Event Report

Workshop on DRUMS
(Distortions Rumours Untruths Misinformation Smears)

24 – 25 July 2017

Report on the Workshop organised by:
Centre of Excellence for National Security (CENS)
S. Rajaratnam School of International Studies (RSIS)
Nanyang Technological University, Singapore
Supported by:
National Security Coordination Secretariat (NSCS)
Prime Minister's Office, Singapore
Rapporteurs:
Muhammad Faizal bin Abdul Rahman, Juhi Ahuja, Nur Diyanah binte Anwar, Joseph Franco, Cameron Sumpter, Dymples Leong Suying, Pravin Prakash, Romain Brian Quivooij, Tan E Guang Eugene, and Jennifer Yang Hui
Editor:
Benjamin Ang

The Workshop adheres to a variation of the Chatham House Rule. Accordingly, beyond the speakers and the presenters cited, no other attributions have been included in this report.

TABLE OF CONTENTS

Executive Summary

The Centre of Excellence for National Security (CENS) organised a workshop on 24 and 25 July 2017 titled “Distortions, Rumours, Untruths, Misinformation and Smears (DRUMS)”, which refers to information operations and the phenomena known as “fake news”. The workshop explored new and existing methods in countering DRUMS in the online and real worlds, assessed the methods available to counter DRUMS from a multi-disciplinary perspective, and studied how states around the world were coping with the proliferation of DRUMS.

The 18 speakers included academics, practitioners, and private sector experts from the United States, United Kingdom, France, Germany, Latvia, the Czech Republic, Hong Kong, Norway, Ukraine, and Singapore. They spoke from the perspectives of anthropology, psychology, journalism, counter-terrorism, technology, hybrid warfare, computational propaganda, education, and national security.

More than 100 participants from government agencies attended the two-day workshop and participated actively in the syndicate discussions with the speakers.

The key findings from the workshop were as follows:

DRUMS is a national security issue

States are turning to hybrid warfare, instead of conventional conflict, to achieve their political goals. DRUMS has been used as part of psychological warfare or hybrid warfare in the Middle East and in Eastern Europe. Russia uses a well-planned campaign of disinformation against NATO, and to support Russian objectives in Crimea. This hybrid warfare is designed to exploit national vulnerabilities, in order to subvert the political system, destabilize the society, or to influence public perception in the target state.

When automated/semi-automated social media accounts are used to publish and spread disinformation very rapidly, especially during sensitive times like election campaigns, this can cause public confusion. In some states, citizens may become more willing to exit society.

DRUMS is a multi-faceted problem

DRUMS is attractive to human psychology, because of a natural tendency to believe negative news, especially among certain groups. Conspiracy theories proliferate because they appeal to our need to perceive patterns even where are none. Herding bias leads us to prefer popular news items, even if inaccurate, over less popular news.

DRUMS can be propagated by state-owned or state-sponsored media, political parties, agents, NGOs, activists, biased “experts”, or websites that spread disinformation for financial gain. The distribution of DRUMS is amplified by social media, where algorithms are used to target readers with information that best suits their biases, and automated / semi-automated social media accounts are used to create the illusion that the news is widely accepted, or to flood out and silence other conversations.

DRUMS requires a multi-prong response

Education can create greater awareness in the population, and to develop critical thinking, digital literacy, and information navigation skills.

Fact checking organisations, publishers, technology platforms, and media companies, can help to verify the authenticity of information.

In some cases, content analysis tools can be used to trace where some pieces of DRUMS have originated from, to identify where they have travelled, and to map the network topology. While this information is useful for analysis, there is no simple technological solution for DRUMS

A society's level of resilience to DRUMS can be improved by greater communication between governments and citizens, winning hearts and minds, enhancing critical thinking, and communicating in ways that do not involve media.

Legislation can give persons affected by DRUMS the right to answer. It can also hold technology platforms and persons accountable for their role in the distribution of disinformation. The responses should be calibrated to the sensitivity of the DRUMS. Heavy levels of censorship can be ineffective in stifling public interest in a topic, and may instead have a multiplier effect by attracting a greater volume of discussion.

Response to DRUMS requires whole-of-society cooperation

States need to keep citizens engaged with national objectives, and to build trust. When citizens lose trust in authorities, they seek alternative sources of information, and conspiracy theories flourish.

States and social media platforms need to cooperate to find feasible solutions to DRUMS, including creating greater user awareness, and developing tools to stop the spread of DRUMS. Social media platforms need to take responsibility for their role in DRUMS.

Media companies and NGOs need to provide independent fact-checking services to verify the authenticity of information.

Framing National strategies to counter DRUMS

NATO member states have developed counter-measures including strategic communications, exercise scenarios, and coordination with other organisations. Norway has developed its "total defence concept" of support and cooperation between armed forces and civil society. Governments need to develop long term strategies to respond to the problem of DRUMS, and to review these regimes regularly to future-proof them.

Panel One: Why People Believe DRUMS

Believing Chicken Little: Political Orientation Predicts Negatively-Biased Credulity in Americans

Daniel Fessler, Department of Anthropology and Center for Behavior, Evolution and Culture, UCLA

Research has shown that negative false information (concerning hazards) has more credulity (is more believable), and will therefore spread faster, endure longer, and have greater impact, than positive false information (concerning benefits). The study shows that the likelihood that negative false information will be believed also varies with the political orientation of the audience.

- During Halloween in the United States, parents do not allow their children to take unwrapped candy or fruit from people while trick-or-treating as they believe malicious actors may adulterate food to harm or kill children. There has never been a recorded case of this happening, but parents almost universally believe it to be true.

- Human brains are equipped with a set of tools for the acquisition, retention and transmission of practical knowledge and effective technology passed down through generations. However, functional characteristics of cultural information are often opaque or completely unknown to learners, so people need to be credulous (trusting) if they are to take advantage of the cultural knowledge to solve problems.

- Too much credulity leads to sincerely held but false beliefs and/or manipulation by malicious actors. Learners must therefore weigh the costs and benefits of credulity with each piece of potentially helpful information. Cultural acquisition devices have developed biases to create the least costly error.

- For example, failure of a smoke detector may be annoying when it is triggered by burnt toast (false positive) but it will be fatal if it fails to activate when a fire breaks out while you are sleeping (false negative). This is the asymmetry in the costs of false positives and false negatives when it comes to hazard information. Therefore, humans have evolved systems that are biased towards greater credulity when messages concern hazards, relative to those concerning benefits.

- People are more likely to believe information when it is presented as potentially harmful. Moreover, if people generally believe the world to be dangerous, they are more likely to believe in the existence of newly discovered dangers, which becomes a self-perpetuating cycle.

- The more conservative a person is, the more they show a bias towards evaluating statements about hazards as more believable than statements about benefits. A recent study of psychological characteristics of conservatives and liberals in the United States indicated that liberals tend to value the opportunities afforded by change and cultural heterogeneity, while conservatives value the safety of tradition and maintaining the status quo. Researchers hypothesised that political conservativism is more consonant with an elevated negatively biased credulity than political liberalism. Questions involving the same information (but framed as either a

hazard or a benefit) were presented to people from the two political perspectives and the hypothesis was confirmed.

- The liberal-conservative spectrum breaks down into three constituent parts: social conservatism (e.g. opposing abortion/same-sex marriage); military conservativism (positively assessing the value of force for resolving both personal and international conflicts); and fiscal conservativism (favouring lower tax rates over social welfare programmes). Further research revealed that only social conservativism predicts negatively biased credulity.

Suspicious Minds: The psychology of Conspiracy Theories
Rob Brotherton, Barnard College, Columbia University

Human beings create conspiracy theories because of innate psychological biases and cognitive shortcuts, such as the tendency to attribute intention to ambiguous events, assumptions that significant events require grand explanations, and the human propensity to perceive patterns in the world around us, even when they do not exist.

- Human beings are susceptible to psychological biases; our brains take shortcuts and our beliefs are influenced by heuristics without us necessarily realising it. Three psychological biases may be particularly involved in the likelihood of an individual believing in conspiracy theories: the intentionality bias, the proportionality bias, and our ability to recognise patterns in the world.

- An early experiment from 1944 showed people a rudimentary animation of shapes moving randomly around a screen and asked them to describe what they saw. Most participants outlined a narrative, perceiving the geometric shapes to be acting out human characteristics, motivations and desires. The study illustrated that our minds are finely tuned to understand and interpret what we see as human-like intentions; we are biased to see intentions rather than accidents or coincidences.

- A more recent study, using the same moving shapes, found a correlation between participants' perceptions of intention and human qualities in them, and a tendency to seek out and believe in conspiracy theories.

- The proportionality bias (or magnitude-matching principle) explains the tendency to assume that significant events must have significant causes, and conversely, insignificant events have insignificant causes. For example, a TWA plane crash near New York in 1996 killed all 230 passengers on board which produced grand explanations and conspiracy theories, but when US Airways flight 1549 successfully crash landed on the Hudson River in 2009 with no casualties, observers were satisfied with the explanation that the plane's engines collided with a flock of birds.

- Another example of the proportionality bias is the assassination of US President John F Kennedy, which generated several enduring conspiracy theories, while the non-fatal shooting of President Ronald Reagan in 1981 produced none.

