doi: 10.29843/JCCIS.202001_(39).0001

假訊息防制工作坊主題演講

運算宣傳：2019「假訊息防制工作坊」工作坊主題演講
Keynote Speech for the 2019 Workshop on "Fake News and Information Warfare"

Introduction by Professor Chen-Chao Tao

Department of Communication & Technology, National Chiao Tung University

My dear colleagues and friends, it is my honor to introduce Professor Phillip Howard. My first impression of Philip came from my colleagues who were responsible for contacting and inviting Philip. At that time I thought that Phillip was a very serious and busy man. It is very difficult for him to find time to accept an invitation. However, after we got in contact, my impression of him was dramatically changed. He is an energetic sunny man. The first question he asked was "Where can you get stinky tofu? I want to try it."

Thus, from this common example in our everyday life, you can see how communication using computer media could easily deliver misinformation and even unintentionally create a misunderstanding; that is the topic of Professor Howard's research.

He is currently the director of the Oxford Internet Institute. This is one of the most prestigious institutions and a pioneer in internet communication technology research. I think his level of academic success is also excellent. He already published 9 books and more than 140 articles. However, I think there are three reasons that make him stand out from other scholars.

First, he started the misinformation, fake news and information battle research field in 2012. Everybody remembers what happened in Taiwan in 2012. President Ma had just completed his first presidency and got re-elected in 2012. Professor Howard initiated computational propaganda research far before the current time.

I think the term computational propaganda perfectly reflects the nature and the specific feature of the information battle in current networks. This is because propaganda is a very old issue, and so we can connect it to the field of literature from a long time ago. However, the effects of computational methods are evident. Currently, because of social media, algorithms, artificial intelligence, and the speed and size of propaganda are totally different in new ways.

Second, regarding his research, I read his books and his papers. His results show the vulnerability of the algorithms used in big companies such as Facebook or Google. Their algorithms are easily influenced and attacked, even by common people. Therefore, people can manipulate search results, including what is shown on Facebook, to manipulate public opinion. I think the most serious issue is the malicious impact of social media, artificial intelligence and algorithms since specific groups can use this kind of technique to manipulate public opinion to benefit a specific group.

Currently, we know that everyone should install antivirus software on their own computers or laptops; however, big companies such as Facebook, Line, and Google behave as though they do not even know that they have to prepare some software to protect their algorithms. Thus, their algorithms are easily influenced by any person.

The last reason is that Professor Howard is not only a scholar but he is also an advocator to build a worldwide network consisting of policy-maker and journalists to fight against fake news together. He seeks to alert others about the seriousness of the influence of social media, and initiates many civil engagement programs to let citizens know that we should pay more attention to illegal information. Please join me in welcoming Professor Phillip Howard.

Lecture by Professor Phillip Howard

Director of the Oxford Internet Institution

Good morning. Thank you very much, Professors Tao and Minister Lo, for having me today to present some research on the trends we've noticed in computational propaganda, and hopefully answer a few questions regarding the direction of global politics.

I'm going to start with an outline: what the research says about misinformation and its role in public life. I want to convince you over the 35 minutes that this is a social problem in which research is extremely important.

"Social research" is one of the reasons we know about these problems, and I would argue it will be the source of the solutions. What am I going to do today? I do not do science fiction or predictions as a social scientist; I want to work with evidence. So Im going to talk about some of the evidence we've been collecting from other parts of the world about how misinformation works and what type of impact it has.

The Oxford Internet Institute, of which I am a part, is a medium-sized faculty that started about 15 years ago for conducting several different things. Our mission within the computational propaganda lab is to solve public problems and increase civic engagement through social data science. I'll give you some examples of what that looks like as we go ahead.

We're approximately one-third computer scientists, one-third social scientists, and one-third humanists. This is an unusual configuration for a department; our computer scientists have to learn social theory, and social scientists have to learn to code or appreciate the craft of code. One of the reasons this type of multidisciplinary department is important is because so many of our contemporary social problems require a multidisciplinary perspective.

These are just some of our colleagues: my colleague Victor Mayer Schoenberg is famous for the phrase Big Data. He wrote the book Big Data, and he's the reason policymakers around the world used this phrase. Several scholars are studying artificial intelligence, the ethics of AI, and its application in our public lives.

So much of what we experience in contemporary politics now is driven by information technology; I would argue that multidisciplinary research must be part of the solution set and must be part of our future.

The research I'm going to speak of today has been supported by the National Science Foundation in the United States and the European Research Council in Europe. Public science agencies supported the scientific questions, and the Open Society Foundations on Media Freedom supported the public engagement. Sometimes these are separate projects in which public science agencies support the science, and we must go elsewhere for supporting public engagement. So these are the funders that support our work, which I'll tell you about now.

