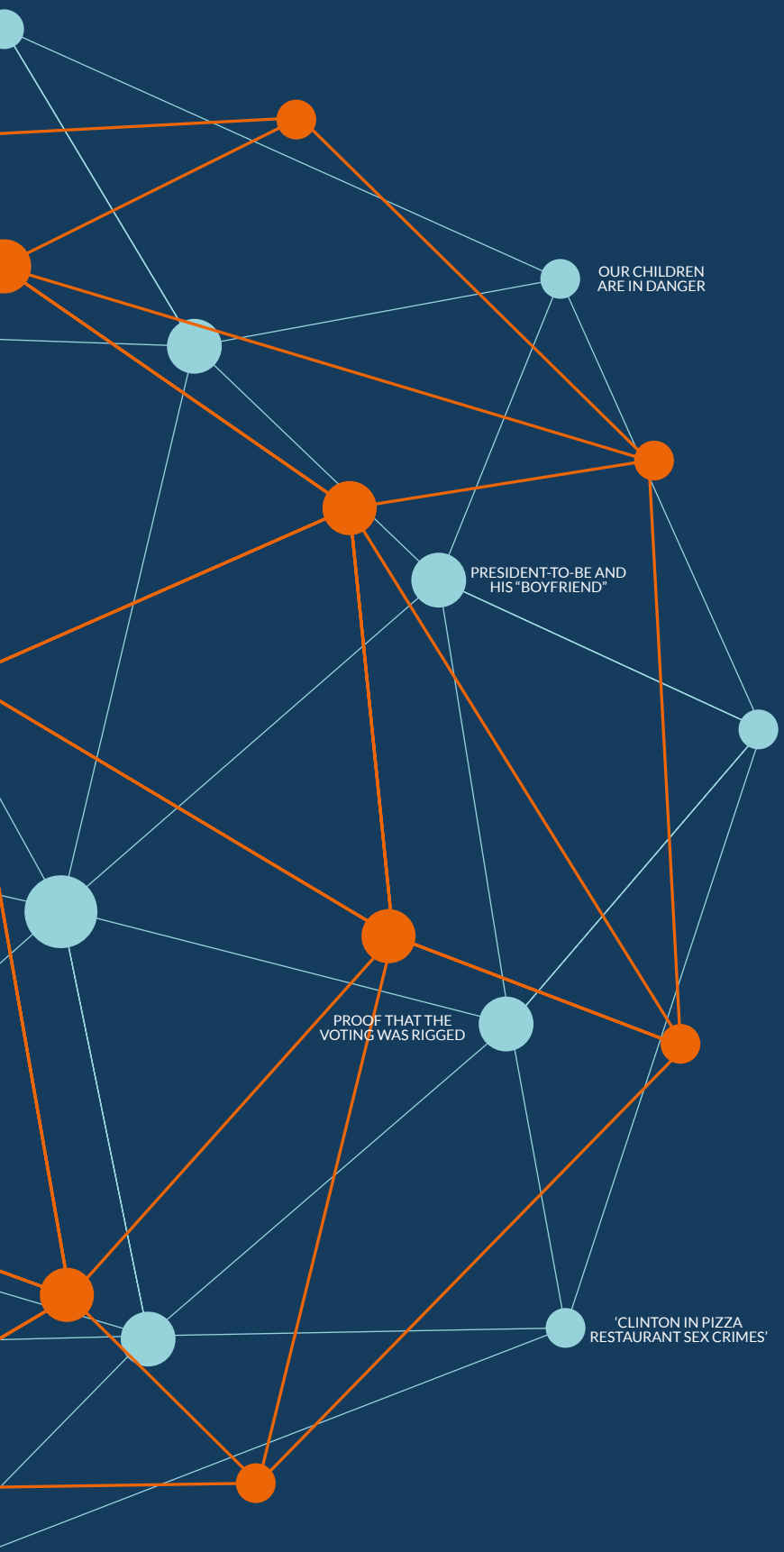
Take the small town of Veles in Macedonia as an example; it's not exactly a household name, and its 40,000 inhabitants are mostly poor. But as implausible as this may now seem, it could have been Veles that helped Donald Trump get elected as the 45th President of the United States of America. For it was here, back in 2016, that at least 140 websites were based, supplying a constant stream of information in support of Donald Trump's candidacy.

It was from websites and social platforms based in Veles that God-fearing American voters first got the joyful news about the Pope's decision to endorse Donald Trump as the next US president. And it was from Macedonia that they first heard of Hillary Clinton's use of a pizza restaurant for a variety of sexual crimes, as well as the shocking news that some of the Democratic candidate's closest associates committed suicide on the eve of the presidential ballots to avoid being found out.

Not only was all this a pack of lies, but millions of Americans who either believed or reacted to the information didn't have the slightest idea that it was generated by people who lived thousands of kilometres away from America's shores, and was peddled around the world by internet operators who didn't speak a word of English.

Nor is this an exclusively American story. When in September 2014 the people of Scotland rejected the option of becoming independent from the rest of the United Kingdom, a number of websites instantly produced "proof" that the voting was rigged. A petition asking for a recount of the ballots gained hundreds of thousands of signatures before the entire affair was exposed as a hoax.

Two years ago, news emerged in Germany that Lisa, a Russian girl of 13, was gang-raped by Muslim immigrants. The horrific crime – it was said – was covered up by politically-correct German police. The story, which within days notched up more than a million views on Facebook alone, prompted a wave of indignation. Hundreds of Germans converged on their parliament holding placards proclaiming "Our children are in danger" or "Hands off my child", and Russian officials formally raised the



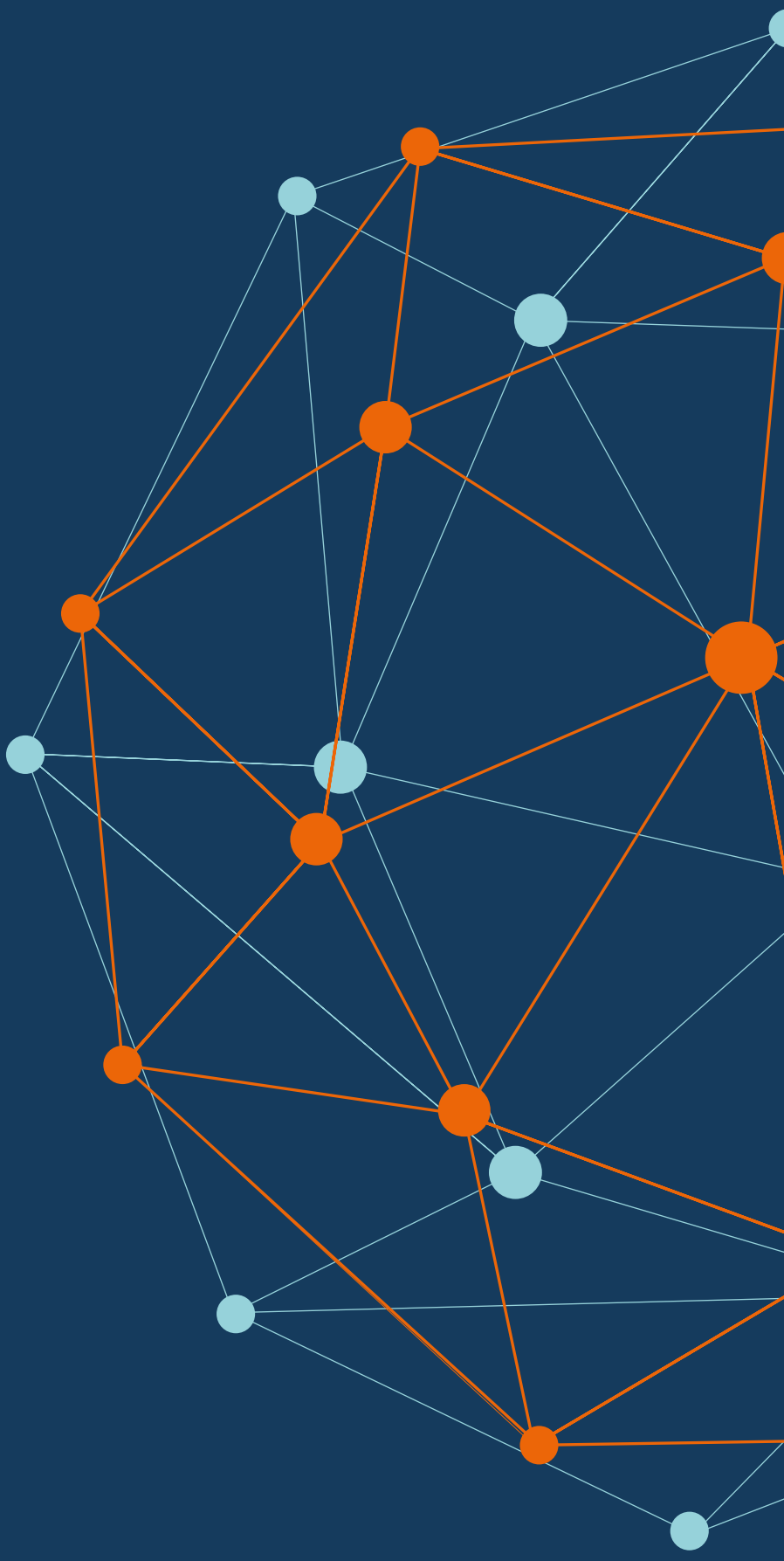
Antecedents

- **6th century BCE:** Chinese military theorist Sun Tzu famously declared "All warfare is based on deception."
- **18th century:** in revolutionary France, the so-called "canards", single printed sheets of paper, contained almost entirely fabricated stories.
- **19th and 20th century:** in the US and Europe, the "yellow press" emerged, daily newspapers usually in tabloid format peddling sensationalist content for sales.
- **21st century:** distributed mass communications technology allows states, criminals and pranksters to find a global audience for disinformation.

83%

of Europeans surveyed accepted that Fake News represents an existential threat to their way of life.

Source: *survey by European Union statistical agency Eurobarometer.*



Cont...

matter with the German authorities. Except the story was a pure fabrication. No such incident happened, and the unfortunate Lisa never existed.

And last year, just as Emmanuel Macron appeared to be coasting to victory in France's 2017 presidential elections, the story emerged that he was gay: pictures of the president-to-be and his "boyfriend" circulated on most social websites. Yet again, pure rubbish.

Welcome to the strange world of Fake News, a parallel universe which, if not checked, threatens to undermine confidence in our institutions and order.