- A third psychological quirk is the human ability to perceive patterns in the world, even when confronted with ambiguous images. Research has shown that people are more

likely to see a meaningful pattern in meaningless visual noise when they are manipulated to think they lack a sense of control. In the same manner, conspiracy theories can be considered cognitive illusions whereby people feel inclined to connect the dots between ambiguous points of information.

- Conspiracy theories are not all about grandiose plots but have their roots in fundamental aspects of human psychology – our tendency to find patterns, seek meaning and subconsciously embrace biases in systematic ways.

Fake news: A danger for Democracy or a Gift from Freedom of Speech?
Nicolas Arpagian, Academic Director of the Cyber Security Program at the National Institute for Security & Judicial Studies, France

The most effective approach to addressing the problem of fake news is not limiting the freedom to publish or broadcast information, but developing society's capacity to critique and evaluate the conveyor and content of the message, and providing the public with tools to do so.

- The concept of 'fake news' is not unique to contemporary communications; humans have always attempted to bend truth, manipulate others and modify reality. In 1881, the French Third Republic passed a Law on the Freedom of the Press which guaranteed the right to publish information with due regard to certain responsibilities, principally concerning libel and defamation. Once information deemed fake is published, opponents may challenge its veracity in court based on this legislation.

- Two days before the 2017 French Presidential election, an announcement was made on the 4chan forum (a popular destination for internet pranksters and hackers) by someone claiming to possess several million documents regarding Emmanuel Macron, including damaging information, bank account details and private messages between Macron's campaign team members. WikiLeaks announced that the documents contained controversial details, and many newly created Twitter accounts in the United States began tweeting vaguely about the supposedly damaging information without offering details.

- The pre-election freeze on media during the weekend of the vote mitigated the effect of the disinformation campaign. However, more fake news arose when the newly elected President Macron and his wife hosted Donald and Melania Trump for dinner at the Eiffel Tower in July and a doctored image emerged purporting that the bill had been over €150,000. Again, Twitter accounts were specifically created in attempts to magnify the false story.

- With the rising tide of disinformation, the traditional media in France sought to expose fraudulent stories through the creation of a website called Décodex, where users could enter a URL and find out the accuracy of a given news item. However, the initiative received criticism for ostensibly claiming to be an authority on truth.

- The project CrossCheck, financed by Google, has brought together a range of different publishing organisations to collectively verify the authenticity of information collectively, as a peer review system for the media. This type of strategy may be used increasingly in the future.

- The French Government has also combatted disinformation through counter radicalisation campaigns, which are aimed at thwarting the narratives coming from extremist organisations. There has been scepticism that individuals willing to take their own lives would be swayed by a government website, but it is still considered a useful resource for those who may be having doubts about involvement.

- To combat fake news, it is more effective to promote critical thought among audiences and the verification of information, than to limit freedom of press or the capacity to publish or broadcast information.

Syndicate Discussions

- **Issue: Social networks may amplify level of fear** – Online and offline social networks may amplify the level of fear in society. It does not matter if these networks consist of close or weak ties, or if the information has been verified to be true. Negative news gets spread three times faster in these networks than positive ones, which would usually lead to an escalation of fear.

- **Issue: Ethical issues in setting the algorithms used by social media platforms** – Social media platforms such as Facebook now utilise algorithms which can identify an individual's interests, and target him / her for advertisements or articles which he / she may find interesting. These algorithms should be used responsibly, as they can be manipulated for undesirable objectives as well.

- **Issue: Legislative enhancements to manage the spread of fake news** – In France, individuals can raise issues or cases of fake news, using the Press Law of 1881. This law delineates the limits to the freedoms and responsibilities of the press, and applies to content posted on online media platforms. For example, if there were incorrect news published in a newspaper or on a website, individuals can publish letters addressed to the editor of that media platform to allow the "right to answer". However, if the fake news continues to be published, then the individual has the "right to respond" in court.

- **Issue: Opinion can become news when it is published** – The implications of personal opinion becoming news or fake news depends on who has said it and in what context. Anyone can publish on social media as individuals representing themselves. This data is stored on the web for long periods of time. Hence, something published a long time ago can be attributed to an individual years later – which can sometimes be damaging to reputation, especially if the individual is a public figure.

- **Issue: Disruptions caused by disinformation and foreign influence/interventions during electoral campaigns** – Before the advent of social media, politicians had to raise awareness in the print media (via paid advertisements) or by enticing journalists to write about them. Now anybody can publish anything without verification. For example, during the recent 2017 French Presidential campaigns, various Twitter accounts published contradicting information about the candidates. This resulted in the candidates having to disseminate a large amount of information in a short amount of time, leading to some confusion. One solution is for

political candidates to have strong and credible social media campaigns from the start.

- **Issue: The usefulness of websites to debunk fake news** – It is a huge challenge to debunk all fake news or disinformation because there is an enormous amount of content out there. Further, it may be more meaningful and efficient to remove whole websites which frequently post fake news, rather than individual stories.

- **Issue: 'Inoculation' of the public against conspiracy theories** - By presenting the flaws in conspiracy theories, it could be easier to present information that counters these alternative facts. An individual with a greater level of trust in his/her community could see reduced levels of susceptibility towards conspiracy theories.

- **Issue: A better understanding of individual rationalities and biases can help reduce negative biases** - By providing insights into the inner workings of the human brain, individuals may find it easier to understand and mitigate various cognitive biases and heuristics in online decision making.

- **Issue: Varying differences between cultures contribute towards appetite for risk-taking** - Cultures selectively emphasise different characteristics. Underlying personality characteristics also affect appetite for risk taking e.g. pessimists were more risk-averse; optimists were more risk prone. Societal and technological innovation increase opportunities for expression at a micro individual level.

- **Issue: Risk-taking is dependent on the perception of present and future danger** - For instance, even well-educated and liberal individuals are found amongst vaccine deniers in the United States. This could be attributed to a relatively high percentage of children with autism in the affluent neighbourhood community they are residing in as compared with children being afflicted by measles.

Distillation

- States should consider legislative mechanisms or enhancements to prevent the spread of fake news.

- State and society should consider how to limit the spread the negative news to prevent the sense of fear within society to escalate.

- Personal opinion is no longer 'personal' in the social media age, and public figures should be cognizant of this.

- Social media can be used as both a tool for disruption and for effective political campaigning, depending on how it is utilised.

- Fake news or disinformation has and will always exist. The question lies in how humanity evolves with the technology available to combat it.

Panel 2: State Actors and DRUMS

Denouncing 'Fake News' as a Social Control: China's Rumour Management Strategy on Social Media

Fu King-wa, Associate Professor at the Journalism and Media Studies Centre (JMSC), The University of Hong Kong.

The Chinese government uses different levels of censorship, intervention and control to control the flow of information, depending on both the content and context of issues. Heavy censorship may be counter-productive as it often increases public interest in the topic which has been censored.

- The term 'fake news' is problematic because it is very difficult to define what is truly fake news. This is because, in journalism, it is impossible to completely prevent error due to time constraints and the lack of information.
- 'Fake news' also implies an intention to falsify and mislead, which sometimes is not the case. There is thus a need to differentiate between fake news and propaganda, with the latter referring to an intentional attempt (often by those in power) to proliferate news stories to further their interests.
- The liberal camp tends to perceive fake news, and the prominent politicians and public figures who propagate it, as buffoonery. However, there is a need to perceive this phenomenon seriously, as opinion polls in the United States suggest that the traditional media enjoys a very low level of trust. This suggests that alternative media is being taken as legitimate sources of information by large portions of society.
- China has a very different context given the centrality and control of the state in managing media and information. Most of the media is owned and controlled by the party-state and thus social media takes on shades of reliability because it becomes the sole repository of unofficial news.
- The term 'rumours' has different connotations in China, enjoying a level of reliability because they are unofficial and also because the people have low levels of trust towards official information sources. Rumours are also seen as a form of protest against the regime.
- The Chinese government has started a campaign to manage rumours. This involves using regulation to license service providers who implement rumour management strategies on online content through a dual strategy of debunking rumours and implementing censorship.
- The research on censorship asked two research questions. Firstly, it attempted to discern if the level of censorship and the strategy used was topic specific. Secondly, it investigated whether the dual strategies of censorship and debunking rumours worked effectively. The research was conducted by analysing conversations and posts on Weibo before and after an accident which triggered a significant level of criticism towards the government.

- The findings suggest that there are 3 main groups of issues that attract differing levels of censorship from the Chinese state. The first group refers to issues that are politically sensitive and highly speculative. The regime tends to respond to these issues with heavy censorship. The second group refers to local government issues and behaviour and are largely not seen as highly sensitive issues. These posts and conversations are generally met with a moderate level of censorship and debunking. The third group consists of non-sensitive issues such as environmental issues, and tend to encounter very limited censorship from the government.

- The study also suggests that often, when conversations and posts are dealt with through heavy censorship, the issue tends to attract a greater volume of discussion. This suggests that heavy levels of censorship tend to be an ineffective means of stifling public interest in issues, instead having a multiplier effect of sorts on the level of interest in the topic.