Since 2016, we've seen a variety of ways in which misinformation has been presented on social media. I'm going to describe how we collect our evidence in our process. Next, I'm going to talk about the evidence we found concerning Russian intervention in the U.S. election in 2016. Then, I'll offer some examples of what I think this might mean for contemporary politics. I'm still learning about politics in this region. But I can share what we've learned from other parts of the world. Let me start with a taste of how we collect our evidence.

All of you who are using social media will have some form of automation following you. Forgive me, but especially journalists and politicians will have "bots," or automated accounts that lock onto your account, generate content, and send it to you.

My particular team studies Twitter for the most part, and we've moved onto other platforms; I'll explain why, but our earliest research was on Twitter. This is an example of the kind of account that we study. I'm sure you've seen accounts like this; they're easy to identify by hand with a manual heuristic because they have a crazy number of followers compared with the number of accounts that they follow.

They generate thousands more messages than any human would naturally generate. Some of the accounts that we follow in English will not talk about politics for years. They'll talk about soap operas, soccer scores, and football scores, and then suddenly move into the

area of "politics."

In this particular account, the bear might give it away, but this is an account that was monitored and generated by the Russians to target misinformation at the United States in English. Some of the accounts that we have caught make mistakes. They tweet in Cyrillic in a Russian character set and then go back to work in English. This makes it easy for us to catch them. Others like this one are very subtle until they wake up one day and become very passionate about politics.

When we start a fresh scoop of data, we often start with President Trump's follower list. I don't mean this as a political joke or political insult; I mean simply that his Twitter account has many bots following it. These are accounts you've seen with no pictures and perhaps a series of numbers for names. They generate no information until the moment that they're needed. We will take a scoop of such data and look for patterns in how it is used and how these accounts are activated.

Now, automation by itself in social media is not so much of a problem. It's not the code that is the issue. The challenge is when these automated accounts are used to push "fake news," or what I would prefer to call "junk news," in large amounts to a population.

In this particular case, content from Russia Today, one of the sources of political misinformation about Islam, is about Muslim women in hijab ruining the Spanish beach vacation. It turns out that this is a doctored image, and this did not happen at all; immigrants breaking through the passport control in Morocco also did not happen in this way. These are forms of misinformation we called "junk news," whereas it turns out in English the term most used by journalists is "fake news."

It turns out that it's very difficult to operationalize as a social scientist. It's very difficult to look at a piece of news and know how much fact-checking went into the article or how much editorial oversight there was; we can't tell this as independent researchers. The best we can do is evaluate the organization behind the news production. We prefer the term "junk news" to refer to organizations that produce sensational, extremist, or conspiratorial content.

Sometimes they produce content that is commentary like what we would think of as

an op-ed (opposite the editorial page) or a commentary essay. But they use the colors of a professional news outlet or they use the presentation of a professional news outlet. The public may not always know the difference between a "commentary essay" and something that is actually "news."

So, our goal in conducting the research is to try to identify the networks of accounts: sometimes automated, sometimes fake. We need to figure out what messages they're trying to propel into the public and then see if we can make an attribution as to who is behind the misinformation.

We've conducted multiple studies over the last few years. I'll talk a little bit more about how these studies reveal a global trend later, but for the most part, every region is covered in some way. We have attempted most recently to focus on Tunisia and Egypt in Africa. We also have case studies coming from Latin America and Southeast Asia. This is now a global problem, rather than a problem for a particular neighborhood or a particular region.

One of the things I want to emphasize as I mentioned earlier is that this is a problem that has been exposed by social science, and the appropriate solutions will be found through research.

We have conducted multimethod research because when you simply conduct a large quantitative study by itself, it can be very difficult to find the punchline. Understanding the importance of the evidence is what we call "Big Data." Unless it is matched with qualitative data; it's often the qualitative or the ethnographic that really helps us to interpret the impact.

For example, one of my team members has returned after spending time with a company in Poland that sells access to 40,000 fake Facebook user accounts, which are rented 10,000 at a time to customers who will ask for he messaging. Their number one clients are not politicians. It's not the government that pays to rent these firms or rent these fake accounts.

Which industry do you think would pay to rent tens of thousands of fake Facebook users at a time? Which industry would you say?

Some good guesses; it's not entertainment, although some of the best of these accounts have been designed for Hollywood stars. It is actually pharmaceuticals. The pharmaceutical

industry rent 10,000 fake Facebook accounts to post that they have a migraine or a headache and then 10,000 more to share a new medicine for managing the migraines. They gain public interaction, and this is how they advertise their goods on social networks.