What's new about Fake News?

When discussing the scale and impact of "Fake News", it is worth bearing in mind that the term itself has become very controversial. It is at best a catch-all name for very distinct operations. It covers differing motives, political and strategic, commercial, or even sophisticated pranks. And it covers a range of practices, some of which were well-known long ago, while others are new products of the digital revolution.

The concept of Fake News also describes a small but very worrying group of "weaponised" communication technologies, brought into today's internet reality from the dusty corridors of the Cold War. These could be more dangerous today than their creators ever imagined.

Yet when all is said and done, the peculiarity of Fake News is not deception and lies as such, but the intentional use of such practices in strategic mass communication campaigns, deploying a dangerous combination of social media, computer software, mathematical algorithms and sophisticated advertising techniques.

Do-it-yourself deception

Until relatively recently, the main method of disseminating information was paper.

We all knew the difference between a well-printed broadsheet, edited by a staff of hundreds, produced by thousands of print workers and distributed by tens of thousands of commercial agents, and a photocopied sheet of paper, usually in an awkward typeface, thrust in our hands by a street peddler or demonstrator, or shoved in our post box. We instinctively knew that one was likely to be more reliable than the other.

As for broadcast media, with audio or moving images, these could be produced only by very large institutions, by states or the biggest media businesses.

Yet the advent of the internet has removed the established media's exclusivity. Anyone can generate content and, at least at first sight, a website created by a teenager in his or her bedroom can look as professional as The Times. While one aspect of this technological change is positive – it empowers people to be creative and allows literally anyone to access and address a world audience almost cost-free – electronic platforms have also become powerful instruments of propaganda.

In Europe, up to a quarter of the population now gets its news exclusively from internet platforms, so information is a commodity sold at ever-cheaper prices. A recent survey from the Reuters Institute for the Study of Journalism combined with further analysis from the Oxford Internet Institute, both based at Oxford University, have shown that even when people get their information from established media sources, it comes to them through news aggregator platforms such as Facebook or Google. The survey showed less than half the readers were aware of the information's original source.

At the same time, readers scan news aggregator platforms for headlines and read stories regardless of where they come from, so someone reads a story about a natural disaster in Argentina as it is being reported by a website in Nigeria. Consumers start thinking all this information is generated and supplied for free, and that it does not matter whether you read about the political situation in Venezuela from a news outlet in Spain, a country with a democratic tradition, or a news outlet in Cuba, where all sources of information are state-controlled and financed.

The result is a vicious circle: established media brands erode, entry barriers to new suppliers of information decline, purveyors of Fake News become ever more credible.

Cont...

The technology of disinformation

And if this were not enough, technology means that purveyors of Fake News can reach huge audiences. Software can create social media accounts by their hundreds of thousands. For example no less than 150,000 such accounts operated in Britain in 2016, during the EU referendum campaign.

These spoof accounts on Facebook and Twitter not only churn out false news but also recycle false information, giving it "traction", and the more a story appears on social media, the more credible it appears.

This huge technological power pays no attention to national frontiers or regulations, and is just in its infancy. Newly emerging digital manipulation technologies can also make false information look real, by supplying doctored videos showing real people saying invented things or performing invented actions.

In the 2016 US presidential elections, websites alleged that Hillary Clinton said certain things. By the time the next US presidential ballots take place, candidates will be "seen" to be making statements which appear real, via faked images in hi-tech doctored videos.

State-sponsored disinformation

Most worrying is the growing body of evidence suggesting that governments of certain countries around the world are now actively engaged in using Fake News as a weapon. Of course, this is not entirely new. Britain, for instance, established a "Ministry of Information" exactly a century ago with the purpose of putting out propaganda. Almost every major country subsidised radio stations that broadcast to the world with the same intention.

But, yet again, the scale of Fake News is much bigger — up to 40 percent of the entire news volume circulating in the US media prior to the 2016 presidential elections was fake. And the ability of foreign governments to disguise their identity has also grown. From the indictment issued in March 2018 by Robert Mueller, the American special counsel investigating the latest presidential elections, it emerges that agents in the pay of the Russian government spent years establishing a US presence, complete with fake financial transactions to appear as purely American entities in the run-up to the presidential ballots.

"For decades, military strategists have argued that the next battlefield may be our brains, with informational war emerging as a key component of modern combat."

Russia's splendidly-named "Internet Research Agency" which employed hundreds of people during the past few years and operated tens if not hundreds of thousands of accounts on Twitter, Facebook and other websites, is only the best-documented government effort. One can be certain that other governments around the world have similar organisations, and plenty are studying the potential of Fake News to undermine their opponents.

Restoring trust

There is a lot to suggest that the deeper purpose of inter-state Fake News campaigns is not just to influence this or that vote, but to discredit a rival's political system, undermining its democratic institutions, in particular confidence in citizens' sources of information.

And that seems to be working: in Britain, the percentage of those saying that the news they get can be trusted has dropped from 50 percent to only 43 percent last year, while in the US the figure is only 35 percent.

In most cases, the institutions that are losing trust are not internet bots or social platforms, but those which used to enjoy it the most: mainstream, established media, now increasingly viewed as indistinguishable from much of the low quality content which goes by the name of news online.

Countering this won't be easy: legislation allowing governments to close down websites or social platform accounts can be indistinguishable from censorship, and may be self-defeating, since most national restrictions can be bypassed by the ingenuity of the ever-evolving technology. Still, that does not mean that legislators and governments are bereft of options, although none will be fool proof.

- One approach is the development of enhanced government intelligence capabilities, able to spot trends in the internet and blogosphere. That will give decision-makers early warning of impending Fake News campaigns, and allow useful lead time for rebuttal. Many big companies already have such units to protect them from fake campaigns about their products, and the Foreign and Commonwealth Office in London now has a unit which does exactly the same for British decision-makers.
- Another option is strict regulation during electoral campaigns to diminish the impact of Fake News. It is clear, for instance, that French rules which prevent the publication of any electorally-relevant information 24 hours before ballot day insulated President Emmanuel Macron from the assault based on his stolen personal emails; the same happened in Italy during the country's recent elections. And the EU was spurred to action to limit the impact of Fake News in the run up to the 2018 elections to the European parliament.
- But the most important measure which governments can take is to force internet providers and the owners of social platforms to share responsibility for the information they carry. Just as newspapers are responsible before the law for the material they publish, so should the online-based companies be which, after all, make their money from the same content for which they claim to carry no responsibility.

"A website created by a teenager in his or her bedroom can look as professional as The Times."

To be sure, all these regulations carry risks to individual freedom of expression. But the only other option, which is to allow a free-for-all, carries even greater dangers.

Without being able to agree on shared verifiable facts, there can be no legitimacy in public debate, and little informed decision-making. And without being able to distinguish between fact and fiction, more young men and women may volunteer for violence: Fake News is one of the biggest drivers of radicalisation and terrorism.

The public in most countries seem to get it: in a recent survey compiled by the European Union's statistical agency Eurobarometer, 83 percent of Europeans surveyed accepted that Fake News represents an existential threat to their way of life. The more fragile and recent their democratic institutions were, the more the people of those countries feared Fake News.

We know this phenomenon is corrosive to our institutions; we just don't yet seem to be able to forge a consensus about what needs to be done to contain or counter-act it.

INTERNATIONAL LAW AND THE NEW DYNAMICS OF INFORMATIONAL CONFLICT

Cameron Doley
Senior Partner, Carter-Ruck

As yet, international law provides very limited assistance in combatting the scourge of Fake News and disinformation warfare.

No binding treaties or international agreements have been concluded and, while the Joint Declaration on Freedom of Expression and "Fake News", Disinformation and Propaganda was adopted by the UN, the OSCE, the Organization of American States and the African Commission on Human and Peoples' Rights in March 2017, this represents soft law at best, imposing desirable standards of conduct which are not directly enforceable. As such, it is not a great help to those seeking a stronger and more coordinated response to the dissemination of Fake News.

Furthermore, insofar as the Joint Declaration does provide guidance, it conveys a strong presumption in favour of freedom of expression, warning that "prohibitions on disinformation may violate international human rights standards", and adding that "[g]eneral prohibitions on the dissemination of information based on vague and ambiguous ideas, including 'false news' or 'non-objective information', are incompatible with international standards for restrictions on freedom of expression".

At a regional level, however, we are seeing some efforts to fight Fake News, with the Council of Europe and the European Commission taking significant initiatives. The former advanced a proposal that was adopted by the Committee of Ministers in April 2016 which stated that officials and public figures should neither accuse journalists and media of disseminating propaganda or disinformation, nor induce them to engage in its dissemination.

The EU Commission has now gone further and is convening a multi-stakeholder forum for cooperation in the battle against disinformation. This platform includes governments, online platforms, advertisers and the advertising industry, and is scheduled to publish an EU-wide Code of Practice in July 2018.

It is at national level, however, that we are witnessing the most determined action on Fake News. Germany and India have passed controversial laws making technology companies and administrators of social media groups accountable, while Israel, Italy, Russia, The Philippines, the UK and the US all have legislation pending, which proposes to impose new obligations on technology companies and in some cases individuals, ISPs and website administrators.

While this action might be seen as encouraging, it has obvious limits in terms of its solely domestic reach. Efforts to deploy existing law are similarly limited. For example, the Democratic Party in the United States has commenced a suit against the Russian Federation (together with the Trump campaign and WikiLeaks) following the latter's apparent intervention in the 2016 presidential campaign, but in the absence of an appropriate international forum it has been obliged to file its claim in a federal court in the Southern District of New

York and to rely not on international law provisions but solely on US domestic law.

Many would argue that this situation needs to change, so as to meet a fast-evolving threat which already transcends national and jurisdictional boundaries. It would not be the first time such measures were considered; the UN's Draft Convention on Freedom of Information in 1948 provided that limitations on freedom of expression might be legitimate to curtail false reporting. However, the Draft Convention was never ratified. The same language was also proposed for inclusion in the International Covenant on Civil and Political Rights, but did not make it into the final document.