Mapping and Understanding Information Actions in Cyberspace: The Case of the French Presidential Elections

Kevin Limonier, Associate Professor at French Institute of Geopolitics (University of Paris 8); and Scientific Director of the Russian-Speaking Infosphere Observatory (Castex Chair of Cyberstrategy, National Institute of Advanced Defense Studies - IHEDN)

Russian influence on the French Presidential elections consisted of external state influence combined with local collaboration. Russian misinformation was spread through a complex and heterogeneous ecosystem of people and organizations throughout France.

- The Russian-Speaking Infosphere Observatory was founded during the French Presidential election campaign by the government to monitor and analyse Russian information activities. Given the continuing investigations into the alleged Russian interference and influence in the American Presidential elections, the French government regards studying Russian behaviour as being of utmost importance. The purpose of the observatory is not to analyse alleged Russian attacks but instead to comprehend how digital space has become a vector of misinformation especially from Russian speaking countries.

- Russian media like RT or Sputnik are the flagships of the Russian soft power complex and have gained an important audience in Western Europe, especially in France and Germany. They cannot be considered neutral actors as they often openly support populist movements, especially far-right parties and in the French context, particularly the National Front (France) led by Marine Le Pen.

- At the heart of the proposed propagation framework of Russian misinformation strategy are the media platforms owned by the Russian state. Unlike cyber-attacks, the attribution of rumours and misinformation campaigns is not difficult to attribute because these platforms are owned by the state.

- There are also 3 main identifiable misinformation and rumour vectors within this framework that are mobilized to spread the desired content to a wider audience. The first group consists of common people who sincerely agree with the socio-political line of argument being propagated by RT and Sputnik and will thus share the content without any incentive or nudging.

- The second group is made up by the blogs and websites that make up an ecosystem proliferating fake news and conspiracy theories in French. For this ecosystem, content from RT and Sputnik are vital sources of legitimacy and raw materials to be used for their own purposes. The groups behind these websites may often have little to no connection with Russia, often employing misinformation for their own objectives and purposes.

- The third group is specific to social networks with automated or semi-automated accounts that mass-replicate content to artificially multiply RT or Sputnik's audience.

- The Observatory employs many tools to study these three main vectors. One of the main tools employed is a database created to identify the main social network actors participating in the propagation of Russian state media content on social networks. Through building and employing this database, it is observable that the French speaking 'Russo-sphere' is highly heterogeneous, made up different political inclinations. A clear majority of this 'Russo-sphere' are not paid agents and share this information of their own volition. Another part of this sphere are bots and activists accounts that transmit information in large, rapid quantities for political purposes.

- Russian influence on the French Presidential elections was not direct. Russian state media mass produced misinformation, but this would not have had any significant effect without a complex ecosystem of people and the convergence of interests between these heterogeneous actors.

- The phenomenon of external state influence synergized by local collaboration is by no means a new one. What has changed is that we now have the capacity to map this phenomenon and understand this using big data analytics.

The Power of Fake News: Gulf States Seek to Rewrite Rules Underlying International Relations

James M. Dorsey, Senior Fellow, RSIS

The Gulf Crisis is supported by psychological warfare from state-controlled media outlets that facilitate the proliferation of fake news. These outlets produce news that reinforces the beliefs, biases and prejudices of their audiences, to entrench the state narrative that supports the conflict.

- DRUMS are a long-standing fixture of public relations, public diplomacy, dispute, conflict and warfare and are a part of psychological warfare.

- The only way a journalist can reduce the risk of being manipulated by a source is to obtain as many different accounts and perspectives as possible. Journalists must also repeatedly check every piece of information to prevent being misled and used.

- Psychological and cyber warfare has played an important role and lies at the core of the Gulf Crisis. The Gulf Crisis started with psychological warfare pursued by state controlled media outlets and in the absence of independent, hard-hitting journalism and analysis. State controlled media in several Middle East states have purposefully orchestrated and facilitated the proliferation of fake news to entrench the state narrative that has served to enhance the crisis.

- Global changes in the role of media and the expectations of media consumers have made psychological warfare much easier.

- This explains why the controversial state-owned Al Jazeera network has been a central actor in the crisis, with detractors of Qatar demanding it be shuttered. Al Jazeera understands that a significant section of the market has shifted from demanding facts to craving a media product that reinforced their own beliefs, biases and prejudices.

- Al Jazeera has had a revolutionary impact on the media landscape in the Middle East, fostering a media environment in which individual media outlets are increasingly sophisticated, opinionated, controversial and combative while parroting the parent state's narrative.

- Crafting the message in pluralistic rather than autocratic environments is far more laborious. It involves government backing on a global scale of legitimate organisations, the creation of fake organisations, the funding of organisations like powerful think tanks in key capitals and influencing journalists and analysts associated with credible news outlets.

- This highlights the tension that exists in modern journalism between being a hard-hitting journalist or who is completely objective and the need to maintain influential sources and contacts coupled with the desire to be part of the power elite.

- Psychological warfare always has been and always will be a fixture of political and social life regardless of regime type. Technological advance and an increasingly globalised world has made dealing with and combating psychological warfare far more complex. While there are no absolute counter-measures, an independent, critical media may function as an antidote.

- Cyber war involving DRUMS is the new frontier. Like all forms of warfare, it needs to be bound by international conventions, norms and regulations. While these norms will certainly be imperfect, they will function as a necessary starting point.

Syndicate Discussions

- **Issue: Possible developments in tools used to trace information or fake news** – An enhancement which can be considered is the use of content analysis tools together with tracking tools currently used to trace where the information travels. This can be used to trace the source of translations between languages, for example, the Macron leaks were found to be most likely translated from French to English by bots.

- **Issue: Limits placed in China on information control** – Laws exist to restrict the spread of rumours in China. For example, service providers in China require licenses to operate and are only allowed to carry news, but not produce news. Mobile and internet users can also be traced via their mobile phone usage and their residential addresses. There are also government crackdowns on online streaming, and several websites and social media platforms are blocked.

- **Issue: Legal issues concerning "fake news"** – National and international legal standards are being questioned because of actions taken based on the belief in fake

news. For example, the belief in the presence of weapons of mass destruction in the Middle East led to an invasion by Western states. Defining what constitutes “fake news” would also be questioned, as issues may be raised when individuals sue for defamation based on news which is partially or fully false.

- **Issue: Conspiracy theories thrive in political climates where there is instability and uncertainty** – This occurs mostly in closed, autocratic systems, where the conspiracy theories are fed both by the government and the distrust of it. For example, conspiracy theories in the Middle East are static and have remained somewhat consistent over generations.

- **Issue: Network topographies or infrastructure of social networks are a means of power** – Knowledge of this enables better visualisation of problems in cyberspace. For example, it is not very useful to be able to geo-locate Twitter or Facebook accounts, because bots can be used to post from a different location with the same account. Text mining has produced some results, but insufficient to solve such issues.

- **Issue: Laws to regulate the media are essential to prevent the spread of rumours and untruths** – For example in China, strict media regulations ensure that individuals are penalised for spreading rumours. However, rumour debunking is not always effective, as it diverts resources and attention away from addressing potential grievances.

- **Issue: Not all critical content of the Chinese government is censored** - Criticism targeted at local governments are allowed to propagate online within limits; whereas criticism targeted at the national government is immediately censored by federal authorities.

- **Issue: Chinese propaganda strategy involves the involvement of state employees deploying manual censorship** - There have been recent moves to limit, control and remove the uploading and sharing of user-content generated videos from Chinese social platforms (e.g. Weibo). However, censored content could further intensify online interest and direct people to backchannels to access content through privatised means (e.g. Virtual Private Networks or Tor).

Distillation

- More consideration should be placed on the legal responses to fake news, both within states and at the international level.

- More tools should be developed to trace sources of misinformation and fake news. Since the content may cross borders, translation and content analysis capabilities should be developed to address cultural and language limitations to analysis.

- Conspiracy theories are categorised under the DRUMS umbrella, but should not be dismissed entirely as they may reveal actual political situations.

- There are possibilities of developing new methods of cyber visualisation of fake news, based on the principle that mapping the infrastructure can be an advantage.

- Censorship efforts may fail if they result in a lack of trust in the government. Governments may gain credibility if they recognise their flaws publicly.

Panel 3: Media and DRUMS

Distinguishing Fact from Fiction in the Modern Age
Andreas Schleicher, Director for the Directorate of Education and Skills, Organisation for Economic Co-operation and development (OECD)

To defeat fake news, governments need to become more innovative, open, inclusive and creative in the policy-making process. The education system should revamp its teaching methods to improve digital literacy and information navigation skills in people.

- Digitalisation has made the world increasingly connected but also more complex and volatile. The primary characteristics of digitalisation - democratising, concentrating, particularising, homogenising, empowering and disempowering – have also triggered the creation of virtual barriers and distrust.

- With abundant content and a wide group of consumers, these effects of digitalisation have made it possible for fake news to proliferate in social media echo chambers.

- To overcome the virtual barriers and curb the success of fake news, governments should adopt more creative methods in their policy-making processes. Work needs to be done to revamp the learning process in schools so that there can be teaching of skills to help people navigate the complex world of abundant information.

- The seven core skills to be embedded in future schools' curriculum are: (1) creativity, (2) critical thinking, (3) problem solving, (4) innovation, (5) collaboration, (6) data gathering, and (7) communication.

