RSIS WORKSHOP ON UNDERSTANDING AND COUNTERING ONLINE FALSEHOODS AND INFLUENCE OPERATIONS

Event Report

4-5 November 2019

RSIS S. RAJARATNAM SCHOOL OF INTERNATIONAL STUDIES
Nanyang Technological University, Singapore

NSCS NATIONAL SECURITY COORDINATION SECRETARIAT

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, Gulizar Haciyakupoglu, Terri-Anne Teo, Joseph Franco, Cameron Sumpter, Jennifer Yang Hui, Dymples Leong Suying, Eugene EG Tan, and Nazneen Mohsina.

Editors:
Gulizar Haciyakupoglu and Muhammad Faizal Bin Abdul Rahman

The panel sessions of the workshop are captured in the conference report with speakers identified. The syndicate discussions (Q&A sessions) are given without attribution.

TABLE OF CONTENTS

Executive Summary

The Centre of Excellence for National Security (CENS) organised the workshop on 'Understanding and Countering Online Falsehoods and Influence Operations' from 4 – 5 November 2019 at the Marina Mandarin Hotel in Singapore. The two-day workshop brought together nineteen speakers from different organisations including academia, think tanks, international organisations and grassroots movements and explored the topics of online falsehoods and influence operations with attention to the experiences of different countries.

'Understanding and Countering Online Falsehoods and Influence Operations' workshop focused on a wide range of issues concerning influence operations and aimed to capture the prominent debates in the field. The first panel set the context of the workshop and stretched the discussion from online falsehoods to influence operations. Building on this context, panels on day one discussed online falsehoods and influence operations in Asia and election meddling, respectively.

Both panels drew from cases from different countries. The panel on Asia discussed trolling against humanitarian efforts in the Philippines, information operations directed at Hong Kong, and the plague of online falsehoods in Sri Lanka. The panel on elections and information manipulation captured the variety of concerns related to information manipulation during the election period with references to the experiences of countries from different continents, including Brazil, Sweden, Indonesia, and Malaysia.

The second day of the workshop focused on the reception of online falsehoods, future concerns, and contemporary countermeasures. The panel on tactics, technology, and future concerns reviewed the technology and tactics leveraged in influence operations. It also explored potential future threats, including the advancement of deep fakes and whether they pose a significant threat within the grand scheme of malicious information manipulation efforts. The session on the reception of online falsehoods and inoculation allowed for a smooth transition from the supply side of the question to the reception aspect and countermeasures after

that. During this session, speakers unpacked the ‘psychology of misinformation,’ and shared methods of inoculation against misinformation with references to cases including anti-vaccination, and climate-change. The final panel of the workshop, ‘Countering Online Falsehoods and Influence Operations,’ reviewed various response measures. The speakers shared their diverse experiences with references to cases including experiences with equipping civil servants to counter disinformation campaigns, a media literacy programme at a high school in Finland and a grassroots citizen initiative in Lithuania.

The event attracted over two hundred participants from government agencies, academia, think tanks and representatives of foreign governments and allowed for fruitful exchanges and networking opportunities.

The key issues that the workshop had discussed were as follows:

1. **Russia and China are under the spotlight with their capacity to conduct influence operations**

The penetration of information technology, contrary to some expectations, has not democratised Russia and China. Instead, it equipped them with the tools to conduct 'hostile information operations.' While Russia and China both aspire to solidify their regime's power and 'decouple' the US and Europe in the economic arena, their political, economic, and regional goals and operation methods show differences. For instance, Russia bids to lift Western sanctions and have access to European financial support, while China wants to use the European market as a stepping-stone for economic and technological advances and pursuing its course of globalisation. While some of the 'Western' states have been primarily occupied with the Russian influence, China's ambitions on this front will likely receive more considerable attention in the near future.

2. There is an industry around social media manipulation

There are groups and entities offering “click” and “like” harvesting and disinformation dissemination as services. For instance, in Indonesia and Malaysia, local politicians and political parties leverage ‘cyber troops’ to circulate disinformation, propaganda, and other manipulated content, especially during the election period. Correspondingly, the primary culprit of the disinformation problem in Indonesia and Malaysia are the malicious acts of domestic actors rather than foreign influence operations. Akin to this, inauthentic accounts engage in trolling against human rights organisations in the Philippines. There are also cases of the trading of social media accounts. For example, an inquiry into the information operations directed at Hong Kong revealed that some dormant accounts became active during the operation, and some accounts showed signs of changing owners.