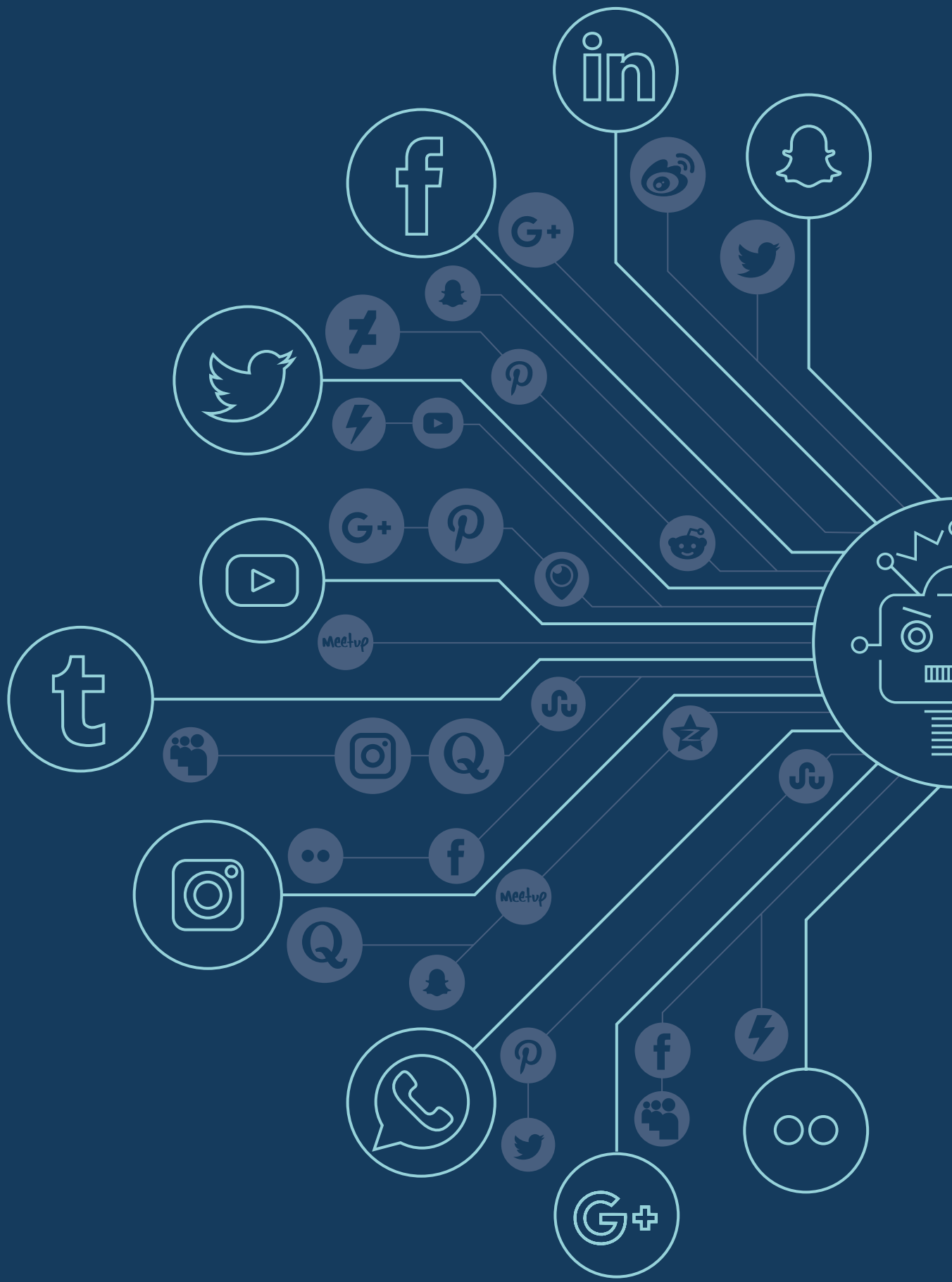
More recently there has been a suggestion that computer-based attacks should be treated as a form of armed conflict and be brought within the provisions of the Geneva Convention. This would, however, seem hard to sustain and those wishing to deploy such provisions in the case of transgression would in all probability find themselves having to demonstrate a level of damage or injury akin to that involving an armed attack using conventional weapons.

The ultimate goal for those seeking to combat Fake News and disinformation warfare would thus seem to be a significant development of the hard international law framework, probably by way of the ratification of a new treaty. Meaningful steps to this end could involve a range of initiatives including multi-stakeholder cooperation around pre-emption involving not only governments but regional bodies, technology companies and non-governmental organisations. Common protocols and processes for crisis management, new multi-agency fact-checking mechanisms, intelligence sharing, automated systems and public education programmes could all play their part and, in this way, the world could foster not just a legal and regulatory environment hostile to Fake News, but a culture that detects it, eschews it and nullifies its effect.

"Prohibitions on disinformation may violate international human rights standards... general prohibitions on the dissemination of information based on vague and ambiguous ideas, including 'false news' or 'non-objective information', are incompatible with international standards for restrictions on freedom of expression."

Joint Declaration on Freedom of Expression and "Fake News", Disinformation and Propaganda

cameron.doley@carter-ruck.com


Meetup
Meetup

RESPONDING TO FAKE NEWS THROUGH REGULATION AND AUTOMATION

Samantha Bradshaw
Oxford Internet Institute, Computational Propaganda Unit

Monetising clicks – incentivising junk news

One of the systemic factors underlying the burgeoning Fake News economy is that the technology and social media companies monetise our attention. If a content creator can deliver edgy information that attracts attention and encourages users to 'click through' to a story, they can generate advertising revenue. Fake News stories are often written with emotional appeal — to spread based on vitality opposed to veracity — and there are clear monetary incentives in place to maximise the production and distribution of this information. If social media companies incentivised high quality content — as opposed to emotionally appealing or outrageous stories and information — we may not have quite the same problem we're having now, where there is a race to the bottom in terms of content quality.

A swarm of bots and cyborgs

Recently, there has been heightened attention around how bots are distorting conversations on social media. In elections and referenda around the world, bots have been used to artificially drive up user engagement by liking, sharing, or retweeting content. Automating these interactions can serve to generate a false sense of popularity or consensus — not only around traditional consumer products, but also around political ideologies or individual beliefs.

Not all bots are bad and many remain an integral part of the internet ecosystem. Originally, bots were developed to perform repetitive and mundane tasks, such as conducting network maintenance or organising and cataloguing content. However, bot functionality was also extended to human interactions through internet Chat Relays, customer service tools, and social media interactions. Today, there are a variety of different terms and functions for these automated accounts, from harmless web crawlers to more malicious bots that are used to spread spam or disinformation.

Over the past two years, bots have been used to push polarizing messages to voters throughout the United States and Europe. Social media companies — such as Twitter, Facebook, and Google — have increasingly become concerned about the proliferation of bots on their platforms and have taken several steps to remove these accounts. There are a number of incentives to remove "bad" bots from online spaces as they not only undermine the quality of legitimate user interactions, but also the quality of user data that is sold to advertisers who want to reach real consumers.

One thing that many people do not realize is that there is an entire political economy supporting the buying and selling of botnets that can be put to purpose. These services are not only found in the deep corners of the internet's "Dark Web", but also on the mainstream internet where 1000 followers costs on average £20. As innovation continues in areas such as artificial intelligence and machine learning, bots will become increasingly sophisticated, making their detection and removal by platforms even more difficult.

Cont...

Planned offensives

Extremely effective disinformation campaigns involve careful planning, but in general there is a low barrier to entry. During the 2016 US election, disinformation stories were crafted and disseminated alongside traditional offensive cyber operations—such as email hacks and data leaks. For an attack this large, it would have taken months of preparatory work to identify networks of people and engineer situations to gain access to email accounts and sensitive documentation. It also takes time to execute a dissemination strategy, which typically involves strategic data leaks, crafting conspiracy theories, and the propagation and amplification of messages by bots until they are ultimately taken up elsewhere in the blogosphere, partisan media, and mainstream media.

'Pizzagate' is a clear example of an offensive that deployed all the elements discussed above. Email leaks — secured through phishing attacks — targeted Hillary Clinton's campaign manager John Podesta. In the raft of hacked emails were receipts from a pizza diner called Comet Pizza in Washington DC. These receipts eventually formed the basis of an online conspiracy that suggested John Podesta and Hillary Clinton were running a paedophile ring in the basement of this pizzeria. This conspiracy was amplified so broadly that a man named Edgar Welch drove to the pizzeria with a gun, fired shots in the air during business hours, and proceeded to search for children who were "trapped" in this basement. No one was hurt, and Welch was arrested and sentenced to four years in prison. Nevertheless, this example demonstrates the power of a well-executed disinformation campaign.

Clamping down: regulatory responses

Tackling Fake News is no easy task for government regulators. Increasingly, policymakers around the world are searching for new ways to deal with the spread of bad information online. However, new regulations that seek to thwart the spread of "false" or "fake" content could have a chilling effect on free speech. Instead, governments should look towards mechanisms that would encourage the enforcement of laws that are already in place to deal with harmful forms of content. Other initiatives could focus on the deeper systemic issues, such as how social media algorithms incentivize the spread of false, extreme, or other forms of negative content.

Another area of regulatory intervention could look at the surveillance economy and how data is used to target political messages to individuals online. Unscrupulous political and state actors have already exploited user data to target people with political messages and advertisements. These posts — sometimes called dark advertisements — are often tailored to an individual, so the message one person sees could be very different from another. We have seen political advertisements targeting minority communities during the 2016 election in the United States and in the United Kingdom to suppress voting and political participation. Ultimately, dark advertisements polarise voters, lower trust in institutions, and degrade the quality of our democracy.

Governments are taking a number of positive steps to improve transparency in political advertising. Some positive interventions include verifying the identity of people and organisations purchasing advertisements on social media, and allowing users to see who and why they are being targeted by messages. Other legislation requires social media companies to create a public archive of all advertisements bought and sold, to hold political parties accountable for any dark advertisements they are purchasing during their campaigns.

Clamping down: computational responses

Artificial intelligence is often proposed as a solution to Fake News. There are a number of areas where AI is really effective in flagging, blocking, and removing content online. In areas such as child protection or terrorism, great strides have been made in applying AI and machine learning models to tackle the spread of harmful content. However, it is difficult to automate a response to "Fake News" because what is considered "truth" can be subjectively different for everyone, as opposed to issues related to child protection or terrorism where the decision to remove content is much more black and white. At the same time, most "Fake News" and propaganda is switching from simple text to video and images, where there is still limited AI capacity.

"...platform companies like Facebook and YouTube are concerned about the proliferation of fake accounts and bots, because it undermines the quality of the user data."