- In addition, these eight key character qualities should be inculcated through schools for a more holistic education: (1) empathy, (2) resilience, (3) mindfulness, (4) inclusion, (5) curiosity, (6) ethics, (7) courage, and (8) leadership.

- There are three methods through which future curriculum in schools can foster the key skills and character qualities necessary to develop digital literacy and information navigation skills in people. First, future schools and teachers must be willing to collaborate and share with other schools and teachers. Second, the curriculum should be integrated and connected with the real-world issues. Third, the hierarchical nature of the student-teacher relationship should be removed so that there is better engagement and learning. With these three methods in place, learning will be an activity that is not limited by a restrictive curriculum. This will help to develop people who are able to effectively navigate the expansive digital world.

Fake News – Who are the new gatekeepers?
Han Fook Kwang, Senior Fellow, S. Rajaratnam School of International Studies

Fake news has emerged because the ongoing information revolution is powered by user-driven phenomena such as filter bubbles, herding bias and programmatic advertising. Online content consumers are now the new gatekeepers of information legitimacy.

- In the current age of online news consumerism, print media is gradually fading as online platforms emerge strongly. Fake news has emerged because of the ongoing information revolution.

- To succeed against fake news, it is important to understand how news is created, how it is disseminated and how people become the active filters in searching for what to read and repost (disseminate) based on their interests. The phenomena that are making fake news successful on online platforms are: (1) the existence of filter bubbles; (2) herding bias; and, (3) programmatic advertising. These three phenomena work in favour of fake news and also towards the demise of the traditional newspaper.

- Filter bubbles exist where online news consumers use filtered searching extensively to restrict what they read and the sources they obtain news from. This creates a myopic perspective of the world and current issues. The consumer only consumes what is of interest to him without getting the full picture.

- Herding bias exists where people act and function in herds to believe what their social group believes in, even when accuracy and legitimacy are in doubt. Fake news thrives in such an environment because there are more people who are interested in reading popular (even if inaccurate) news clips that are highly trending on online platforms, than content which is not trending (even if accurate).

- Programmatic advertising allows advertisements to be targeted to online social media users based on their preferences and interests, which have been gathered from their browsing history. These factors are driven by the behaviour of the people; therefore, the new gatekeepers of information are the people.

- Governments need to understand how these phenomena favour fake news and have caused the demise of traditional media, especially if they are worried that other states are using fake news to target them politically.

Global Engagement Centre (GEC)'s Approach to DRUMS
Daniel Kimmage, Head, GEC, US State Department

GEC has recently shifted its focus towards coordination and the use of technology to counter misinformation. GEC continues to coordinate with other reliable agencies to ensure that has effective engagement strategies.

- GEC was established in 2010 to lead the US in counter propaganda as part of the overall counter terrorism efforts. Since GEC has no financial powers, much of its work has relied on networking and cooperation functions such as working with the Salafi centre to enhance US's counter-terrorism efforts.

- From 2012 to 2013, the GEC focused on direct communication and campaigning. From 2014 to 2016, the GEC focused on partnership building to develop better credibility for its campaigning efforts.

- GEC has recently shifted its focus towards coordination and the use of technology to counter misinformation. GEC has started leveraging on technology such as A/B testing and sandwich surveys to evaluate the efficacy of its messaging and communication.

- There are still challenges facing GEC: Firstly, it is not possible to compete with the immense volume of misinformation online and it is difficult to counter every false piece of content online. Secondly, there are no clear metrics to instantly identify fake news. Thirdly, the question remains whether the counter-messages should be positive or negative.

- One way to overcome these challenges will be to encourage respectful discourse, sharing of accurate information and critical thinking amongst online users. GEC aims to demonstrate that institutions have better worth than fake news agencies in open discussions about ideas. GEC will continue to coordinate with other reliable agencies to ensure that has effective engagement strategies.

Global Fake News and What the BBC is Doing to Combat It
Arti Shukla, Assistant Editor (Asia), BBC Monitoring

BBC relies on the team at its User-Generated Content (UGC) hub, "Reality Check", to review user-generated and social media content for authenticity and credibility, as well to conduct forensic checking of news footage. BBC uses its expert network establish the authenticity and credibility of news that it receives. It also educates its viewers and readers on information literacy.

- Fake news feeds existing concerns, expectations, and fears. It uses skewed but agreed views to create chaos, confusion and paranoia.

- BBC maintains a strict set of editorial values: (1) accuracy of the truth in the information obtained; (2) impartiality to reflect breadth and diversity of opinions without taking sides; (3) fair and open-minded evaluation of evidence and facts; and, (4) independence.

- BBC leverages on technology and public education to uphold its editorial values and prevent fake news being published on its platforms. To achieve this, BBC relies on its UGC hub, "Reality Check", in coordination with expert network agencies, data journalism and public education.

- The UGC hub has a team of journalists who review user-generated and social media content before it appears on any of BBC's digital, radio or TV platforms. A thorough verification process of checks and filters is used to check for authenticity of the content and the social media account to establish the credibility of the information obtained.

- BBC also uses forensic checking of footage to establish credibility and has a dedicated page that publishes BBC's "Reality Check" of trending news as a pro-active method to answer readers' questions on speculative and sensational news.

- BBC's expert network, comprising BBC Media Action, BBC Monitoring and BBC World Service, coordinate to establish the authenticity and credibility of any news-worthy information that they receive.

- BBC relies on data journalism to keep a close track of trends in the world. BBC's Trending team leads this effort by providing educational videos and articles on how people can consume online content responsibly.

- BBC also uses various methods to educate its viewers and readers on information literacy and create awareness of the importance of establishing the credibility of any content online before believing it and disseminating it to others.

Syndicate Discussions

- **Issue: Creating knowledge and sensitivity are crucial to identifying fake news**– Facebook and Twitter have been at the forefront of trying to combat fake news. Mainstream news media has only recently begun taking steps to address the issue of fake news. Online forensic tools and tagging mechanisms are useful in identifying fake news. However, inculcating sensibilities in audiences/readers to identify inaccurate information is key. This includes educating users about the 'social media filter bubble' and its effects of creating potentially harmful echo-chambers.

- **Issue: Whether a post-modern perspective on DRUMS is dangerous**– If every individual is entitled to his/her own truth, then the premise of fake news falls. It is dangerous to apply such a relativistic approach in politics especially, because propaganda or untruths from adversarial states may have grave national security implications.

- **Issue: It is a great challenge for mainstream print media to meaningfully participate in combating fake news** – Profits for print media organisations have plummeted since the advent of social media. However, online media is not a viable business model as most revenue from advertisements goes to Google or Facebook. Media organisations may have the resources to contribute to combating fake news if they are acquired by tech companies.

- **Issue: Presenting facts alone might not be the most suitable way to tackle the challenges of fake news** - The presentation of facts in a narrative format which appeals to individual biases might better resonate with individuals as it could reduce potential resistance.

- **Issue: An increase in technology companies purchasing news agencies could see new opportunities for rejuvenation** - News agencies are further empowered with resources to find their specialty or niche branding in the current digital world (e.g. Washington Post), as readers are willing to pay for quality journalism. The balance between ensuring journalistic integrity and a sustainable business model is a challenge for news agencies going forward.

- **Issue: There is an increasing reliance and trust in the credibility on news agencies to be the arbiter of facts** - The British Broadcasting Corporation (BBC) fact-checking tool “Reality Check” was used during the Brexit referendum to provide users with accurate information about various campaign promises made by both the Leave and Remain camps. “Reality Check” was made into a permanent feature on their websites after the Brexit referendum.

- **Issue: The increasing commercialisation of social media sites amplifies echo chambers within communities** - This is compounded with increased targeted advertising capabilities on social media platforms. Data industrialisation companies such as Cambridge Analytica in the United States allegedly have the ability and technological tools to predict and monitor the activities of individuals; from pre-intent to post-purchase.

Distillation

- Knowledge and awareness creating about DRUMS may be more important than rushing to combat it.

- Taking a post-modern stance that all information is subjective may be counter-productive to national security strategies.

- There is an increasing reliance and trust in the credibility on news agencies and fact-checking websites to be the arbiter of facts. Their challenge is to find a balance between ensuring journalistic integrity and a sustainable business model going forward.

- It is vital to inculcate sensibilities in audiences/readers to identify inaccurate information, including educating users about the ‘social media filter bubble’ and its effects of creating potentially harmful echo-chambers.

Panel 4: Information and DRUMS

Integrating Resilience in Defense Planning Against Information Warfare
Janis Berzins, Director, Centre for Security and Strategic Research, National Defense Academy of Latvia, Latvia

The level of resilience to information warfare needs to be monitored consistently. It can be enhanced by explaining adversaries' goals to citizens; winning the hearts and minds of citizens; enhancing critical thinking; enhancing the standard of journalism needs to be enhanced; and exploring means of communications that do not involve the media.