It's the same messaging and structure for political content; fake accounts that generate normal content with friends and family and then suddenly start talking about politics.

Being able to match the fieldwork with this kind of lab work with a large-scale computational study over multiple platforms and to do this internationally—it's what makes it possible to identify general trends in misinformation.

About a year ago, Facebook provided to the U.S. Congress a data set of three and a half thousand known fake accounts that were managed from St. Petersburg in Russia and active during the U.S. election. They gave us access to the accounts to understand what these accounts were designed to accomplish. So I can use this evidence and share a little bit about how these accounts were used to communicate in this particular context. I'll offer three figures with data about how these accounts were used for misinformation.

The first point is fairly straightforward. This follows the rhythm of the political year and the activity of the Facebook accounts. The point of this figure is simply to show that the fake political accounts burst into activity whenever there's an important political event. For example, Trump gets the nomination; Clinton and Trump engage in the debates; the Russian activity spikes up and down. The activity of these fake accounts flows in parallel with major events in politics.

The second point of this figure is that while a significant amount of activity occurred through 2016 into the election, the bulk of Russian activity actually came after the election. We spend time worrying about 2016, what might have happened, but it's almost as if the Russians decided that maybe their efforts had been successful. Afterwards, they employed many more people and resources for generating interaction between the fake accounts on politics in the United States.

The third point of this figure is that the accounts started well before we thought they did. In fact, some of them go back quite early to 2012. Almost as long as social media has existed

and as it has evolved, there has been some political figure experimenting with how to use it for manipulation. So, the rhythm of fake accounts mirrors the rhythm of politics. The activity has increased over time, and the origins stem from the very beginnings of social media.

The data they provided covered multiple platforms and not just Facebook. Facebook provided information about ads and organic content. There was also information from Instagram, Twitter, and YouTube. Google provided some information on search but in PDF format. They must have thought we would be printing the data. However, we could not analyze the PDFs. I think this must have been a deliberate choice of the company to not collaborate and not cooperate with the government because this data doesn't exist in PDF format naturally.

The information I share today does not apply to the data from Google and reveals things similar to the previous figure. The bulk of activity started in 2016, but most of the activity came after 2016. I'm going to draw your attention to two lines in particular. First, I'll start with the lower line. This is the rhythm of Facebook ads placed by the fake accounts. I offer this one to illustrate that, overall, the impact I think of Facebook political ads is relatively minor. It's not political ads that tend to capture the imagination and have an impact on voters. It's the organic content; it's the interaction. When you think you see some friends having a natural interaction, it can be very difficult to tell that such political engagement is paid for or sponsored. That is the kind of interaction that we have commonly seen.

The second line is the flow of content over Instagram. I offer this because we spend most of the time in the United States, Europe, and the UK speaking about Twitter and Facebook. But more recently, Russian activity has moved on to Instagram, and we have no data about Instagram. Twitter and Facebook at least have a flow of data that independent researchers can play with. Instagram does not provide this.

Instagram is where the younger users are, and I love my colleagues but none of us use Instagram successfully. So there is definitely an age difference. This is to say nothing about Tik-Tok (抖音). We don't know what goes on with misinformation on Tik-Tok. And few researchers study Line. We know there are multiple other platforms, but for the most part,

Instagram is a closed platform for us.

Finally, we can say something about the topics—the kinds of information that were proposed by these fake accounts to try to shape public opinion. As you would guess, these are topics designed to polarize the public to create divisions. To divide public opinion along the lines of disagreement that they already were aware existed.

An important part of the misinformation around the U.S. 2016 election was targeted to discourage voters. Therefore, messages such as the following were circulated: “If you have certain political values or aims, don't vote at all,” “Make a protest by boycotting the election,” “Don't vote,” or “Maybe voting has moved; it's not on Tuesday, it’s now on Friday.” But this was untrue. Some others such as “You don't need to bring an ID” or “You can vote by making a telephone call; you don't need to come.” This was targeted at particular voters for one side or the other. In many cases in the United States, the information was targeted at the far right, the ultra-conservative or extreme conservative and at African-Americans, indicating a race-based appeal.

Some of the misinformation we know was also directed at Latinos. In the United States, gun control, abortion, and how to react to school shootings are polarizing issues, and the Russians knew how to exacerbate the tension.