3. There is a wide variety of tactics leveraged in influence operations

Malicious actors leverage various tactics, including the cross-platform spreading of disinformation, algorithmic manipulation, click baits, and bots in their operations. The 'niche platforms' such as Tik Tok are gaining traction among hostile actors. The advancements in technology pave the way for the sophistication of tools, including bots. For instance, while earlier versions of bots would use a single language, sophisticated bots are multilingual. However, existing bot detection measures are not trained to catch such new generation bots. Deepfakes are yet another problem that became more concerning with the developments in technology. While Deepfakes may attract attention, their effect may remain limited, and over-emphasis on Deepfakes may deflect attention from the fundamental problems in the society that facilitate the penetration of disinformation. Additionally, hostile acts stretch beyond disinformation efforts. For instance, Russia capitalises on various measures in its influence operations on other countries including disinformation campaigns,

intelligence operations, and economic collaboration with political motives. Russia leverages multiple groups, including political allies, extremist groups, ethnic minorities, and non-governmental organisations in its efforts.

4. Capacity building and collaboration are essential components of the fight against influence operations.

The training of practitioners in government, civil society organisations, and others involved in the solution process is a primary step in drafting countermeasures. Strategic communication professionals are indispensable in the processes of disinformation identification, damage mitigation, and response construction and communication. The coordinated collaboration among different stakeholders of the solution process is crucial. For instance, Sweden, in its efforts to safeguard election from manipulation, held national operations forums that congregated diverse stakeholders from different industries involved in protecting election integrity, including the security sector and transportation agencies. Media literacy

initiatives also carry significant importance in equipping information consumers with the skills required to fight disinformation. A media literacy initiative in Finland, which incorporates the subject in the school curriculum and receives the support of the fact-checking institution *Faktabaari* is worthy of note. The effort not only equips students with the necessary skills to identify disinformation and consume trustworthy information but also trains educators with contemporary materials.

5. **The technology leveraged in countermeasures has to advance on par with the developments in malicious tactics.**

Current bot detection mechanisms fall short in identifying sophisticated bots. Also, algorithms are failing to identify trolling in a multilingual communication setting, where people use multiple languages interchangeably in their engagements. Current methods to locate disinformation include cyber forensics, ‘collective action theory,’ ‘identifying affiliations across networks’ and ‘coordinated clickbait and

colour theory based detection.' Open-source intelligence allows the tracing and identification of disinformation efforts. Some of the intelligence analysis tools practitioners can use in this process include geolocation, automated identification, software that helps detect bots engaging in information manipulation, and identification and analysis of inauthentic social media accounts and hashtags.

6. **The exploration of the psychological dimension of misinformation provides a window into how misinformation influences reasoning.**

With respect to this dimension, challenges to countering misinformation are threefold: (a) the employment of 'motivated reasoning' may result in "backfire' effect," (b) the attempt to discredit false information may kindle scepticism about and infringe trust in facts, and (c) the 'fluency of false claims' may increase. The methods of inoculation include: (a) 'fact-based method,' (b) method 'based on the use of logic,' and (c) leveraging trustworthy sources in the inoculation process. The 'psychology of misinformation'

has to be studied to create effective inoculation methods against misinformation.

Panel One: Online Falsehoods and Beyond: Influence Operations

The New Disruptive Media and Southeast and East Asia

Markku Juhani Mantila, Chief of Technical and Scientific Development Branch, NATO StratCom COE

Summary: Information manipulation is not a new instrument of conflict and foreign interference, but social media has made it more efficient and affordable. Information manipulation transforms from the application of soft power to sharp power when it shifts from persuasion to destabilisation.

- Information manipulation has been an instrument of conflict for centuries. Britain had used information manipulation to frame the World Wars against Germany as justifiable to gain the support of the Americans. The US and Soviet Union had

used information manipulation among other foreign interference measures during the Cold War. Information technology has not transformed Russia and China into democratic states but instead gave these authoritarian states new tools for hostile information operations.

- The Russian annexation of Crimea in Ukraine was the wakeup call that roused the West to the seriousness of hostile information operations as one of the hybrid threats that emanate from hostile foreign states. Russian information operations during the 2016 US presidential election demonstrated the threat of information manipulation as part of covert influence campaigns by hostile foreign states. Information manipulation is again the new normal in geopolitical contestations.

- An ecosystem of technology companies openly sells Clicks and Likes on social media as a service to maximise the reach of dissemination of falsehoods. This service offers several options at different

prices based on the number of Likes. Most of these companies are purported of Russian origin. Given that people today are hyper-connected on the digital space, authoritarian states have been quick in adopting social media for information operations to influence the masses both domestically and abroad.