- Disinformation campaigns are not only about the spreading of untruths, but can encompass selective retelling of true information to create an alternate vison of truth.
- People are now more willing to exit a society due to political and economic reasons. Based on the Exit, Voice, and Loyalty model by Hirschman, citizens are more willing to leave because the costs of voice and loyalty to the citizen are becoming higher and the benefits becoming less attractive.
- One common denominator of the misinformation sources studied is their ideology of anti-globalism and anti-Western democracy. These groups include alt-right, alt-left, Russian, and Muslim groups. These ideologies have become more pervasive because of the perception that political leaders are not fulfilling their end of the social contract.
- The nature of warfare is changing. Development of weapon systems is expensive, and states would rather fight an information war rather than a conventional war. Part of this strategy seeks the destabilization of society rather than the destruction of society. It moves the battlefield from the physical domain to the psychological and cyber domains.
- China and Russia have incorporated information warfare into their military doctrines. Success of these doctrines correlates positively to how citizens and businesses are willing to exit the target state politically, economically, socially, or culturally.
- The level of resilience to information warfare needs to be monitored consistently. This can be operationalized by defining measurable criteria that can be iterated on a regular basis. Examples of such criteria include: how willing people are to defend their country, and the level of trust in state institutions.
- Resilience needs to be enhanced at a cognitive level. This is done on five levels: first, the strategic goals of adversaries and how they are implemented must be explained to citizens; second, gaps in strategic communication between government and society need to be reduced to win the hearts and minds of citizens; third, critical thinking needs to be enhanced; fourth, the standard of journalism needs to be enhanced; and fifth, governments need to explore means of communications that do not involve the media.

Mapping the News Ecosystem
Jonathan Albright, Research Director, Tow Center for Digital Journalism, Columbia University

Network analysis can determine how news was spread across the political spectrum during the American election. Political messages can be spread cheaply and widely using established platforms like YouTube and Google.

- Small websites carrying news articles were not motivated by advertisement revenue. Studies on the flow of information show that articles from these websites were instantly shared on direct messaging platforms.
- There are new trends in how data flows are being studied. Researchers are looking to map real time sentiment, social trends such as the use of emoji, cookies, and voting records.
- Micro-propaganda can also be mapped on a network to see the relationship between political groups and news sites. Issue and interest clusters on Google Plus were studied. Liberals were more trusting of larger network websites like CNN and MSNBC, compared to conservatives, who typically shared smaller information resources.
- Far-right groups are using alternate broadcast methods like YouTube and Google to reach a wider audience. Videos can be automatically created by trawling and pulling data from YouTube API, and creating content based on a few keywords.
- Government websites and candidate websites are close to the centre of the mapped information system.

The State of Fake News in Germany
Karolin Schwarz, Founder, hoaxmap.org; and, Editor, correctiv.org

Fact-checking websites are essential in combating fake news. Germany will penalise social media websites who fail to take down news items that fail independent fact checks. Fake news operators have added new methods such as printing out fake news and giving them out as flyers on the street.

- Most of the fake news incidents in Germany involve claims of sexualized violence. These reports of fake news usually involve refugees claiming social welfare, and have been the case since February 2016.
- There are a few ways that fake news operators convince people that the story is true: first, operators use ‘eyewitness’ accounts as a way of authenticating the story; second, photos and videos are falsely attributed to people like refugees or locations to create panic; third, falsely attributed quotes; and last, create fake documents to ‘promulgate’ new rules.
- Users of Correctiv.org can dispute the veracity of a website, and the news article in question is submitted for independent fact-checking. Correctiv.org then gives a ranking (number of Pinocchios) to determine how truthful a piece of news is. Users are also informed that a piece of news is disputed before they share it.

- Germany has new legislation in place (passed in June 2017) to compel social media websites to take down offending articles. Social media sites like Facebook will be given 24 hours to take down "obviously" illegal pieces of news, which may cause an incitement to violence, and 7 days to take down an article if it fails an independent fact-check. The law provides fines up to 50 million Euros if social media networks do not comply.

- There is a strategic shift from fake news operators, moving from Facebook to Russian social media site vk.com; and moving vigilantism on to the streets. Online conspiracy theories have also been printed out and given out as flyers on the street, ostensibly to target people who are not on social media.

Syndicate Discussions

- **Issue: It is a major challenge to attribute responsibility to actors in relation to DRUMS in the online space** – News posted on social media sites such as Facebook is branded as 'Facebook news', even if it is posted directly by the news organisations. This makes accountability dubious, and disproportionately increases pressure on sites such as Facebook to act.

- **Issue: Hyper-partisan websites have been largely ignored in many countries** – At the meta-level, these websites need to be closely scrutinised as they may sway public perceptions in politically harmful ways. They may also serve as fake news outlets for international audiences.

- **Issue: DRUMS may be used by states as a form of psychological warfare** – For example, Russia used (and continues to use) propaganda online and offline to achieve its tactical objectives in Crimea.

- **Issue: Distinctions between populism and nationalism should be distinguished** - Populism occurs when politicians engage in unsustainable politics and policies whereas nationalism is the defence of a country's national interests. This has arisen because of the misconception, in globalisation, that all countries share common national interests.

- **Issue: The identification of early triggers of hybrid warfare to forewarn incidents before cyber-attacks occurs** - It is hard to predict as the timeframe to have sufficient warning is marginally thin. It is dependent on public sentiment as well as covert forces for monitoring and counter intelligence purposes.

- **Issue: Refuting fake news over social media platforms** – There are certain topics which are more susceptible to fake news. For example, in Europe, articles or content on crimes being committed by refugees tend to be spread wider over social networks as they are largely fuelled by xenophobia. Effort should therefore be taken to fact-check content, and refute if the news is found to be false. However, some conspiracy theories are more difficult to disprove due to the lack of publicly available information.

- **Issue: Assisting in the need to fact-check information –** While some may be more cognisant of fact-checking the content of articles or reports first before sharing them, there are many who readily share content which may not be true. What can be done would be to enable the flagging of articles which have been checked to be true.

Other articles containing questionable content may also be flagged. There should also be some mechanism to assure there is no abuse in flagging fake news as true.

Distillation

- States need to keep citizens engaged with national objectives, and not drive them to want to exit their society.
- Strong societal resilience and trust are vital for a state to address issues arising from fake news.
- Foreign misinformation and influence operations need to be declared as soon as they are discovered, but must not be done to deflect political pressure or obscure the truth. Doing so may cause citizens to lose trust or become cynical with the government.
- Tech companies are acting against fake news and radical movements online, and states must work with them to find feasible solutions. This can be more effective than attempting to legislate against untruthful news sources.
- Citizens who feel excluded from society may seek alternate news sources to validate their views, leading to a polarised society.
- Social media sites are in a tough position. Larger questions need to be asked on who the responsibility should lie with, and what role “platforms” such as Facebook should take.
- Fact-checking is essential to combat DRUMS, but equally important is creating a “hoax map” to inform the public of what fake narratives are being spread.
- Efforts should be taken in developing mechanisms to label, tag, or flag news as fake.

Panel 5: Technology and DRUMS

How Democratic States Combat the Multidimensional Threat of Influence Operations
Jakub Janda, Head, Kremlim Watch Programme; and Deputy Director for Public Policy, European Values Think-Tank – Czech Republic

Multidimensional disinformation efforts from hostile foreign states include intelligence operations, disinformation operations, use of local political allies, local radical and extremist groups, minorities, non-governmental organisations (NGOs), and economic operations with political goals. Governments need to respond by placing this on the foreign and security policy agenda; challenging state-sponsored disinformation efforts; exposing disinformation campaigns; and building societal resilience.

- Countries face disinformation efforts from hostile foreign states, which employ various tools to influence domestic behaviour: intelligence operations (including cyber), disinformation operations, use of local political allies, local radical and extremist groups, minorities, non-governmental organisations (NGOs), and economic operations with political goals. While the aims and volumes of foreign disinformation efforts differ from country to country, the mechanisms are largely similar.

- Governments need to craft policy to limit efforts by hostile foreign powers to change attitudes. This should be based on specific and objectively measurable factors which are sustainable in the long-run.

- In terms of devising national policy, four areas in terms of responses must be addressed: (1) put hostile disinformation efforts on the foreign and security policy agenda; (2) publicly challenge supporters of state-sponsored disinformation efforts; (3) disclose the substance and vehicles of disinformation campaigns; and (4) systematically build societal resilience.

- To place hostile disinformation efforts on the foreign and security policy agenda, a national security audit must first be conducted to codify interests in a precise manner. Policymakers should consider both classified and open source intelligence to establish a clear strategic situational picture at this phase. This task should not be left to the intelligence community, but should be a shared effort to broaden the scope of assessment.

- Scenarios should be considered to project how a threat will evolve in the next three to five years. Policymakers should also consider how their political system can be prepared to face the threat. First, coordination mechanisms as well as counter-measure strategy must be crafted. Vulnerabilities and blind spots must also be considered in threat assessment. Second, institutional adjustment must be tailored by establishing common understanding among ministries and agencies.

- To publicly challenge supporters of hostile foreign influence, political and public consensus are important.

Computational Propaganda in China and Beyond
Gillian Bolsover, Researcher, Oxford Internet Institute – United Kingdom

Propaganda is now created and disseminated using computational means, including the use of bots to automate activities, disseminate messages, flood out information, and target users. The key to fighting computational propaganda is educating citizens in critical thinking, information seeking and access to diverse and impartial information.