Let me talk now about how this is a global problem and why this is relevant in countries around the world. Over time, we have studied several different kinds of regimes, including authoritarian regimes and democracies. My research started when I was living in Budapest. In the summer of 2014, the Malaysian Airlines flight was shot down over Ukraine. I watched as my Hungarian friends received multiple kinds of misinformation. They read stories that claimed that Americans had shot this plane down because they thought Putin was on the plane. There was another story that local democracy advocates in Ukraine had shot the plane down. There was a third story of a lost tank from World War II that had been stuck in the jungles, came out confused, and shot the plane down.

That’s when we found the goal of misinformation was not to mislead everybody with one story but to mislead everybody with multiple conflicting stories, some of which were

ridiculous or made no sense. But if you give every section of the room a different story, there's no consensus on how to respond; there's nothing to organize around collectively, and it's much harder to share grievances or even share a sense of how to solve a public problem.

Now, over time, we've actually seen more and more countries with organized misinformation campaigns. Our very first inventory in 2017 counted 28 countries with organized misinformation campaigns. These were not just authoritarian regimes but also democracies. In authoritarian regimes, it's often a military unit that is assigned to conduct social media manipulation. Sometimes teams are simply paid as in the case of Mainland China where large numbers of people are paid to generate misinformation. In democracies, it is often the political parties that pay communications consultants to conduct misinformation campaigns, especially around election time.

The number of countries doing this work increased from 28 in 2017 to 48 in 2018. In 2019, 70 countries around the world showed evidence of organized misinformation campaigns, and these are not lone hackers or students operating out of a basement. These are teams with job ads and secretaries, performance bonuses, and an organizational structure. They are formal organizations in the sociological sense. They get paid different amounts in different parts of the world, but they're pervasive.

Another thing we observed this year is that there are more and more countries with organized misinformation campaigns targeting other countries. So, at first, most of the organized misinformation campaigns were directed at a country's own voters or citizens. This year we counted seven—Iran, India, Pakistan, Russia, Saudi Arabia, Venezuela, and China—with known teams targeting public opinion outside their borders. Usually, these teams organized in multiple platforms over multiple languages and had highly professionalized bureaucracies.

We also noted for the first time that "learning" countries send their representatives to study how to conduct misinformation to countries that were good at it. These educational teams engaged just like our workshop today. They have workshops too, and this is how the tricks spread and evolved.

I could say quite a few things about what these organizations do and how they work. 87% of the countries used humans to populate their accounts with content. 80%, or four out of five, used automated accounts or fake accounts with code that push out content. Sometimes the code is sophisticated. It doesn't generate content when we sleep, and then it wakes up. Sometimes it's not sophisticated. It sends a message every second for the course of weeks.

7% of the countries used hacked or stolen accounts of some kind or other. All of this is based on media reports and investigative journalism from within a country or particular academic reports that we know of. 75% of the countries used deliberate disinformation and media strategies to manipulate voters along with clear messaging. Sometimes this involved a connection between a national broadcaster and a communications consultant.

73% of the strategies involved amplifying messages by colonizing a hashtag. Sometimes the topic had nothing to do with politics but you can targeted it significantly with the keyword used in the misinformation.

In 71% of the countries we studied, pro-government or pro-party propaganda in structured campaigns advanced one particular party in about a third of the campaigns. The messages were designed to create divisions in society, particularly on issues related to gender, race, or the role of women in politics and public life.

We've noticed across many of the reports that we've studied, prominent feminist intellectuals and female politicians and journalists are particular targets for misinformation, and unfortunately, such strategies have often been successful at pushing women out of public life.

Let me get to the question about how to measure the impact of these things. I think there are several qualitative observations that I would make, and gender is one: so much misinformation targets female public intellectuals and personalities unfairly.

Further, let me talk briefly about what I think the trends ahead are. I will try to stick close to the evidence and the things that we know now. In the next few years, I think it's safe to say that every budget bill, every tax issue, every complex humanitarian disaster, every

hurricane, every political issue, every school shooting will have some kind of automated campaign for and against it, or blaming a particular party or community, or using some political spin. Every major national issue will have some kind of automated campaign around it.

For the last few years, our research has been mostly about Russia. Our original research grant was to study how Russia and Mainland China target voters in democracies when they vote. We had only caught the Russians at this activity.

In the last few months, China has emerged as a superpower in misinformation. Our historical study revealed that the Chinese government attacked the Taiwanese president a few years ago on social media. We know that they go after Tibetans in exile, and much of the automation is on issues that are important to Mainland China. But until very recently, they hadn't been interested in public opinion overseas.