- The largest digital media market in the world is in Asia, where China has the most significant share in terms of numbers of TV channels, journalists and WeChat users. China's considerable share of the digital media market enables it to use information to project a significant international presence in building its soft power or using its soft power coercively as sharp power when necessary. While Russia uses information manipulation more as a blunt force to break, hack, harass and confuse its target audience, China uses information manipulation more surgically and surreptitiously.

- The preoccupation with Russian information operations has left the West with inadequate bandwidth to monitor and

confront Chinese information operations. This situation is likely to change, given growing suspicions of China’s intent and influence campaigns beyond its borders. The risks from China's influence are increasing as the West becomes more dependent on Chinese capital and China dominates the 5G technology. Stronger relations between China and Russia could also enhance both states’ capabilities to conduct hostile information operations.

Information Operations and Psychological Operations: Selected Model

Kamil Basaj, CEO INFO OPS Poland Foundation

Summary: The information environment is also a cognitive environment. The ability to manipulate information and the perception of information can be used in disinformation efforts to influence the decision-making processes of individuals and social groups. Disinformation is the art of social manipulation that the Russians had been developing since the 1950s.

- Research on Russian academic data in the field of psychological and information manipulation had uncovered the algorithm of manipulation. This algorithm uses models of subjectivism to build false pictures of reality. Analysis of human behaviour and experience enables hostile actors to understand how the target audience perceives the reality around them. Different individuals may perceive multiple reflections of reality in the same environment. This condition is a psychological vulnerability that hostile actors could leverage for disinformation campaigns.

- Russia conducts disinformation campaigns in the physical, virtual and cognitive environments, which collectively affects perceptions of reality. Reconnaissance of these environments could enable information-gathering of the activities of hostile actors to profile the thinking patterns of the target audience. Hostile actors would use knowledge of the target audience's thinking patterns to plan disinformation campaigns. These campaigns may firstly entail using false

information and secondly manipulating the transmission of real information to exploit the target audience's thinking patterns.

- The process of analysing Russian disinformation campaigns entails mapping the distribution of propaganda in the information environment. In propaganda, separate narratives that are seemingly unconnected could converge to influence the target audience's perceptions of an issue. Russia's narratives could firstly originate from its news sites and then multiply in various websites. Secondly, the network of blogs could widen the circulation of narratives. Thirdly, the exchange of opinions in social media, including by inauthentic accounts, could further amplify the popularity of the narratives and obscure its Russian origins. The outcome is a toxic information environment where social media and search engine algorithms make these narratives more accessible to Internet users. The ultimate phase is a more targeted campaign to influence specific events and individuals.

- Defence against disinformation campaigns is a multi-phase process. Firstly, there should be an analysis of the content, its distribution patterns and cognitive impact, and how the content could evolve. Secondly, there should be an anticipation of the hostile actors' possible next steps, their sequence and associated risk scenarios. Thirdly, there should be an analysis of similar disinformation campaigns in other states to determine the potential negative impact that could happen locally. This process could facilitate the early detection of disinformation campaigns and implementation of defensive measures.

Russian and Chinese Influence Operations in Europe

Veronika Víchová, Head, Kremlin Watch, European Values Think Tank

Summary: Russia has attempted to interfere in the domestic politics of European states, especially after its annexation of Crimea. The growing influence of China in Europe is also raising concerns about foreign interference in Europe. In countering influence operations,

there is a need to identify similarities and differences between Russian and Chinese approaches.

- Russia uses seven tools to influence the domestic affairs of other states: (1) disinformation operations; (2) intelligence operations; (3) relevant political allies; (4) non-governmental organisations; (5) radical and extremist groups; (6) parts of ethnic minorities; and (7) politically-motivated economic cooperation. Disinformation does not happen in isolation but conjunction with other tools of influence operations.

- Russia is proficient in identifying vulnerabilities in the states that it targets. Russia, therefore, uses different combinations of the seven tools to target the vulnerabilities - such as emotive issues – of different states in influencing policymakers and the public. Political allies could play the role of translating Russian disinformation into local languages. Disinformation and political allies may promote Russia but more importantly undermine local democratic

and regional institutions – such as the European Union (EU) and North Atlantic Treaty Organisation (NATO) - and people's trust in these institutions.

- The process of state capture that Russia employs comprises four phases: (1) influence; (2) strategic deal; (3) partial elite capture; and (4) soft regime change. Ideological proximity, financial interests and media support could be entry points for influence. Pro-Russia politicians who rose to power and make economic deals with Russia in critical infrastructure sectors could pave the way for a strategic deal. Russia could use disinformation to paralyse political opposition and use strategic corruption on local politicians to achieve partial elite capture. States that incorporate Russian influence in its national policies and regional engagements are susceptible to soft regime change.