- Computational propaganda is propaganda created and disseminated using computational means. Propaganda is the manipulations of representations to appeal to audience emotions to achieve predetermined ends. The use of bots, pieces of code that automate activities online and replicate human activity, is one of the ways by which computational propaganda is being conducted. Bots can be used to disseminate message, flood out the amount of information that is available on the topic, silence conversation, and target specific users.

- The scale and nature of computational propaganda varies a great deal in different countries and contexts. It is therefore important to consider computational propaganda in its context and not apply lessons learnt from different contexts without considering the interaction of information systems with the political system.

- In China, computational propaganda is used in the censorship system, for blocking content. The Chinese state, however, prefers to use the human resources at their disposal, rather than automation, to promote their opinion.

- On the other hand, small interest groups use social media platforms to artificially inflate their voice in advocating messages that are counter to the Chinese state.

- The challenge of propaganda is not its existence, but how people respond to it. Susceptibility to propaganda is dependent on an individual's worldview and ability to understand propaganda.

- Social media sites facilitate computational propaganda due to their commercial nature and structure. Commercialisation of the Internet exacerbates and fortifies echo chambers and easily digestible information. Online information and social media architectures do not represent what users think they are or want them to be.

- Computational propaganda should be fought, not through regulation and removal, but by educating citizens in critical thinking, information seeking and access to diverse and impartial information.

Facebook's Approach to Authenticity
Alvin Tan, Head of Public Policy, South East Asia, Facebook - Singapore

Facebook is taking steps to address online misinformation, including providing tools for users to report offending content, employing artificial intelligence to review content, and increasing the size of its review team. It is also using machine learning to detect fraudulent fake news sites that are financially motivated, and working with third parties to provide fact checking.

- After the U.S. election in November 2016, Facebook recognised the harmful impact of fake news on its community. Fake news makes the world less informed and erodes trust. While not a new phenomenon by any means, the medium of fake news dissemination has changed. Facebook has therefore made addressing misinformation its priority.

- Facebook emphasises the need for policy to keep users safe, foster civility and responsible behaviour as well as promote free expression and sharing. Facebook has established Community Standards to determine what users are allowed to post on its platform, forbidding content that extols hate speech, violence, spam, pornography, human trafficking, and identity theft. It hires subject matter experts as well as engages in partnerships to help them understand and enforce the policies better. Facebook's policy aims to be principled (providing same treatment for everyone globally), operable and easy to understand.

- Facebook also provides users with tools to report content that violates the community standard. It provides around the clock review and employs artificial intelligence to keep pace with the large amount of reported content. It is also planning to add an additional 3000 individuals into its review team.

- Facebook is working to fight the spread of fake news in 3 key areas: Firstly, it is disrupting economic incentives for its creation. A large segment of fake news is financially motivated. For instance, spammers make advertising revenue by masquerading as legitimate news sources, and posting hoaxes to drive traffic towards their sites. Facebook employs machine learning to detect fraud and stop fake spam accounts.

- Secondly, it is building new products to make it easier for users to reporting fake content. It is also working with third parties to conduct fact checking. In the U.S. and some parts of Europe, users can flag or report false news. To promote informed sharing, users will be shown warning that content has been found dubious by fact-checkers, before they can share that content.

- Thirdly, Facebook is helping users make more informed decisions, by providing users with more context about stories so they can make informed decisions about what to read, trust and share. It is also exploring ways to give people access to more perspectives about the topics that they are reading. To this end, the company is conducting a pilot study of the efficacy of fact-checking products. It has also outlined ten tips on how to spot fake news.

- In the long-term, Facebook believes that media literacy should be enhanced to educate users about evaluating content. The company works with the Media Literacy Council to boost some posts. Through the Facebook Journalism Project, it also develops news products in consultation with journalists and seeks to establish strong ties with the news industry.

Syndicate Discussions

- **Issue: Defining content or photos allowed on social media platforms** – Social media platforms such as Facebook often need to decide if content or photos should

be allowed or not. For example, the well-known historical Vietnam War era picture, of a girl whose clothes had been burnt off her back due to a napalm attack, was the source of controversy in Norway, for possibly promoting nudity or exploitation. However, Facebook determined the photograph was politically significant and therefore allowed the photograph to be displayed on its platforms.

- **Issue: Publicly available data versus those less available** – In China, WeChat is the most significant form of social media and instant messaging application used. This also suggests how data may be more difficult to be accessed, as these closed platforms offer privacy to their users. Researchers studying topical issues in China find it difficult to penetrate the discussions and groups taking place on WeChat, unlike in other countries where Twitter can offer publicly available data.

- **Issue: Combating propaganda in society** – One way to deal with propaganda is by introducing fresh propaganda to counter the original message. This has happened in many states, including China. What would be ideal is to equip individuals with the literacy tools to assess propaganda for themselves. Another way would be to promote “agnostic pluralism”. This suggests an acceptance of conflict coming from the clash of propagandas, and thereby seeking the potentially positive aspects coming from the conflict and taking actions from there.

- Issue: Consideration for mandatory real name user login and authentication when posting online content to promote user accountability - Scaling artificial intelligence could remove fake accounts from social media platforms and websites. False positives which are flagged online can be taken up by human moderators for further review.

- **Issue: Fostering community resilience online** - The reliance on the network of individuals could promote a sense of distrust and hostility towards various out-groups (excluded groups), and could increase the nature of exclusion. The introduction of alternative viewpoints could provide credence towards out-group heterogeneity and variety on social media platforms online.

- **Issue: Use of artificial intelligence could lead to significant economic and political implications** - It is crucial for the public to understand the implications of the pervasiveness of artificial intelligence. Initiatives such as civic education and media literacy could aid in challenging media distortions online.

Distillation

- Governments need to craft sustainable long-term policy to limit disinformation efforts by hostile foreign powers.

- Fake news that is funded by advertising revenue must be countered through disruption of economic incentives for its creation.

- To boost societal resilience against the impact of fake news, education in critical thinking, information seeking and access to diverse and impartial information should be implemented.

- Individuals and society have significant roles to play in determining the type of content allowed to be displayed publicly.
- More literacy tools for society to suitably assess the available content on their social media platforms should be encouraged.
- Platforms should hold those who post content online accountable, by encouraging real-name user identification, which may help prevent the use of fake accounts.

Panel 6: Hybrid Warfare

NATO as an Alliance in the New Hybrid Warfare Environment
Barbara Maronkova, Director, NATO Information and Documentation Centre, Ukraine

NATO's fight against "fake news" has reached a higher level, as disinformation and propaganda operations aiming at weakening the Alliance have considerably increased since the annexation of the Crimea region by the Russian Federation in 2014.

- Interconnectedness makes hybrid warfare a complex challenge to overcome. Russia's hybrid warfare primarily involves military manoeuvres such as the deployment of troops and the provision of support to Separatists located in Eastern Ukraine. This approach is combined with large-scale cyber-attacks, energy blackmail and a highly aggressive propaganda campaign.

- The leaders of NATO's member states developed counter-measures that encompass strategic communication, exercise scenarios and coordination with other organisations. The Atlantic Alliance also identified cyberspace as the fifth operational domain after land, sea, air and space. This led to the definition of cyber security standards and minimal requirements.

- NATO is faced with a well-planned campaign of disinformation. Some Russian government officials, journalists and "experts" are used to sharing false information. As a response, the Atlantic Alliance refers to real facts and figures. It actively debunks myths on a case-by-case basis, instead of waiting for persistent plots theories and libels to vanish.

(Mis)information Wars – the State of Play in Norway
Per Kristen Brekke, Deputy Director, Norwegian Directorate for Civil Protection (DSB)

Norway has developed a strategy that aims at protecting vital societal functions against multiple security challenges, including hybrid threats. This strategy is based on a whole-of-society approach and a high level of local, regional and national coordination.

- Hybrid warfare is designed to exploit a wide spectrum of national vulnerabilities. Norway's "total defense concept" was coined as an answer to these multifaceted issues. It is based on mutual support and cooperation between the armed forces and civil society in time of crisis, including the three phases of prevention, preparedness planning and crisis management.

- Norway's police force expects campaigns of misinformation to be launched by foreign intelligence services during periods of security tensions. These influence operations are likely to happen along diplomatic, economic and military lines. The "total defense concept" is thus in the process of being enhanced, with a view to strengthening societal safety and resilience.

- The Norwegian Directorate for Civil Protection (DSB) identifies abnormal situations and works to ensure that hybrid threats are appropriately dealt with by all actors involved. The latter include national, regional and local stakeholders such as

ministries, infrastructure authorities and NGOs. DSB and county governors facilitate coordination between these various levels.

Hybrid Walfare in the Baltics: Threats and Potential Responses
Andrew Radin, Associate Political Scientist, RAND Corporation

Security threats from the Russian Federation remain a paramount concern in Baltic states. Russia may use non-violent subversion, covert violent action, or conventional invasion, in Estonia, Latvia and Lithuania, unless the US and NATO have a credible response.

- Hybrid warfare is understood as the use of covert or deniable activities, supported by conventional or nuclear forces, to influence domestic politics. Russia's seizure of Crimea and its involvement in Eastern Ukraine provide textbook examples of hybrid conflicts in which non-military means such as information operations have become a strategic tool.