Recently, with protests in Hong Kong, we found China operating in multiple platforms: Twitter, Facebook, Instagram, YouTube, and many other smaller platforms. They operate in multiple languages and are keenly interested in global opinions about the situation in Hong Kong.

So now, there are at least two world superpowers in misinformation: Russia and China. And then there are other regimes that are learning to adopt these approaches and to develop their own agencies with their own government budgets to conduct similar work in their own spheres of influence on the issues that they care about. So it's not just about the world superpowers.

Many of us have seen the activity of misinformation during elections. In the next few years, I expect we'll start to see misinformation campaigns between elections on special issues. Whenever a lobbyist wants to get relief from the legislature, have a tax bill passed, or get special consideration, these kinds of techniques and tricks will be used to get what they need out of politics. We'll see more and more special issue campaigns.

I don't believe that we've seen true artificial intelligence yet on the misinformation

programs. But I do think this is coming. If someone can retrieve the data from your credit card and the content from your social media feed and figure out what face, what voice, what words, and what rhetoric you'll respond to, they'll be able to compose a tailored message that will be directed at you.

Artificial intelligence may make it possible to send each person in this room a different political message from politicians, meaning we can't have faith that we all see the same content or that a political figure says the same thing to each person.

This is not in the United Kingdom votes in December, you vote in January. This is not for now but for down the road.

Then, my final observation is that much of this misinformation is a deep threat to democracy itself. There are many definitions of what democracy is and how it works. My favorite is the very simple one: democracy is when we choose the choosers. We choose the people who make good decisions for us. Ideally, we only do this every few years: we make a choice, they go to work, they don't bother us, they make good decisions that use evidence when they make their decisions, and then they come back to us for a vote.

This process of misinformation undermines the role of science by getting us to go along with politicians who follow their gut, who do the critical thinking and question the experts, but don't always believe in evidence when making their policies. I think there are a number of countries that now show when this type of politician, who does not rely on evidence, is elected, they make poor decisions, exacerbate problems, and create a cycle of degradation. Taking expertise out of public life results in poor policy decisions. This is about undermining the public's confidence in the role of science. In solving social problems, that is important and worth preserving and the longest-term existential threat to the future of democracy.

Let me say something about how academics will save the world. Universities genuinely do have a role to play, providing a neutral platform for producing research and conducting investigative work along with professional journalists. It's part of our function to ask the tough questions, demand truths, and argue that the truth has value. My view is that certain

policy changes will strengthen our democracy, and I have several ideas I can share with you now.

One of the challenges in public life is that the best data about public problems is held by Silicon Valley. The best information about our behavior, our aspirations, and our attitudes is not held in the National Library or by the nation's hospital systems, but is held in San Francisco. So an important part of these ideas involves loosening that grasp so that independent investigators, hospitals, social scientists, and libraries have access to the data if required for studying these social problems.

Let me start with the first example: the idea of reporting the ultimate beneficiary. I think we should be able to look at any particular device that we have and ask it to tell us who is benefiting from our data—which organization, which politician, which government.

Our basic devices now can't do that. We know that the data is collected, is shared in many different kinds of infrastructure, and ends up in data mining firms. It's bought and sold by other people. Some countries have rules to try to prevent this, but on the whole, the rules are rarely effective. We should be able to hold each device accountable because it is keeping track of us.

Then, we should be able to donate our data. If I want to give my data to my favorite political party, my favorite social scientists, my favorite hospital, I should be able to. This is a mode of civic expression in today's world. Our infrastructure should tithe. This is a very old concept. If we're generating immense amounts of data and sending it to Silicon Valley, some portion of it should come to the national libraries. In each country, if we're able to get large grants and ethically conduct research on our human subjects, then we've already passed more ethics rules than any of the Facebook data scientists have ever passed. We should be allowed to examine this data for the public good.

It's also important to be able to look under the hood of the social media sites to understand what the algorithms do and understand how they distribute content. At a very basic level, every ad placed on a social media platform should be archived for later analysis. I would also say that when political parties purchase ads, a searchable archive should be

available to the public, journalists, and academic researchers.

Now I offer this is as a last joke: mostly as a way of declaring a faith that this is worthwhile work. “I’m sorry Jeanne your answer was correct but Kevin shouted his incorrect answer over yours, so he gets the points.”

This can be depressing work, and I hope I haven’t suppressed your enthusiasm for democracy too much. I do think that the value here in exposing truths, preserving them, detecting them, and making sure that political leaders hear them itself is intrinsically worthwhile.

We can produce functioning democracies again. Social media is here to stay. The best thing we can do is ensure that it respects our democratic values and helps us all make good decisions on Election Day.

Thank you very much for your time.