- The differences in Russian and Chinese influence operations are in their political objectives, economic goals, regional goals and modus operandi. Politically, both

Russia and China aim to cement their regimes' power. While Russia seeks to limit the threat of domestic revolution, China seeks to legitimise itself in the international space. Economically, both Russia and China aim to decouple the US and Europe. While Russia tries to end western sanctions and gain European financial sponsorships, China seeks to leverage the European markets as a springboard for economic and technological gains and its vision of globalisation.

- Regionally, Russia seeks to (1) strategically co-opt Germany and France by exploiting domestic anti-US sentiments; (2) increase Eastern European oligarchs' dependence on Russia; (3) establish a belt of neutral or puppet states in central Europe; and (4) end the presence of NATO and EU in the West Balkans. China's regional goals are not clearly defined, but it seeks to: (1) expand its technological presence – 5G – in Europe; and (2) cultivate certain western states as proxies of the Chinese Communist Party (CCP). In achieving

these goals, Russia has exhibited more openness and quantity in its influence operations, reaching out to far-right and far-left groups, and using multiple channels of disinformation to spread falsehoods. China, however, has been more aggressive in public diplomacy, reaching out to the political mainstream, conducting politically-motivated economic operations, and using disinformation to spread a grand narrative of China's peaceful rise.

Syndicate Discussions

Issue: Objectives of disinformation operations. Disinformation may complement the soft power instruments that foreign states use to influence opinions. Disinformation can also divert public attention to issues that malicious foreign states are exploiting to disrupt the target state. Russia and China use disinformation for both objectives of building soft power and disrupting target states.

Issue: Ethical use of information operations for building influence. Three essential principles underpin the ethical use of information operations. Firstly, the narratives and associated literary tools that are used must be based on truths. Secondly, the operations must be transparent in its source and affiliations. Thirdly, the operations must benefit the target audience and not impose limitless influence over them.

Issue: Countermeasures against disinformation. Countering disinformation requires a multifaceted approach. This approach would include measures to (1) protect the media environment; (2) active measures such as strategic communications to monitor, investigate and debunk online disinformation; and (3) deter disinformation through punitive measures such as laws and economic sanctions against hostile states. Also, society needs to build up its resilience against disinformation.

Issue: Building resilience against disinformation. Societal resilience against disinformation would require (1) establishing openness in discourse on difficult issues, (2) leaders and influencers in every country speaking up against fake news and raising awareness about its dangers, (3) promoting quality media that is free and independent; and (4) implementing good primary education to equip the youth with critical thinking skills and media literacy.

Issue: Building and emphasising the strengths of an open society. A society that has a higher degree of openness, acceptance and tolerance of socio-political differences would be more resilient against disinformation. These societal attributes may reduce the opportunities and vulnerabilities that malicious actors can exploit to destabilise a society. Social media companies can support open societies by helping to expose the source of fake news and promote awareness of its dangers.

Issue: Understanding the psychological behaviour of social media users. The process of building the psychological and behavioural profiles of individuals is necessary to understand why they would engage with certain online disinformation narratives. This process requires analysing the decision-making process and attentive retention models of the individuals.

Issue: Social media profiling may help in targeting vulnerabilities of social media users. The use of data gleaned from social media enables the psychological profiling of individuals and their cognitive vulnerabilities. Profilers from the military sector can build an accurate picture of target groups as a lower cost. These profilers may target targeting pro-defence groups or individuals who have expressed interest in geopolitics.

Issue: Russia and China learn from each other's disinformation tactics. Russia and China learn from each other by experimenting with tactics that work. Russia emulates China's tactics against Taiwan for social media trolling in Europe. China follows Russia in using various financial means to target

politicians, populists and journalists in its influence operations. In the future, Russia and China may cooperate in disinformation operations primarily in the Balkans states where both powers are active.

Distillation

- Information operations serve primarily political objectives, including malicious ones. In countering disinformation, it is useful to distinguish between those that come from hostile foreign states and non-state actors; and those that non-state actors spread but can benefit state actors.

- Countering disinformation requires measures in both the digital and non-digital spaces. Measures such as strategic communications, fact-checking, laws and cooperation with social media companies address the digital space while building societal resilience and collaborating with the civil society to build trust address the non-digital space.

- Hostile foreign states that engage in disinformation campaigns and influence

operations are learning from each other's tactics and can potentially cooperate in the future. This cooperation poses a national security challenge that target states should monitor closely.