- Non-violent subversion alone is unlikely to be able to influence Russian-speaking communities living in Baltic states. These large minorities (25%, 26 % and 6% of the Estonian, Latvian and Lithuanian populations) face political and economic challenges, but many Russians speakers are well-integrated, and they do not share an evident desire for separatism.

- However, covert actions such as the support for anti-government proxies could escalate to conventional warfare and trigger a NATO response. Military invasion backed by political subversion could also lead to a nuclear standoff with NATO. The credibility of the US and NATO's reaction is essential in deterring Russia from engaging in such scenarios in the Baltic states.

Syndicate Discussions

- **Issue: Emphasising the need for social resilience within societies** – There may be difficulties emphasising social resilience in societies which live in peace. There must be efforts to find out the potential challenges facing those societies in the future, and how individuals perceive risks and danger. Norway is focusing on "forward resilience", considering defining the concept with experts, and learning how the Baltic nations build their resilience against Russian disinformation.

- **Issue: Resilience to fake news** – Countries like Lithuania tend to be more resilient to fake news, as they have lived under Soviet propaganda and are used to receiving news which is untrue. Lithuania presently enjoys an open society where civil society and the media can expose untruths. This helps build a more resilient people, as there are sections within society who are attentive in ensuring factual content.

- **Issue: Tracking Russian language propaganda in the Baltic states** – Tracking Russian language propaganda includes surveillance of propaganda sources online as well as talking to individuals. However, time and resources are limited, considering the expanse of propaganda sources. Large investments are required, including machine translation of content from or into the Baltic languages for analysis.

- **Issue: Creating a cyber-strategy at the regional and national level** - The NATO Centre of Excellence is a centre which analyses realistic hybrid warfare scenarios

and trains NATO member countries. This creates a common level of understanding of cyber capabilities and competencies between various member states.

- **Issue: The importance of having a clearly defined national cyber strategy** - This includes the explicit identification of hostile and non-hostile threats to cybersecurity, and the necessary mechanisms and strategic interests required to deal with hostile threats.

- **Issue: Cyber equivalent for forward defence** - A cyber equivalent of forward defence would require the transparency of cyber-attack details and the means by which to disseminate information regarding the attack to the public.

- **Issue: International groupings can posit a whole-of-community response when facing cyber-attacks** - Cyber-attacks on countries should trigger a NATO-like response and a whole-of-community approach from international groupings. However, at the political level there is little consensus on the activities which would entail a full spectrum approach and response.

- Issue: Most “fake news” directed against NATO is not particularly sophisticated, which makes it easy to dispel. However, these hoaxes need to be tackled at an early stage to limit the damage they are likely to cause.

- **Issue: Working with journalists.** Ad hoc partnerships with trusted journalists have proved to be particularly effective in spreading correct information and pushing back against fake news stories.

- **Issue: Countering non-violent subversion**. Non-violent subversion should be confronted with targeted measures such as increased Russian-language broadcasting of counter-messages. Countering covert action will also require continued support for Baltic security forces. At the same time, strengthening conventional deterrence will involve improved transparency and public relations to reduce the risk of Russian miscalculation.

Distillation

- Fact -checking and verification are essential in the fight against DRUMS.

- Addressing hybrid threats is a challenging process, as the line between civilian and military issues is blurred.

- Non-violent subversion is unlikely to be a game-changer by itself, as covert and overt violent action remain major threats.

- More efforts should be taken in improving the level of resilience within societies to fake news and propaganda.

- Drills or simulated activities of potential challenges to society should be practised in states living in peace, including how society should react when confronted with propaganda.

Closing Panel/Moderated Discussion

Shashi Jayakumar

- The approach to tackle DRUMS is case and context specific. By analogy, in cyber offence operations, there may never be a strategic arms limitation treaty. The Tallinn Manual is the best attempt to codify cyber laws, but there is little binding force in the real world.

- Disinformation operations and subversion are increasingly being recognised by state and non-state actors as being more efficient and less costly than conventional warfare or even diplomacy. Despite this recognition, it is unlikely there will be international understanding to deal with it soon.

- Fake news and disinformation is not static, it is evolving. For example, in Germany, the nature of fake news is changing, even as the state is trying to do useful things to try and counter it. This also means that the nature of fake news and disinformation will change further as actors will attempt to be subtler and look for new pain/pressure points to target.

- The legal regimes and legislation to manage DRUMS will also change and will have to be updated. These regimes must be future-proofed to develop systems to minimise the shocks and stresses of disinformation operations and the likes.

- The online space is unique in the sense that it is easier to bring people in to the system, but more difficult to bring people out. For example, individuals have been radicalised wholly online, but there are no known cases of people being de-radicalised wholly online.

- It is crucial for governments to take people into confidence, and directly educate them about the threats involved with DRUMS. DRUMS is increasingly turning into a national security issue. In Singapore, the nature of the government-people conversation has always been de-securitised, but this may change soon.

- Some of the best disinformation hybrid warfare campaigns take place well before they are identified. Therefore, the counter-action must take place equally early and further upstream.

Daniel Kimmage

- Information structures remain a black box. Algorithms are increasingly diversifying the user experience, making it harder for researchers to generalise across platforms. It is becoming more challenging to understand how we consume information.

- The commodification of the political space and its implications are also challenging to predict. The platforms that serve up our information, and the parties that have an interest in commercialising certain types of information, have put the world in an interesting situation.

- In this conference, there was not a comparable amount of research into the offline world. We are still seduced by data and the online world.

- There is still more analysis than solution. In the counter-terrorism world on the other hand, there are more solutions than actual research. The DRUMS problem is being approached the right way: conducting research first and offering solutions later.

- To understand a state actor, we need to look at propaganda and disinformation in the context of foreign policy objectives and political culture. It cannot be analysed in isolation. For example, as mentioned by Mr Andrew Radin from RAND, the overall foreign policy objectives of Russia in the Baltics must be analysed by including their disinformation tactics as a component.

- Many important solutions have been discussed during the conference: education, media literacy, exposure of techniques, and legal frameworks.

Arti Shukla

- Hazard and paranoia feed fake news, and it is being used excessively in political elections by politicians interested in gaining popularity. For example, these techniques were employed in the past Indian election, Brexit, and the most recent US election.

- Sometimes fake news is in the interest or short-term interest of a government. In the US and in the Indian media alike, there is an abundance of fake posts/trolls on social media being put up by government supporters. Hence there is a lack of government effort and will in this regard to deal with this issue.

- There is no single solution. The media, governments, and technology companies will have to come together to find solutions, while involving citizens. Citizens must be educated and made more aware of risks they face, and get involved in fact-checking. A multi-disciplinary and multi-organisational approach must be taken to effectively manage disinformation, if not eliminate it.

Daniel Fessler

- Education is key. Critical thinking skills are a 21st century goal for education.

- In the world of smart phones, public education is not just about learning things; it is about learning how to think about things.

- Arriving at one's own assessment of information is key, but this is not equivalent to arriving at one's own truth. There is a danger in teaching students that their own conclusions are as valid as others, because they risk ending up with alternative facts and realities – a post-modern world in which there is no objective truth. This would be a perverse outcome of an educational push towards critical thinking across the board. Thus, objectivism and positivism must be stressed alongside critical thinking.

- Assessments made by third-party organisations (think tanks and media organisations) are crucial. When potentially self-interested actors are the arbiters of legitimacy, consumers should adopt a perspective of scepticism. These third-party organisations play an important role in creating awareness, even though they lack sufficient resources to maximise their potential.

- Tech-giants such as Facebook and Google profit directly from users' use of information, and it is in their self-interest to protect the legitimacy of their platforms. When filter bubbles become extreme, the whole system will break down. Because of their public responsibility and profit-driven self-interest, these organisations should set aside a fraction of their annual profit in a blind trust administered by independent foundations to distribute it to fact-checkers.

- The credibility of independent fact-checkers should also be questioned. Organisations need to monitor and police each other for bias, for legitimacy to be enhanced.

- Publicly identifying how misinformation channels are being distributed disarms the actors. However, this carries the risk of abuse by government officials. For example, during the McCarthy era in US history, malicious actors targeted their political opponents under the guise of publicly airing the identities and agendas of hostile foreign agents.

- Governments need to maintain healthy freedom of press.

- State actors tend to be extremely sophisticated even if they appear not to be, as some of the scams/disinformation appear obviously fake. According to some economic analyses, such transparent scams tend to attract less intelligent readers, who are more likely to forward information.