Nevertheless, there are indicators that could be used to flag different types of content and potentially to identify Fake News. For example, algorithms can down-rank content that individuals share but don't actually click through to read. Nevertheless, having AI make decisions about what content is true and what is false would be morally and politically perilous, resulting in a range of free speech issues that would de-value social media. Instead, computational responses are best suited to identifying instances of harmful, fake or conspiratorial content going viral and flagging them for action, but review by human editors should always remain a part of the take-down process.

Watching, learning, applying our best laws

Social media hasn't broken our legal and regulatory systems. There are still many laws that can be applied to protect individuals from hate speech, harassment, defamation, and other forms of harmful content. What is needed is better enforcement of existing legal structures, as well as the terms of service agreements developed by companies. This won't solve all problems around Fake News, but it will ensure that the internet remains a free and open space for ideas and conversations.

With every new technology there has always been a period of learning, and old laws now need to be updated for present times. The invention of the printing press, radio, and television all had similar learning periods where society updated its norms, regulations and laws to limit bad behaviour while reinforcing the good. With social media, we are currently in this learning phase.

New technologies always bring uncertainty, and it's not always immediately clear how our old laws can be updated to address some of the changes we're facing today. But laws are designed to be durable, and it's important that government, citizens, lawyers and industry have an open and active conversation about how law can mitigate harms while enhancing democracy.

13%

The number of Twitter accounts that are actually automated.

REMOVING FAKE CONTENT FROM THE INTERNET

Alasdair Pepper
Partner, Carter-Ruck

In today's hyper-connected environment, potentially damaging information can surface on a multitude of platforms, from traditional media, independent websites, online reviews, blogs and social media platforms through to the suggestions and links contained in search results.

If you have reason to believe this may happen, the priority is to minimise the risk that the negative material is published in the first place, by contacting the publisher before publication and if necessary obtaining an injunction from the relevant court.

In England, injunctions are usually effective to prevent publication of specified material and the fact that an injunction has been obtained often goes unreported.

Despite the principles of open justice, the identity of the parties can be anonymised and the publication of subject matter restricted, so that it is not possible to identify the individuals involved or the subject matter of the injunction from the court papers or any publicly available judgment.

As for material that has already been published, the first step is usually to complain directly to the primary publisher, the website host, Facebook, YouTube, Twitter, or any other social media platform and search engines, demanding the immediate take down of the damaging information. In addition to the relevant law, you can often claim that the information should be deleted on the basis that its publication is in breach of the terms and conditions of sites like Facebook and Twitter.

If that doesn't work, the next step could include: making a complaint to the Information Commissioner's Office or bringing proceedings for defamation, misuse of private information or breach of copyright, or under data protection laws (in the UK this would mean making a complaint under the Data Protection Act 2018 and the GDPR, including the so-called "right to be forgotten", now also referred to as "right of erasure").

Combining these options can increase the likelihood of removing, delisting or rectifying inaccurate information or personal data. It can therefore increase your chances of preventing or reducing potential damage to your or your organisation's reputation.

These techniques can be very successful. There have been numerous instances of action securing the removal or amendment of multiple articles, posts and other online material including photographs:

- One high net-worth individual succeeded in securing the removal of about 400 URLs from Google, following a campaign of take-down requests. This strategy also resulted in the removal of hundreds of posts from social media websites such as Twitter, Facebook and Instagram.
- A prominent academic got personal photographs shared over the internet taken down from newspaper websites, other sites, blogs and Twitter, and secured the delisting of hundreds of images from various search engines.
- A well-known personality took action and prevented the publication of a story in four major newspaper groups, going on to secure the removal of private material from websites, blogs, Twitter, YouTube and elsewhere, reducing exposure on search engines and permanently removing content from host websites.
- Content from a number of internationally-recognised publications in various countries has been 'geo-blocked' from being accessible in England.
- Numerous individuals have succeeded in achieving substantial amendment to many third party 'Know Your Client' and due diligence reports, often securing the complete removal of negative material and prejudicial classifications.

alasdair.pepper@carter-ruck.com


TRUTH?
HACKING
MAIN STREAM MEDIA
ELECTION
BIG DATA
POLITICS
DEMOCRACY
MEDIA
PAPERS
SOCIAL
NEWS
GLOBAL

THE FUTURE OF NEWS MEDIA

An Interview with Rasmus Nielsen

Professor of Political Communication and Director of Research, Reuters Institute for the Study of Journalism, University of Oxford; European Commission High Level Group on fake news and disinformation online.

Professor Nielsen, you're a leading European authority on this subject, so the big first question has to be: what is Fake News?

If I had any say in this, we would use the term Fake News only narrowly and precisely to refer to false and fabricated content masquerading as news. But it's clear that this is only a small subset of what both politicians and ordinary people mean when they use the term Fake News.

Politicians use it in a highly instrumental way: to delegitimise news media when they report things they don't want reported or of which they disapprove.

But for ordinary people the term resonates with their experience that much of the news they come across is of poor quality: sensationalist or superficial or inaccurate or highly politicised. The reason the term is very problematic is not simply that it's highly politicised and frustratingly general. It's that much of the really dangerous disinformation that circulates in our society is neither fake nor news.

It can be accurate information that is taken out of context and deployed strategically, to hurt someone for political gain or profit. It's often not news in the sense that it's not really about fact-based reporting but simply expressions of opinion that can be seen as outrageous by people who disagree with them, or the promotion of specific views in the public space through social media campaigns.

Why are people seeing so much more of this at the moment? And what is the impact on public perception and trust in news media?

We don't know that people actually see all that much more of this content than they did in the past.

When we do focus groups or interviews with ordinary media users in different countries, people will almost inevitably say "well that's an old problem; there's always been Fake News".

But it's clear there are some developments driving the generation of more low quality or problematic content, as well as new ways in which these are distributed and interpreted.

> **"It's clear there are some developments driving the generation of more low quality or problematic content."**

First, the pressures on business models that have historically sustained professional journalism mean that some news organisations are not able to invest the same time and effort into reporting each individual story as they did in the past. This can mean that they make mistakes or run with things that they should have been more careful or guarded with.

Cont...

So we're talking not just about technology but the commercial pressures which mean that a journalist won't necessarily take the same steps to substantiate or check their sources or ensure balance, or that they've got more than one source before printing an allegation as if it were fact. It's what the profession itself calls churnalism.

Second is distribution. There are communities of users on social media who both promote and engage with this kind of information and it means that there is a fair amount of this stuff flourishing on sites like Facebook and Twitter. This is driven in part by demand but also sometimes because the systems can reward engagement.

Then the final point is about meaning and interpretation. In societies where trust in public institutions and the news media is eroding and political life is growing more polarised, the risk is increasing that any given piece of news or opinion is seen by at least a sizeable minority of the population as so outrageous as to deserve the moniker of Fake News.

This is the dynamic that President Trump plays to very effectively but it's also a dynamic that, say, the Momentum activists in the UK sometimes appeal to. They will point out reporting that some might consider perfectly acceptable, if perhaps partisan, and argue it is Fake News, perhaps because they simply disagree with the line being reported or the stance being taken.

Does this mean that the availability of non-traditional media invariably supports viewpoints and movements outside of the centre, which break through the gatekeepers and go directly to a popular audience?

I would put it a little differently. It's important to remember that the same technological change plays out in different ways in different contexts. So digital media gives everyone more opportunity to express themselves. This reduces the hard power of traditional gatekeepers. How much it changes public discourse depends on the soft power of those gatekeepers, whether these be news media or politicians or other public institutions.

So in countries where public trust in news media and politicians is higher and where politics is less polarised you see the same technologies being used more and more widely - digital media, social media and so on - but you don't see the kind of polarisation and fragmentation and breakdown of consensus and public discourse. I have not seen many commentators suggesting that Emmanuel Macron won in France because of Facebook.

In this race to the bottom, what is the answer for journalism to preserve its professionalism and value?

The questions every news organisation needs to ask itself today are: "what is the problem that we solve and who do we solve it for?"

The old model of trying to do everything for everybody is extraordinarily hard to deliver in a satisfying way. Even genuinely independent and relatively well-funded public service media organisations like the BBC or its German equivalent ARD are finding it hard to do everything for everybody the way they aspired to historically.

When it comes to news organisations that do not benefit from generous public funding but have to pursue professional journalism based on sustainable commercial business models, they have to make a decision. What is the value they create and who do they create it for?

Then they need to focus their activities on that, and I would say currently we see two main models of how news organisations are actively trying to regain trust.

One is the response I would associate with editors like Marty Baron at the Washington Post or Steve Adler of Reuters News Agency, who say the best response is better journalism. It's a return to the classic virtues of professionalism — fact-checking, accuracy and so on — and these organisations are trying to stand out from the scrum by being better at professional journalism. They are still wedded to the idea that they are impartial and that they are serving everybody who is interested in their content.

A different response is offered by news organisations that embrace the proud UK tradition of knowing who you are, what you stand for and who you believe you are trying to serve. In the UK newspapers have historically been unapologetic about having a clear voice and clear editorial line and orientating themselves towards a certain group or certain segment in society.

This model is becoming more widespread even in the United States where you now see not just Fox News and MSNBC in television but online organisations like the Huffington Post and Vox who clearly believe that the way to regain the trust not of the public but of their public is to take a very clear stance on who they are, what they do and who they try to represent.

If you had a principal message about the impact of these changes on individuals and businesses that are often the subject of interest in the news media, what would that be?

I think we should not lose nerve. It's clear that our democracies are becoming far more rambunctious sometimes, even unruly, crude and uncomfortable, and I really appreciate and understand that it would be intensely uncomfortable to be at the receiving end of some of this information.

But open societies with robust institutions can live with discomfort.

"We need to think about targeted responses that deal with the most malicious forms of disinformation."

So from my point of view we need to think about targeted responses that deal with the most malicious forms of disinformation. At the same time we need to have confidence in the systems that have served us in the past, in situations where our politics was highly polarised and disputatious, and continue to renew those institutions — in politics, in the news media, in civil society and increasingly in the technology industry — that enable our democracies to function.

So I would say we need to take this very seriously, but we should not panic.

MANAGING CRISES IN THE AGE OF FAKE NEWS

Claire Gill
Partner, Carter-Ruck

The era of Fake News adds a new dimension to media crisis management.

You are now increasingly likely to face stories that are not just inaccurate or slanted but entirely made up.

One way of dealing with this is the quick and total rebuttal: "This is Fake News!" But this tactic has been over-used of late, and can lead the public to the opposite conclusion.