Panel Two: Online Falsehoods and Influence Operations in Asia

Activism Trolled: Why Human Rights Groups Are Losing the Disinformation Battle Online

Aim Sinpeng, Lecturer, Department of Government and International Relations, University of Sydney

Summary: The trolls target human rights organizations in the Philippines, including the Human Rights Watch Philippines, Amnesty International Philippines, and the Commission on Human Rights. Algorithms fail to identify trolling behaviour online because of the switch between languages in conversations. The governments in Southeast Asia rely on judiciary or law in their countermeasures.

- Trolling is an anti-social behaviour targeted at interrupting engagements and kindling conflict in online groups. Bad mood and earlier exposure to trolling acts can trigger trolling behaviour even in

individuals who claim they would not pursue trolling behaviour. The studies that explore trolling in relation to disinformation have analysed the acts of paid and unpaid human trolls and bots.

- The content analysis of 3-year Facebook data on Human Rights Watch Philippines, Amnesty International Philippines, and Commission on Human Rights (3,000+ posts) demonstrates that the human rights organizations in the Philippines are subject to trolling and negativity online. Inauthentic accounts with trolling behaviours engage with non-troll, human-managed accounts, and they seek to dominate the discourse and trigger more trolling by being the first commenters on issues

- Algorithms are failing to identify trolling behaviour in multilingual communities as the individuals switch between languages during their engagements. The algorithms are trained to analyse a single language conversation.

- Some of the government-led measures against disinformation in Southeast Asia pursue a truth-centric approach. They leverage judiciary or law enforcement in their efforts. The punishments involve hefty fines for individuals or companies.

Tweeting through the Great Firewall

Tom Uren, Senior Analyst, International Cyber Policy Centre, Australian Strategic Policy Institute (ASPI)

Summary: Some of the accounts employed in the information operations (IO) directed at Hong Kong have been active before the protests, and some accounts showed signs of a change in owner during the accounts lifetime. The intensity of the IO against Guo Wengui surpassed the IO directed at Hong Kong. The accounts targeting Daryl Morey, on the other hand, followed the work hours of Beijing, suggesting a possible link with the state.

- Twitter released data on information operations (IO) directed at Hong Kong in August 2019 in two streams. An analysis of the first wave of the data set revealed

that some of the accounts used in the operations have been active since 2017, and the tweets of these accounts were in different languages. The tweets in Chinese appeared after mid-2017.

- There was evidence of the trading of some of the accounts used for IO directed at Hong Kong. For instance, 630 tweets involved phrases such as ‘test new owner,’ ‘test,’ ‘new own,’ and others. Also, some of the accounts were dormant for an extended period before they started tweeting in Chinese and other languages. The main themes propagated by the accounts included criticism of the protestors, support for the law based order and Hong Kong police forces, and allegations of Western intervention in the protests.

- The allegedly PRC-linked campaign against Guo Wengui surpassed the IO directed at Hong Kong. Guo Wengui (Miles Kwok) shared a series of accusations against the Chinese government while Beijing accused him of corruption. Guo Wengui, who fled to the

US, was also accused of being a PRC spy in 2019.

- The Twitter data-set was also analysed to understand information activities against Daryl Morey following his tweet in support of the protestors in Hong Kong. Among others, IO initiated after Morey's tweet was employed to defend actions taken against the NBA. The orchestrators mobilized IO in combination with economic power to create a chilling effect.

- Some of the accounts engaged in the operation following Morey's tweet did not have any followers, some had not tweeted before, and some of them were new accounts. Most of the accounts during the period of Morey's tweet were not very active. The tweets were parallel to the ones used against the protests in Hong Kong.
- The nature of the IO led to the assumption of state involvement, although confirming this claim is challenging. The accounts engaged in IO following Morey's tweet were operating under the work hours of

Beijing with low activity during break times and public holidays.

The Rumor Mill of Sri Lanka: Lessons in Countering Misinformation

Yudhanjaya Wijeratne, Senior Researcher, LIRNEasia

Summary: The blocking of Facebook to prevent the circulation of disinformation and hate speech may fail to prevent netizens from accessing the platform, as seen in the example of Sri Lanka. Lack of clarity on the issue may fuel conspiracy theories. People in communities may leverage their connections to help spread counter-narratives to fight disinformation in WhatsApp.

- Sri-Lanka suffered from a racially charged mob attack in March 2018. Following the attack, the government blocked Facebook. While the Facebook activity plummeted on the day of the block, Google search for VPN increased, and Facebook activity climbed back to the previous levels in a short period.