Workshop Programme

Venue: Marina Mandarin Singapore
Taurus & Leo Ballroom, Level 1 (unless otherwise stated)

Monday, 24 July 2017

0800–0835hrs **Registration**

Venue : Taurus & Leo Ballrooms Foyer, Level 1

0835–0845hrs **Welcome Remarks** by ***Shashi Jayakumar****, Head, Centre of Excellence for National Security (CENS), RSIS, NTU*

0845-0945hrs **Panel 1: Why People Believe DRUMS**

Chair : ***Shashi Jayakumar****, Head, Centre of Excellence for National Security (CENS), RSIS, NTU*

Speakers : **Believing Chicken Little: Political Orientation Predicts Negatively-Biased Credulity in Americans** by ***Daniel M. T. Fessler****, Professor of Biological Anthropology, UCLA*

Suspicious Minds: The Psychology of Conspiracy Theories by ***Robert Brotherton****, Term Assistant Professor, Barnard College, Columbia University; and, Visiting Fellow, Department of Psychology, Goldsmiths, University of London*

Fake News: A Danger for Democracy or a Gift from Freedom of Speech? by ***Nicolas Arpagian****, Scientific Director of the Cyber Security Program, National Institute for Security & Judicial Studies (INHESJ – French Prime Minister's Office)*

0945–1000hrs **Networking Break**

Venue : MMB Foyer, Level 1

1000-1115hrs **Interactive Syndicate Discussions**

Syndicate 1

Venue : Capricorn Ballroom, Level 1

Syndicate 2

Venue : Libra & Gemini Ballrooms, Level 1

Syndicate 3

Venue : Pisces & Aquarius Ballrooms, Level 1

1115–1215hrs **Panel 2: State Actors and DRUMS**

Chair : ***Norman Vasu**, Deputy Head, Centre of Excellence for National Security (CENS), RSIS, NTU*

Speakers : **Denouncing 'Fake News' as a Social Control: China's Rumour Management Strategy on Social Media** by ***Fu King-wa**, Associate Professor at the Journalism and Media Studies Centre (JMSC), The University of Hong Kong*

Mapping and Understanding Information Actions in Cyberspace: The Case of the French Presidential Elections by ***Kevin Limonier**, Associate Professor at French Institute of Geopolitics (University of Paris 8); and, Scientific Director of the Russian-Speaking Infosphere Observatory (Castex Chair of cyberstrategy, National Institute for Advanced Defense Studies - IHEDN)*

The Power of Fake News: Gulf States Seek to Rewrite Rules Underlying International Relations by ***James M. Dorsey**, Senior Fellow, RSIS*

1215–1315hrs **Lunch**

Venue : MMB Foyer, Level 1

1315–1430hrs **Interactive Syndicate Discussions**

Syndicate 1

Venue : Capricorn Ballroom, Level 1

Syndicate 2

Venue : Libra & Gemini Ballrooms, Level 1

Syndicate 3

Venue : Pisces & Aquarius Ballrooms, Level 1

1430–1600hrs **Panel 3: Media and DRUMS**

Chair : ***Benjamin Ang**, Senior Fellow, Centre of Excellence for National Security (CENS), RSIS, NTU*

Speakers : **[RECORDING] Distinguishing Fact from Fiction in the Modern Age** by ***Andreas Schleicher**, Director for the Directorate of Education and Skills, OECD* followed by **Q & A** (10 mins)

Fake News: Who are the New Gatekeepers? by ***Han Fook Kwang***, *Senior Fellow, RSIS*

Global Engagement Center (GEC)'s Approach to DRUMS by ***Daniel Kimmage**, Acting Coordinator, GEC, US State Department*

Global Fake News and What the BBC is Doing to Combat It by ***Arti Shukla**, Assistant Editor – Asia, BBC Monitoring*

1600–1615hrs **Networking Break**

Venue : MMB Foyer, Level 1

1615–1730hrs **Interactive Syndicate Discussions**

Syndicate 1

Venue : Capricorn Ballroom, Level 1

Syndicate 2

Venue : Libra & Gemini Ballrooms, Level 1

Syndicate 3

Venue : Pisces & Aquarius Ballrooms, Level 1

1730hrs **End of Day 1**

1815–2030hrs **Workshop Dinner (By Invitation Only)**

Venue : Peach Blossom, Level 5

Tuesday, 25 July 2017

0800–0830hrs **Registration**

Venue : Taurus & Leo Ballrooms Foyer, Level 1

0830-0930hrs **Panel 4 : Information and DRUMS**

Chair : ***Norman Vasu****, Deputy Head, Centre of Excellence for National Security (CENS), RSIS, NTU*

Speakers : **Resilience in the Post-Truth World: Integrating Resilience in Defence Planning Against Information Warfare** by ***Janis Berzins****, Director, Centre for Security and Strategic Research, National Defense Academy of Latvia, Latvia*

The State of Fake News in Germany by ***Karolin Schwarz****, Founder, hoaxmap.org; and, Editor, correctiv.org*

Mapping Political News Ecosystems by ***Jonathan Albright****, Research Director, Tow Center for Digital Journalism, Columbia University*

0930–0945hrs **Networking Break**

Venue : MMB Foyer, Level 1

0945–1100hrs **Interactive Syndicate Discussions**

Syndicate 1

Venue : Capricorn Ballroom, Level 1

Syndicate 2

Venue : Libra & Gemini Ballrooms, Level 1

Syndicate 3

Venue : Pisces & Aquarius Ballrooms, Level 1

1100–1200hrs **Panel 5: Technology and DRUMS**

Chair : ***Muhammad Faizal****, Research Fellow, Centre of Excellence for National Security (CENS), RSIS, NTU*

Speakers : **Changes in the Social Media and Communications Landscape** by ***Alvin Tan****, Head of Public Policy, South East Asia, Facebook, Singapore*

How Democratic States Combat the Multidimensional Threat of Influence Operations by ***Jakub Janda****, Head, Kremlin Watch Programme; and, Deputy Director for Public Policy, European values Think-Tank, Czech Republic*

Computational Propaganda in China and Beyond *by* ***Gillian Bolsover****, Researcher, Oxford Internet Institute*

1200–1300hrs **Lunch**

Venue : MMB Foyer Level 1

1300–1415hrs **Interactive Syndicate Discussions**

Syndicate 1

Venue : Capricorn Ballroom, Level 1

Syndicate 2

Venue : Libra & Gemini Ballrooms, Level 1

Syndicate 3

Venue : Pisces & Aquarius Ballrooms, Level 1

1415–1515hrs **Panel 6: Hybrid Warfare**

Chair : ***Terri-Anne Teo****, Research Fellow, Centre of Excellence for National Security (CENS), RSIS, NTU*

Speakers : **NATO as an Alliance in the New Hybrid Warfare Environment – Amid Disinformation and Deliberate Twits** by ***Barbora***

***Maronkova**, Director, NATO Information and Documentation Centre, Ukraine*

(Mis)information Wars – the State of Play in Norway by ***Per Kristen Brekke**, Deputy Director, Norwegian Directorate for Civil Protection (DSB)*

Hybrid Warfare in the Baltics: Threats and Potential Responses by ***Andrew Radin***, Associate Political Scientist, RAND Corporation

1515–1530hrs **Networking Break**

Venue : MMB Foyer, Level 1

1530–1645hrs **Interactive Syndicate Discussions**

Syndicate 1

Venue : Capricorn Ballroom, Level 1

Syndicate 2

Venue : Libra & Gemini Ballrooms, Level 1

Syndicate 3

Venue : Pisces & Aquarius Ballrooms, Level 1

1645–1715hrs **Closing Panel / Moderated Discussion**

For this session, all participants and speakers will be able to discuss as a group some of the key issues and takeaways uncovered during the course of the Workshop

Chair : ***Shashi Jayakumar**, Head, Centre of Excellence for National Security (CENS), RSIS, NTU*

1715hrs **End of Day 2**

1800– 2030hrs **Closing Dinner (by Invitation Only)**

Venue : Aquamarine, Level 4

About the Centre of Excellence for National Security

The **Centre of Excellence for National Security (CENS)** is a research unit of the S. Rajaratnam School of International Studies (RSIS) at the Nanyang Technological University, Singapore.

Established on 1 April 2006, CENS raison d'être is to raise the intellectual capital invested in strategising national security. To do so, CENS is devoted to rigorous policy-relevant analysis across a range of national security issues.

CENS is multinational in composition, comprising both Singaporeans and foreign analysts who are specialists in various aspects of national and homeland security affairs. Besides fulltime analysts, CENS further boosts its research capacity and keeps abreast of cutting edge global trends in national security research by maintaining and encouraging a steady stream of Visiting Fellows.

For more information about CENS, please visit www.rsis.edu.sg/research/cens/.

About the S. Rajaratnam School of International Studies

The **S. Rajaratnam School of International Studies (RSIS)** is a professional graduate school of international affairs at the Nanyang Technological University, Singapore. RSIS' mission is to develop a community of scholars and policy analysts at the forefront of security studies and international affairs. Its core functions are research, graduate education and networking. It produces cutting-edge research on Asia Pacific Security, Multilateralism and Regionalism, Conflict Studies, Non-Traditional Security, International Political Economy, and Country and Region Studies. RSIS' activities are aimed at assisting policymakers to develop comprehensive approaches to strategic thinking on issues related to security and stability in the Asia Pacific.

For more information about RSIS, please visit www.rsis.edu.sg.

About the National Security Coordination Secretariat

The **National Security Coordination Secretariat (NSCS)** was formed under the Prime Minister's Office in July 2004 to coordinate security policy, manage national security projects, provide strategic analysis of terrorism and national security related issues, as well as perform Whole-Of-Government research and sense-making in resilience.

NSCS comprises three centres: the National Security Coordination Centre (NSCC), the National Security Research Centre (NSRC) and the Resilience Policy and Research Centre (RPRC).

Please visit www.nscs.gov.sg for more information.