So, unless the story is so obviously fake that no-one will believe it (in which case it may not even be defamatory, because it may not damage your reputation) then we recommend a two-pronged approach.

When faced with false and damaging allegations, secure good PR advisors and good lawyers — preferably ones that will communicate effectively from the outset.

PR advisors will determine the messaging. The lawyers can up the ante, using the law to persuade publishers to stop or change the story, and in extreme cases taking injunctive action to halt a story with a court order.

It is possible to get an injunction to prevent the publication of private material, such as intimate photographs, whether they are real or not, and to stop conduct that may amount to harassment.

"PRs will determine the message...lawyers can up the ante."

You need a plan. Here are seven tips:

1. **Decide your lines of communication** and crisis protocols in advance: know who to call, have a dedicated person internally responsible for making decisions and giving instructions, and nominate a person to deal with the press.

2. **Have an early call with PR advisors and lawyers to:**
   - determine the severity of the situation. What is the allegation, and to what extent is it true or false? Where will it be published (or where has it already appeared)?
   - identify where the threat is coming from. Has a credible online news site threatened to publish a damaging story, or is an individual with an axe to grind threatening to voice their grievance online? Different approaches will be needed for each scenario.
   - decide communication channels, which may include direct communication with the source of the story, putting out public statements or speaking to the press.

3. **Put together information that rebuts the allegation.** You may not need to deploy it all, but your advisors should understand it, including where the weaknesses lie, so that rebuttals or legal letters do not include "hostages to fortune".

4. **Responsible journalists will approach you first for comment.** Engage with the questions but if the allegations are serious consider communicating the answers via lawyers, and copy the editor or website owner.

5. **Consider your legal options.** These include writing a "cease and desist" letter, and in appropriate circumstances threatening legal proceedings or an injunction.

6. **Act quickly.**

7. **Do not over-react.** Doing so may draw more attention to the story.

Your crisis management protocols will be built on the same basic principles as before — but updated to address the new media environment, where threats come faster, with greater intensity, from far wider sources.

claire.gill@carter-ruck.com

GETTING IT IN PERSPECTIVE: THE PUBLIC RELATIONS INDUSTRY vs FAKE NEWS

Francis Ingham
Director-General, Public Relations and Communications Association (PRCA).
Chief Executive, International Communications Consultancy Organisation (ICCO)

Is Fake News really a thing?

It is a thing. It's in the public mind, more than it used to be, because of social media. People can create it themselves and spread it themselves, across multiple platforms.

But it's not just anonymous people acting through new media. For example, Jacob Rees Mogg recently got a lot of support for re-tweeting a highly questionable infographic in The Sun newspaper about how everything will be cheaper if Britain withdraws from the Customs Union. There are lots of examples of people disseminating dodgy content on social channels to influence opinion.

Public trust

In the public vocabulary, the phrase Fake News is often just an excuse to disbelieve what you've read. It includes patent falsehoods as well as inconvenient truths. But we need to get this in perspective. Yes, there have been falling levels of public trust in news media in recent years — but then again there have been falling levels of public trust in everything.

If we look at IPSOS Mori's recent poll we can see that public trust in the professions is lower than ever. But the significance of this can be hugely overstated. In the PR industry, there are many who evince a rather pathetic desire to be loved when what we need most is actually to be respected.

The risk to clients

Over the 10 years I've been running the PRCA everything has got faster.

The news cycle is faster, companies collapse faster, the intensity of scrutiny is much greater and rising all the time.

Unless you combat Fake News fast it can have a rapid effect on an organisation's existence. It doesn't only apply to deliberate falsehoods either: if we look at how Snap lost £900 million in value after one tweet from Kylie Jenner — a tweet which was just an expression of one person's subjective opinion — we can see where the vulnerabilities lie.

The impact on PR today

This means move more quickly. The PR industry is configured better than most to do that. We were already set up to react fast because we shape and respond to the fast pace of the news agenda. We understand frenetic newsroom cultures. And we get social media better than others.

Just a few years back, some may have got away with selling bad social media work because clients didn't get it, but that's changed and the industry has kept one step ahead and has changed to meet growing demand.

If you look at the World PR Report produced by the ICCO — the global voice of public relations consultancies, of which I'm also Chief Executive — you'll see that what's driving the growth of PR is three things.

One is the diversification of agencies' offerings to meet the changing environment. Two is that clients are investing more in reputation management, as CEOs recognise that reputation's impact on the bottom line and their own remuneration is greater than ever. Three is the growth of social and digital work. Social media, multimedia content creation and digital build and production are the fastest growth areas for PR firms.

The future of PR

A considerable part of the disinformation we're seeing is automated. But I don't really see PR itself automating that much. Sure there will be automated tracking and monitoring, but our industry is primarily rooted in personal relationships, insight and creativity. These are the hardest things to mechanise. I can imagine a future in which a robot can write a bad press release. I can't imagine a robot angling it, making it sing, or selling it in.

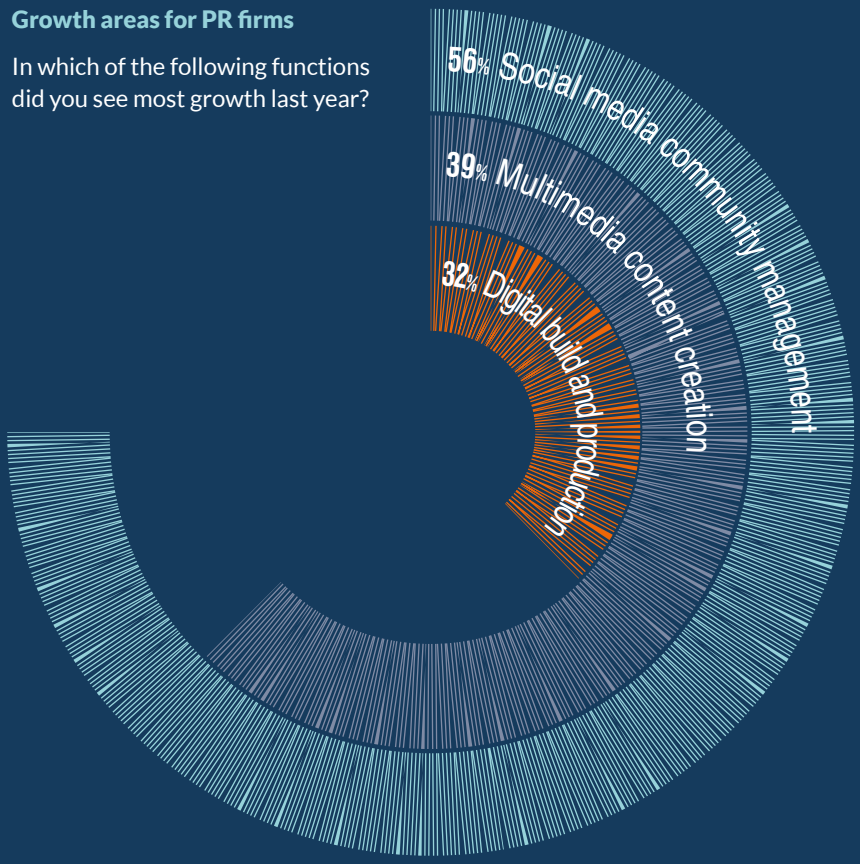
If you had one message what would it be?

Fake News can destroy your company so react quickly when you have to.

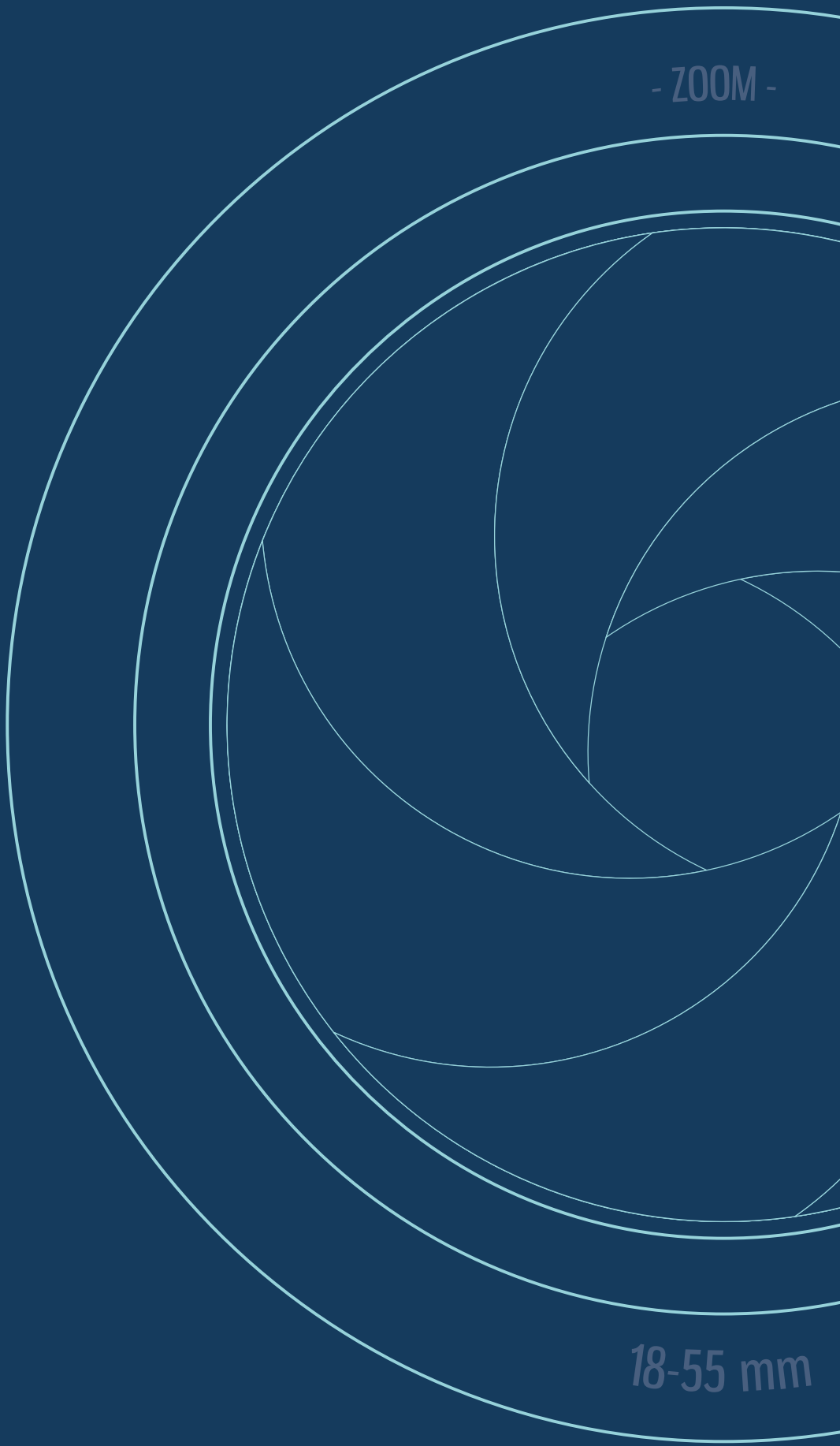
DO	DON'T
React quickly if the statement is material	Go over the top
Seek withdrawal and takedown	Forget that people are expected to have a sense of humour
Get lawyers involved at the outset alongside your PRs if it's serious	Rely on lawyers who are unfamiliar with PR and aren't used to working alongside PR consultants

Growth areas for PR firms

In which of the following functions did you see most growth last year?