- A look into the bot activity following the March 2018 attack showed that the bots were not active before they engaged in the dissemination of negative narratives on Muslims. The bots are getting smarter. For instance, while earlier versions would tweet in one language, advanced bots are multilingual. Current mechanisms of bot detection are not trained to identify such advanced bots. The bot activity is also becoming visible on Facebook.

- In April 2019, following the bomb attacks to churches and hotels, the government first kept silent and then stated that it had not received information while police forces argued that they provided the government with information on the attacks. This lack of clarity gave way to conspiracy theories. One such conspiracy theory claimed that Muslims were poisoning the water.

- The disinformation was spreading primarily through WhatsApp in the aftermath of the 2019 attacks as Facebook was blocked, and individuals were turning to VPN.

- The Watchdog was born in within thirty-six hours following the 2019 bombings. As a fact-checking group that comprises a multidisciplinary team of citizens, it monitors social media for hoaxes and debunk them. The group mobilized connected people in communities to spread counter-narratives to combat disinformation in their WhatsApp groups.

- The disinformation that went into circulation was variations of 59 persistent narratives. For example, disinformation on sterilization emerged in different forms in 2012, 2014, and 2019. There are various groups in the Telegram that create such sticky content.

- Political speech, misinformation, and fake news are interwoven. For instance, agents package politicians' speech into a meme in a telegram group, the meme gets viral in WhatsApp and then migrates to Facebook.

Syndicate Discussions

Issue: Trolling is growing into an industry. Trolling has evolved into an industry unto itself. For instance, troll farms have been known to operate in the Philippines, and some of the employees have backgrounds in public relations, human rights, and digital media. The trolls' tactics could include drowning out the conversation and diverting attention away from the topic. The trolls could share trolling tactics with ordinary people (non-trolls) and influence them to become trolls. Essentially, trolls spread anti-social behaviour.

Issue: There are multiple impediments to curbing hate speech online. Some of the issues include (1) too clear definitions, (2) language barriers, and (3) lack of stringent laws. (1) Clear definitions obstruct the fight against hate speech. A lot of hateful content on social media platforms is not taken down due to the specific/rigid classification and definition of hate speech. (2) Although platforms like Facebook are trying to curb hate speech, the nuances of different

languages often become barriers whereby the meaning often gets lost in translation of languages to English, making it difficult to understand if something is hate speech. (3) As to legal action, there is minimal cooperation on policy level regarding anti-hate speech laws.

Issue: Journalistic networks may allow fact-checked information to reach a broader audience. Disinformation could spread widely by the time fact-checkers conduct their due diligence. A trustworthy network of journalists can contribute to effectively reducing disinformation and misinformation online. For instance, journalists focused on verifying information on-the-ground during the aftermath of the Sri Lankan bombings in 2019. Journalists and activists were able to accurately and efficiently refute disinformation and misinformation through multiple online and digital platforms. While it is not always possible to fact-check disinformation conducted by politicians, it is an effective measure for verification on the grassroots level.

Issue: Effectiveness of legislative tools. The Sri Lankan Data Protection Act, which is modelled after Singapore's Personal Data Protection Act (PDPA) – is currently being tabled in Sri Lanka's Parliament. Legislations can inhibit motivations to disseminate disinformation.

Issue: Economic pressure adds efficacy to social media activism. Using social media to agitate for actions alone may not garner much attention. Combined with economic actions, however, online activism could have much more impact. An information operation could combine social media activism with economic pressure to justify further action for political agenda.

Distillation

- Trolling has graduated into an industry that infects online conversations and personas.

- Hate speech covers many forms of expressions, which spread, incite, promote or justify hatred, violence, and discrimination against a person or group

of persons for a variety of reasons. As such, using a stringent definition of hate-speech would be ineffective. Instead, it needs to be comprehensive.

- Adhering to stringent definitions of what hate-speech entails, language barriers, and lack of strict laws impede efforts to curb hate speech online.

- Social media activism alone may fail to achieve the desired outcome. Social media activism, coupled with economic pressure, may help such activism gain traction.

- Close collaboration and inherent trust with journalists and the media to act as the ‘fourth estate’ can contribute to combatting disinformation.

Panel Three: Elections and Information Manipulation

Swedish Experiences of Protecting an Election

Fredrik Konnander, Head, Counter Influence Branch, Global Monitoring and Analysis Section, The Swedish Civil Contingencies Agency (MSB)

Summary: Sweden's efforts to protect its elections leverage close coordination and collaboration between government stakeholders and private institutions such as the media. These efforts come in the backdrop of attempts by foreign powers to influence elections in several western states such as the US and France.

- Swedish institutions such as the MSB closely monitored two recent elections. The 2018 Swedish national elections and the 2019 European Parliament elections were potential targets for influence operations. For Sweden, cyber attackers have a smaller attack surface to breach the elections systems as the Swedish

electoral process is decentralised and mostly manual. Only the consolidation of counts at the regional level is computerised.

- The MSB monitors several types of possible election interference. Firstly, malign actors may attempt to undermine the electoral process by targeting the validity of poll outcomes. Secondly, influence operations may try to sway voters' political preferences or diminish their motivation to vote. Thirdly, influence operation may attempt to subvert politicians.

- Unlike other countries such as the US, France, and Germany, Swedish elections appear to be more secure. The MSB laid the groundwork early to identify potential influence operations and develop countermeasures. Transparency and the involvement of stakeholders such as the media played a significant role in alerting the public to the threat of influence operations.

- The MSB stresses that elections security is a continual effort, and there are valuable lessons. Firstly, capacity building for countermeasures should be a priority instead of ad hoc initiatives. Secondly, coordination among government stakeholders should be increased. Increased coordination includes organising national operations forums that bring together stakeholders from the security sector up to the transport agencies that deliver the physical ballots.

From Misinformation to Extremism: How WhatsApp is Affording Radicalization in Brazil

David Nemer, Assistant Professor, Media Studies Department, University of Virginia

Summary: The use of online ethnography revealed that WhatsApp drives the social infrastructure of misinformation in Brazil. President Jair Messias Bolsonaro won the Brazilian elections as his supporters had spread misinformation through WhatsApp groups, which still serve as platforms for the radicalisation of right-wing Brazilians.

- Ninety-six per cent of Brazilians who own smartphones use WhatsApp as a messaging platform. WhatsApp became the favoured tool of pro-Bolsonaro voters in Brazil to help their candidate win the presidency. Specifically, WhatsApp groups became a potent tool for the dissemination of misinformation.

- Misinformation spreads through a structure of groups resembling a pyramid. Pro-Bolsonaro partisans create invite-only WhatsApp groups, which were heavily promoted in other platforms such as conservative online forums or YouTube channels. The electorate was divided into three broad categories, and ordinary Brazilians comprised the vast majority. Mistrust of mainstream media drove them to subscribe to pro-Bolsonaro WhatsApp groups mainly to view political rumours and share memes.

- "Bolsominions" are the other category that populates the social infrastructure of misinformation. These are individuals who form a local volunteer army to actively

disseminate misinformation across online platforms and without concealing their political leanings. Finally, the “influencers” are the category who worked behind the scenes to create fake content that the “Bolsominions” and ordinary Brazilians share online.

- Ten months after the elections, Bolsonaro’s base had fragmented into a loose coalition of about ten big groups. WhatsApp had transitioned from being a platform for elections-related misinformation to a platform for right-wing radicalisation.

- Three types of right-wing groups operate in Brazil. Firstly, the “propagandists” distribute propaganda that promotes the perceived accomplishments of the current presidency. Secondly, the “social supremacists” are a subset of Bolsonaro supporters who espouse political views that condone Nazism or advocate for pro-gun ownership laws. Thirdly, the “insurgents” criticise Bolsonaro for being insufficiently radical and call for the return of military rule in Brazil.

Drivers of Election Disinformation in Indonesia and Malaysia

Ross Tapsell, Senior Lecturer and Researcher, College of Asia and the Pacific, Australian National University (ANU)

Summary: The main drivers of disinformation in Indonesia and Malaysia are not foreign influence operations but malign domestic actors. Local politicians and their political parties fund groups and teams of “buzzers” and “cyber troopers” to spread disinformation as part of the campaigning during the election period.

- Research on Malaysia and Indonesia uncovered that the main drivers of disinformation are groups that local politicians and their political parties had funded. Therefore, countermeasures against disinformation should be recalibrated to focus less on foreign actors. In formulating policy solutions, stakeholders should reduce the use of the language of war and armed conflict to frame the problem of disinformation.

- The media oversimplifies disinformation in its coverage of this complex problem in Southeast Asia. The media used Russian election interference for comparison and swapped it for China to describe the issue in Southeast Asia. The media ignores the distinct ecology of election-related disinformation actors in Southeast Asia. This ecology depends more on domestic expertise instead of external big data companies. There is a blurring of lines between a legitimate social media campaign and disinformation.

- Social media does not inherently support authoritarianism as seen in Malaysia, where "cyber troopers" were unable to preserve the Barisan National (BN). In Indonesia, discussions to unravel issues perceived as “hoax news” dominate the social media space. The “weaponisation” of social media for electoral campaigns as a narrative should be viewed with caution. “Weaponisation” can be a pretext for governments to pass draconian laws that stifle legitimate dissent.