Source: *study by OnePoll in July to August 2017 based on a sample of 459 international PR employees in 63 countries.*


- ZOOM -
18-55 mm

NEW THREAT – ESTABLISHED REMEDIES: THE ENDURING EFFICACY OF MEDIA LAW

Adam Tudor
Partner, Carter-Ruck

Despite the fast changing media environment, with disinformation being distributed across multiple platforms by thousands of people every day, the legislative and common law equipment we need to protect individual and corporate reputations is already largely in place and in some respects has been since antiquity.

As in codes of laws from the Romans and the Hebrews through to the Teutons and the Anglo-Saxons, today in the UK it is potentially actionable if one party (the publisher) makes a statement to one or more publishees that causes or is likely to cause serious harm to the reputation of another. This is the tort of defamation, of which the term "libel" refers to statements in permanent forms, with "slander" being the cause of action where the publication is more transient, such as verbal statements. The Defamation Act 2013 sets out the main defences which may be available to a publisher in a libel claim and which in some respects have raised the bar for claimants. However, it remains a striking facet of English law (and a cause of considerable resentment among the media) that, once a claimant has established a prima facie case, much of the burden then shifts on to the defendant publisher.

A successful libel claimant can secure significant damages as well as an injunction preventing further publication – not to mention a prominent apology where the case is settled or is subject to the "offer of amends" regime. So libel remains a popular route for protecting, or repairing damage to, reputation.

Claims before the UK courts can range from mass online and print publication of defamatory statements to millions worldwide, to a defamatory tweet or other social media post to a handful of readers.

Libel and its defences

Perhaps the most obvious potential defence is Truth. For this to succeed, the defendant publisher (and the burden rests squarely on the defendant) must show that the allegation complained of is substantially true. So if you're making a complaint you should tell the publisher as clearly as you can what they got wrong.

Another defence is "honest opinion" which is where the publication is not an allegation of fact, but a comment or value judgement. Obvious examples are things like restaurant or theatre reviews – basically, as long as you actually ate the meal or saw the play, you'll be able to express whatever opinion you like as long as it's honest. But it can get more complicated when dealing with more nuanced allegations – thus, is it an imputation of fact or opinion to accuse someone of being a "racist" or an "extremist"? (Predictably, the answer is that it all depends!)

Perhaps the most elusive of the defences is "public interest". This is designed to encourage responsible journalism on important matters by offering a defence even if the publisher can't prove that what it published was true.

Cont...

Section 4 of the Defamation Act 2013 holds that it is a defence to show that the statement sued over was on a matter of public interest, and that the publisher (most obviously through the journalist/editor) *reasonably believed* that publication was in the public interest. In deciding this, a court will look at all aspects of the case – the evolution of the article, how well-researched it was, whether the claimant was contacted prior to publication, whether the article sufficiently reflected any responses received etc. – and make appropriate allowance for "editorial judgement". Predictably, much depends on that word "reasonable".

Section 4 is a fairly new defence (albeit drawing from years of case law), which at the moment makes it rather unpredictable as a new body of case law builds up around it. We can expect more court guidance in the months and years to come.

The UK has over the years been seen as a favourable jurisdiction for libel claimants, and indeed London has been, and to a considerable extent is still, known as the "libel capital of the world". The UK media have frequently complained (and indeed campaigned) about what they describe as "libel tourism", namely the use of the English Courts by overseas claimants suing over publications with little or no readership in or connection to this jurisdiction.

While the extent of that problem has been hugely exaggerated, the 2013 Act put in place certain safeguards to address it.

But overseas claimants are still entitled as of right to sue in England over worldwide publication if the publisher is domiciled here, and indeed can sue in England over publication here even if the publisher is based elsewhere in the EU or other Lugano Convention countries (such as Switzerland, Denmark and Norway).

There is a lesser-known route which is to claim under the separate tort of "malicious falsehood": an alternative to libel. This can be used when a statement is not necessarily defamatory but nevertheless causes financial harm. Unlike libel, here the burden is on the claimant to prove falsity and malice. So it may sound more dramatic but is generally harder to pursue.

Privacy

If you want to prevent publication of private or confidential information, one can make a claim for Misuse of Private Information and/or Breach of Confidence. The key question a court will consider is whether there is or was a reasonable expectation of privacy on the part of the claimant. If so, the court will then balance Articles 8 (privacy) and 10 (freedom of expression) of the European Convention on Human Rights and will ask if disclosure was in the public interest, and to what extent the information was or is in the public domain.

If the court finds in the applicant's favour, the remedies include an interim injunction and damages, which can make this a very attractive route – indeed, the injunction is likely to be crucial where the aim is to prevent private matters becoming public and where compensation clearly won't be an adequate remedy.

In cases of racial, religious or gender-related hate crimes, or of harassment or blackmail, the court will take these aggravating factors into account. Criminal proceedings should also be considered alongside internet takedown requests and injunctions.

Data protection

Another weapon in the armoury of possible claims is using data protection law. Remedies are available for the unlawful processing of personal data, which can include publication of inaccurate or private data. Under the UK regime, there is an exemption for journalists, but it is not a blanket exemption to the requirements of the Data Protection Act.

In some respects of course the law is evolving to keep up with changes to publishing in the modern age. There is for example the "right to be forgotten" regime which derives from EU Data Protection legislation, under which one can require a search engine to delist or block certain search results that come up when a search is made against your name. A recent case in England established that Google was required to delist certain results that breached the UK's regime for the rehabilitation of offenders, and further rulings are expected.

In that case, the judge remarked that the matter involved "novel questions, which have never yet been considered in this Court". We can anticipate more such questions arising as communications platforms evolve – just as we can reasonably expect that certain longstanding principles will continue to be applied.

adam.tudor@carter-ruck.com

Fake News in the ancient world

"The making of false and derogatory statements has been recognised as a wrongful act from the very earliest times and as an actionable wrong in nearly every modern system of law."

Peter Carter-Ruck, 1972

Law Reforms of King Uru-inimgina of Lagash (24th century BC)

"If a man falsely claims that the virgin daughter of another man was not a virgin, and his claim is proven to be untrue, the false accuser shall be fined 10 sheqels of silver"

The Mosaic Code (discovered 7th century BC?)

"Thou shalt not raise a false report… put not thine hand with the wicked to be an unrighteous witness… Thou shalt not go up and down as a tale-bearer among thy people".

Hammurabi's Code (1754 BC)

"If anyone "point the finger" at a sister of a god or the wife of any one, and cannot prove it, this man shall be taken before the judges and his brow shall be marked (by cutting the skin, or perhaps hair)."

Roman Law (450 B.C.)

The offence of famosus libellus (written defamation) was punishable by death.

Teuton Law (6th century)

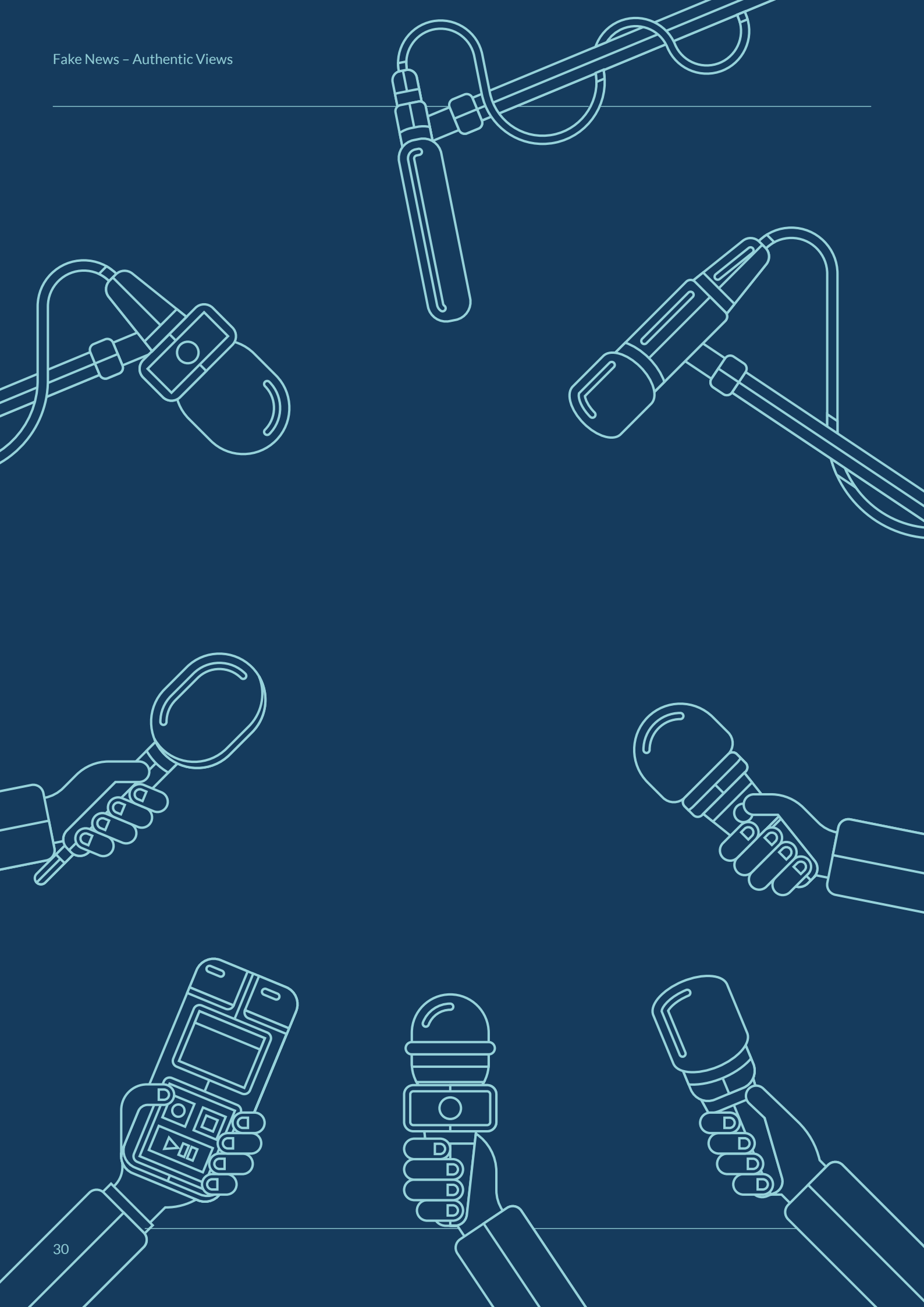
The Lex Salica decreed that if a man called another a wolf or a hare he must pay him three shillings; to reflect on the chastity of a woman secured a fine of 45 shillings, though proof of truth was a complete defence.

Anglo-Saxon Law (9th Century)

In his Doom Book, Alfred the Great introduced the Lex Talionis under which slanderers' tongues were removed.

The Statute of Gloucester (14th Century)

"Every deviser of false news, of horrible and false lyes [against] great men of the realm" to be hanged, drawn, quartered, mutilated or fined, imprisoned or pilloried.



CELEBRITY POLITICS IN THE FAKE NEWS AGE

Mark Wheeler
Professor of Political Communications, London Metropolitan University;
Visiting Fellow at the London School of Economics and the Global Policy Institute

To understand how the phenomenon of celebrity has developed and interacts with politics, and how so-called Fake News has become such an important part of this, we need first to understand a new and related phenomenon.

Social media and mainstream media have begun to feedback into one another, and now the two spheres are beginning to create a new hybrid ecosystem of interacting media that is unfamiliar to many established politicians and institutions.

This is being exploited by new political actors — especially but not exclusively those who can leverage pre-existing public recognition and notoriety and deploy it across novel platforms — to bypass the traditional channels of communication and reach directly to new mass audiences of dissatisfied people, changing the culture and potentially the fate of nations.

Hybrid media drives a vicious cycle

The hybridisation of social and mainstream media is increasingly common. People engage with ideas they encounter first on social media — often Twitter but increasingly Instagram, Facebook and even Snapchat — and then the fact of that engagement alone propels it into what's now often called the mainstream media.

We see articles in newspapers, on TV and on the websites of major news organisations that are reporting on stories that are trending on social media, and on the reactions that stories receive on social media. You get a story about a tweet that went viral; you get stories about how people react to tweets, reporting the replies to a tweet.

In this way we see a vicious cycle of news reporting, raising the profile of specific ideas and helping to construct those ideas, irrespective of whether they are true, and irrespective of whether statements are being reported in context or out of context.

Circumventing the filters

Politicians notice this and see it as a means of circumventing traditional gatekeepers and traditional news media, which previously served as a filtering mechanism, limiting the dissemination of disinformation. This is now a very effective way of influencing the news agenda.

A benevolent view would see this as a way of enhancing popular engagement, strengthening democracy. A less sanguine view would see this as enabling politicians to propagate distorted views, misrepresent facts surrounding policy issues, traduce opponents, and so on.

In this more negative view, we see the new media enabling not democratic engagement but populist demagogy, poisoning public discourse and the roots of a democratic culture.

Cont...

The shifting geometry of communication

The term Fake News is the current buzzword. But the language can change. 20 years ago everyone was talking about Spin. Last year it was 'Post-Truth'. The nomenclature changes but the underlying phenomenon is the same.

What has changed of course through social media is the geometry of political communication. It used to be top down and filtered, by a commentariat that was connected with key lawmakers, celebrities and business. But that commentariat is not just being outflanked by new media, it also took a bath by failing to predict and account for a succession of political shocks — Trump, Brexit, the UK election — which were themselves outcomes of that changing media environment.

This is, in truth, predominantly a UK and US phenomenon for now. But who is to say the process is over, that this will not spread further? We see Italy. What other highly connected societies will follow this route?

What politicians need to know is that they can now use new media to connect directly with their core support base, as Trump does with Twitter, as Corbyn does with Facebook. In the latter case it's interesting that Corbyn's response to the recent allegations of contact with foreign spies was to ridicule the claims on a video that was then shared millions of times on social media.

In this, politicians sense that they can exist and thrive as outsiders to the mainstream. This weakens the centre and propels people from the margins to leadership. It also favours those who have pre-existing celebrity, or who can find strong institutional bases of support for their anti-establishment views.

Trump for example had spent most of his previous life in the news media, as a property developer, as a philanderer, as a gameshow host, as someone leading a somewhat narcissistic celebrity life. On the other hand, a Sanders or a Corbyn can garner similar but opposite support as anti-celebrities because of their supposed authenticity — while using similar techniques of communication to engage with their supporters in pre-existing Democratic or Labour parties.

Whether this is good or bad depends on your point of view. To some it brings inclusiveness and a marketplace of ideas; to others, distorted public spheres, silos and echo chambers.

But one thing is clear. No politician — and no adviser to those active in the public sphere — can afford to disregard this new terrain.

The threat of fake celebrity endorsements

In the US in particular but also in the UK we see celebrity entering into all spheres of public life and into commerce via advertising and sponsorship deals.

OJ Simpson's deal with Hertz is one model. David Beckham's endorsement of his own range of products, or Jamie Oliver's launches of restaurants and utensils, is another.

Where Fake News comes in is troubling. In the US we have seen a wave of false celebrity endorsements of products. Most notably Jennifer Aniston, one of the highest paid actresses in Hollywood, was falsely reported as endorsing a skin cream product. This reached proportions significant enough to spur an FTC investigation.

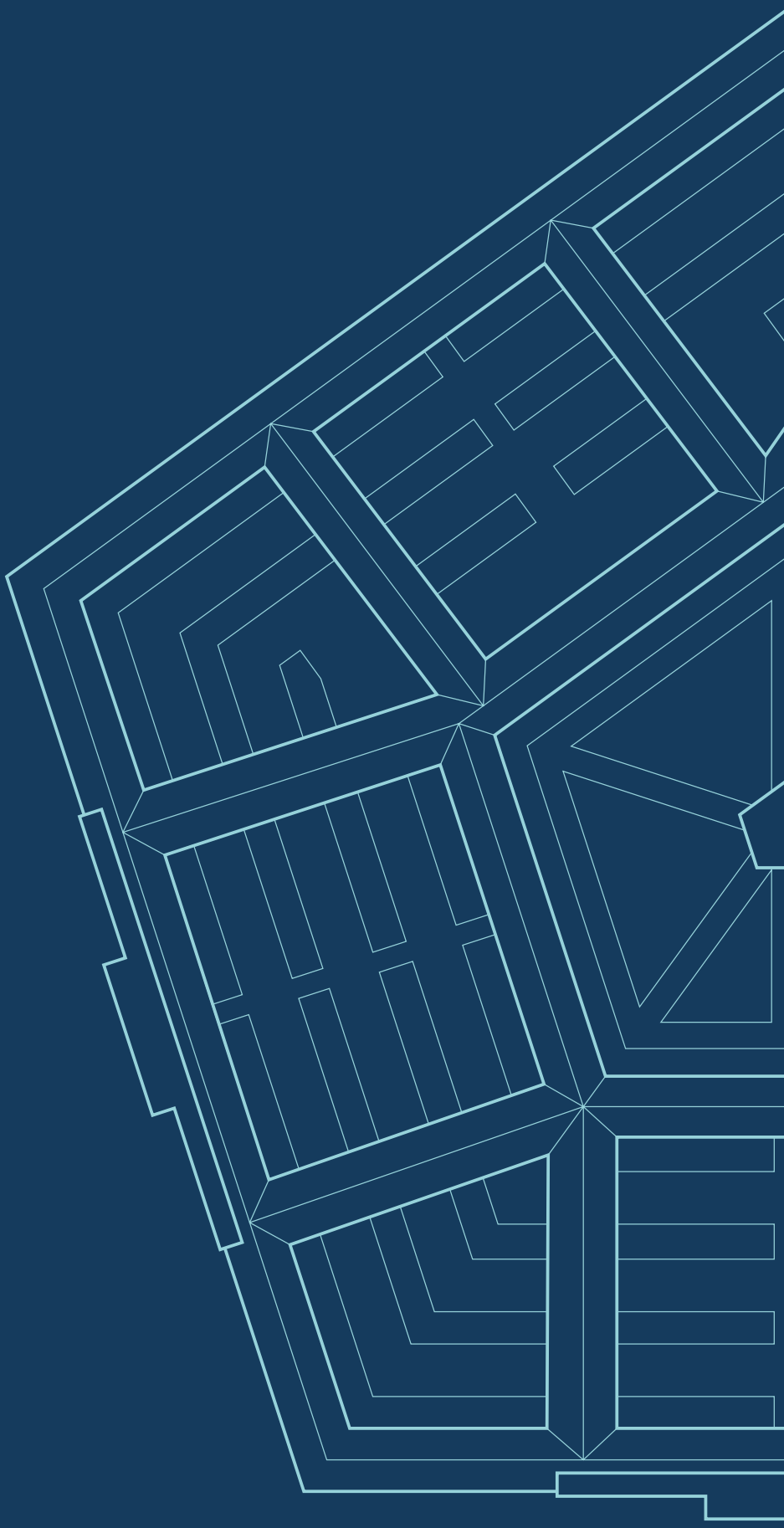
Another model is this: a Fake News clickbait item claims that a major celebrity has been arrested. It's a lie and their image has been used without image rights or US publicity or personality rights. The motive is simply to get clicks. In these instances the celebrities can sue and pursue the sites and the search engines to secure takedown and delisting.

A very new and genuinely disturbing technology is so-called Deepfake, in which video images are adapted to implant the heads and features of other people onto the bodies of participants in genuine videos. This opens a whole new order of threat. It started predictably in pornography but will no doubt quickly move into political misrepresentation, commercial malpractice and criminal blackmail.

The question that poses is: if the tech is soon to become available to create fake images of anyone and anything, how will this impact the public's perception of whether material is true or false? How does one make sense of the world, how does one derive a world view? Perversely this could have the effect of weakening the impact of all mass media and throwing people back onto their trusted personal networks for the formation of their opinions and principles.

Celebrities and their advisers will need to be acutely aware of this new threat, and primed to react fast if it happens.

"Where Fake News comes in is troubling. In the US we have seen a wave of false celebrity endorsements of products."



FROM THE ADOLESCENT BEDROOM TO THE CHIEFS OF STAFF: FAKE NEWS AND FUTURE WARFARE

Dr. Carl Miller
Research Director, Centre for the Analysis of Social Media, Demos

Strange beginnings

In 2003 a teenager called Chris Poole started an anonymous image board site named after a Japanese trend called 4chan. It was a remote, largely anonymous pocket of the Internet, and on it new feelings of identity and collectivity began to set its inhabitants apart from the mainstream. It grew quickly and soon millions of posts were flowing through the site, all of them impenetrable to anyone not steeped in the thickly woven layers of lore, slang, inter-board trolling, in-jokes and running feuds that each of the different boards on 4chan quickly developed.

This might be a strange place to start the story of Fake News, but it was on 4chan where the reality of Fake News today really started. For Fake News is not just people sharing incorrect things. It's the intentional creation and amplification of information with a grounding in human behaviour and psychology to change peoples' attitudes and beliefs. And it was 4chan who accidentally stumbled on it.

4chan saw companies, corporates, and 'normies' joining 'their' space in greater and greater numbers. They thought their internet was being invaded, and decided to launch a counter-invasion.

They began working out how to cause information to spread, how to grab attention, how to use the internet to influence the wider offline world. 4chan's boards began to fill with discussions of social engineering, psychological manipulation, and ideational diffusion, much of it taken from mainstream academic literature. They worked together, tested things, and began to find ways to use the internet to change what people saw and thought. They called it attention hacking, and used it for another invasion: using images of cats.

Attention hacking: proto-Fake News offensives

Part of 4chan's campaign of attention hacking was to use the internet to break into the mainstream media. They used an auto-voting programme that spread on 4chan to manipulate TIME magazine's online public poll to find the world's 100 most influential people. Chris Poole came first. They built fake social media accounts — 'sockpuppets' — to make certain hashtags trend and appear more popular than they were. They created fake websites that looked like the real thing, and manipulated search engine rankings to knock corporate websites off the front pages with their own jokes and forgeries.

Then there were the 'actions' where 4chan would swarm a target. In 2006, 4chan began a series of organised raids on the online game Habbo Hotel. Acting on rumours that moderators there were banning avatars based on their skin colour, they arrived en masse, blocking entrances and causing servers to crash. 4chan celebrated each victory with an endless deluge of shareable images ("memes") of cats.

4chan succeeded in what they set out to do. It wasn't really about cats; all of this was really about seizing and using attention and influence. Forgeries, spoofs, gaming, swarm-actions, manipulating search engines and memes were all part of a new body of techniques and skills that were forming. It was about finding ways of using the internet to become more influential, to change in controllable ways what people saw and even what they thought.

Cont...

The military get interested: UK, Russia, US

Others quickly began to copy and develop the techniques that 4chan pioneered. Political communications consultants brought attention hacking into political campaigns. Viral advertising agencies opened, and the murkier, more illicit side of online advertising sold search engine manipulation software to build bots and spam services.

Militaries can never stay out of questions of influence and they, like 4chan and advertisers before them, re-defined their professional art to put information at its heart. In 2014, a memo was sent across the British military entitled Warfare in the Information Age:

"The common theme" the memo states, "is that information-centric capability employed in information-centric operations can ameliorate many of the shortcomings of a reducing number of platforms and people." A new doctrine was developed, called Integrated Action. "Part of the whole purpose of Integrated Action is to change attitudes and behaviour in our favour".

In December 2014, the Security Council of the Russian Federation also published a new military doctrine. "The characteristic features and specifics of current military conflicts are…military force, information, political and economic measures" they concluded.

Or take AJP 3.10, NATO's Allied Joint Doctrine for Information Operations from November 2009. "The ever-increasing use of technologies such as the internet have resulted in a world where information plays an increasingly important role" it states. The doctrine explains that information operations should be used to target an enemy's 'will':

"For example, by questioning the legitimacy of leadership and cause, information activities may undermine their moral power base, separating leadership from supporters, political, military and public, thus weakening their desire to continue and affecting their actions."

State security and information warfare

Fake News is many things, of course, but as military after military redefined warfare, it became part of a concerted, systematic exploitation of the internet by militaries and state security bureaucracies around the world, facing outwards at foreign publics, and also at domestic populations.

- China employs two million people to write 448 million social media posts to 'distract the public, change the subject'.
- In Saudi Arabia, researchers have revealed thousands of 'fake' Twitter accounts generating hundreds to thousands of tweets per hour of "anti-Shia and anti-Iranian propaganda".
- In Mexico, an estimated 75,000 automated accounts are known locally as Peñabots, flood hashtags associated with corruption or political scandal.
- In the Philippines, salaried social media commentators mount a "fanatic defense of Duterte" and manipulate online polls.
- In Turkey, 6,000 'white trolls' have allegedly been enlisted to manipulate discussions, drive particular agendas, and counter government opponents on social media.

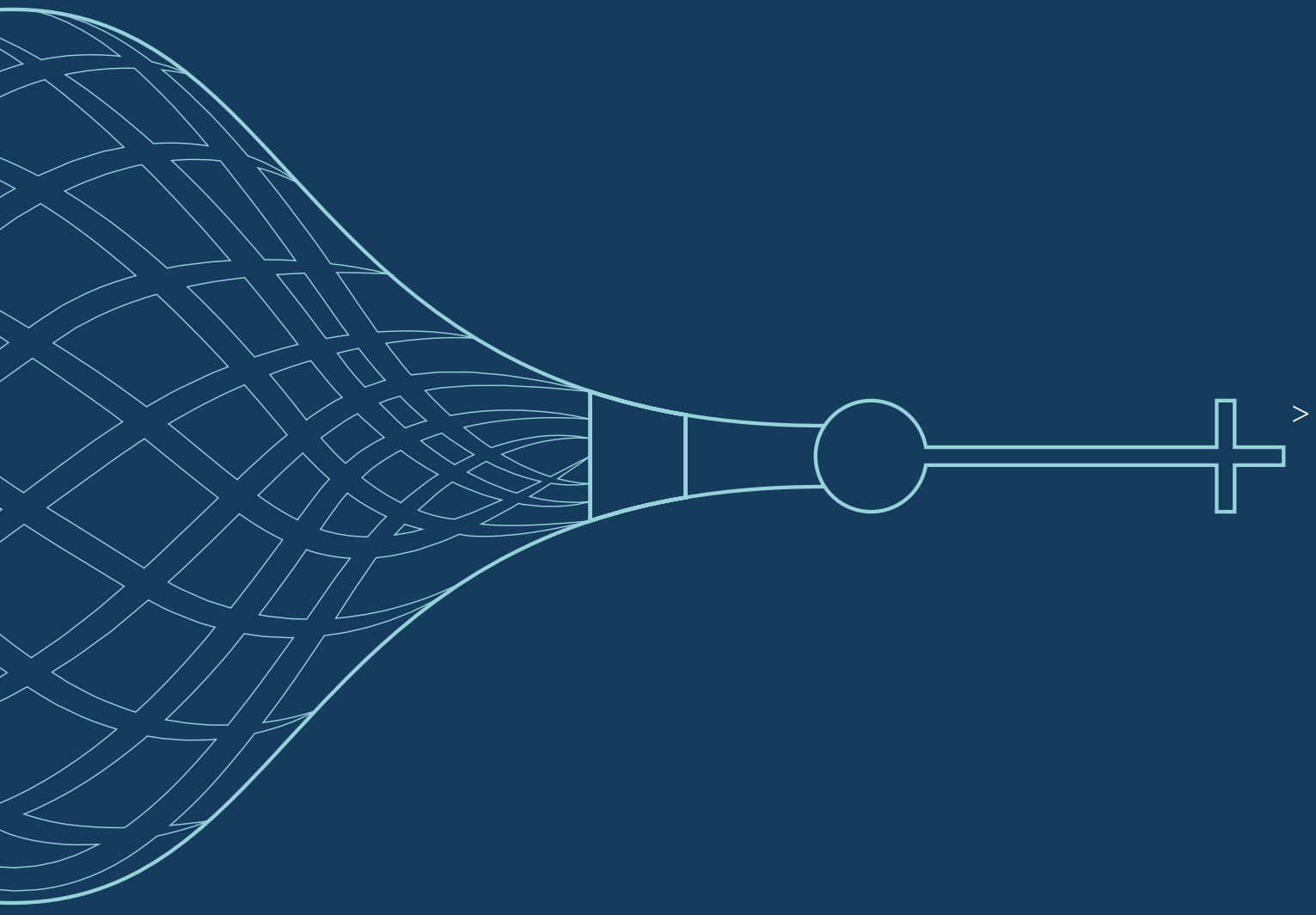
Freedom House assessed 65 countries for online 'manipulation tactics'. They found that 30 had evidence of paid pro-Government commentators, 20 showed evidence of political bots, 16 had seen deliberately misleading news pumped out during elections, and in 10 countries social media had been 'hijacked', forcibly taken over to spread information against the owners' wishes.

Your opinion is a military target

The concept of what a conflict or a military operation really is has widened: transferring outside the kinetic arena and into the battlefield of ideas, information, beliefs and opinions. Compared to a tank, or a missile, Fake News is trivially cheap and technically straightforward to do.

It is a new form of warfare that is not described in international law, and not bounded by international norms. It is also a form of control that inherently benefits authoritarian States more than liberal, democratic or rights-respecting ones.

An assault is being made on your beliefs. Your opinions are objectives, your news diet a strategic target. This is the reality of Fake News; a weapon in a new kind of warfare, redefined for the information age.



“

All warfare is bas

6th century BCE: Chinese military theorist Sun Tzu

sed on deception ”

Carter-Ruck

6 St Andrew Street, London EC4A 3AE. DX 333 Chancery Lane
OFFICE +44 (0)20 7353 5005 FAX +44 (0)20 7353 5553
EMAIL lawyers@carter-ruck.com www.carter-ruck.com