- It is more prudent to enhance the citizens' understanding of legitimate sources of information instead of advocating for regulations on social media use and digital advertising. Policies on media literacy should distinguish between "old media" and social media. Unlike the "old media", social media disseminate information through a "culture of sharing." The "attention economy" in social media incentivises the creation of viral content.

Understanding and Countering Online Falsehoods

Ismail Fahmi, Founder, PT Media Kernels Indonesia

Summary: Indonesian elections over the past five years have seen more incidences of computational propaganda and activities by the so-called "cyber troops." Computational propaganda and "cyber troops" amplify political content and falsehoods to manipulate public opinion.

- Indonesian elections over the past five years have seen more incidences of

online falsehoods. Political personalities enlist “cyber troops” and computational propaganda to spread political content, propaganda, hoaxes and fake news. Besides the political personalities and parties, the government and military also use “cyber troops” to influence public opinion.

- Influence operations on social media seek to sway perceptions by amplifying partisan content, distributing disinformation and promoting hateful speech. For example, a coordinated hashtag campaign had targeted the Indonesian anti-corruption commission. Bots and human-operated accounts hijack hashtags – such as #giveaway that non-political influencers and other legitimate digital marketers use – gain more reach.

- “Cyber troops” have also targeted citizen-level initiatives – such as MAFINDO or the Indonesia Anti-Slander Society - to counter falsehoods. Social network analysis of re-tweets of MAFINDO's content reveals that Indonesians continue to harbour a distrust of the movement

despite its active attempts to be non-partisan.

- Mainstream media still has a pivotal role in the era of social media; and should embrace its functions as the primary conduit for “information arbitrage,” and as a bridge between polarised networks of contending political groups. In a “post-truth” world, the mainstream media can reduce the dissemination of false news through fact-checking. The mainstream media can use their social media platforms to debunk fake news.

Syndicate Discussions

Issue: Regulation of closed encrypted messaging platforms. WhatsApp has limited the number of messages that users could forward, but it can do more. While social media companies insist that they are unable to access the content on their encrypted platforms, they do have access to user metadata that can provide insights into user communication. The lack of financial incentives stops technological companies from doing more to counter disinformation

unless media expose threatens their reputation.

Issue: Social media companies and regulators are often at loggerheads. Social media companies are becoming increasingly influential in their ability to define their role in the spread of narratives. These companies can exercise flexibility in setting their business areas, vis-à-vis compliance regimes to protect their corporate interests. For example, Facebook defines itself as a broadcaster instead of a news outlet to comply with specific regulations.

Issue: Social media companies can be partners in combating disinformation. States may set up hotlines with social media companies to improve the process of detecting and removing disinformation. More legislation may not enhance the level of cooperation between the state and the companies. While laws in democratic countries cannot restrict discourse on social media, the companies' terms of service and community standards are useful tools to take down disinformation.

Issue: Evolution of modus operandi of fake accounts. The methods of using fake accounts for spreading disinformation are evolving. For example, the large amount of resources available during the 2019 presidential election in Indonesia ensured that there were ample funds to hire “cyber troops.” Following the election, fake accounts emulate the K-Pop method of giving away Twitter fans to expand their network.

Issue: Measures against disinformation in political mudslinging. Countering disinformation is an uphill task because politicians of all camps in many countries accuse one another of using fake news. All political parties should increase their awareness of political communications by receiving briefings on how to recognise information operations and the countermeasures. Additionally, the Swedish example of psychological defence entails establishing an agency of journalists and editors to improve the population’s resilience against disinformation.

Issue: Overemphasis on foreign interference in elections in Asia. There is no concrete

evidence of foreign state actors interfering in the local elections of Asian countries. However, the Indonesian government regards the support by Melanesian groups from the Pacific islands for West Papuan independence activists as foreign interference. Activism happens in many countries and should not be considered as foreign interference. Instead, there should be efforts to understand better the neo-colonialist issues that activist groups seek to address.

Issue: Disinformation against media literacy efforts. Disinformation has targeted efforts to improve media literacy efforts. For example, far-right groups in Brazil have used radical videos to discredit media literacy videos and circulate their version of media literacy to their supporters via WhatsApp. In the same vein, hoax busters are less effective if they are affiliated with the government that faces the problem of public distrust. Therefore, there should be more conversations between the government, hoax busters and the broader civil society in promoting media literacy.

Issue: Political communications in democracies are evolving**.** In the Philippines, political campaign teams continue to function instead of taking a respite until the next electoral cycle. This continuous operation blurs the lines between election campaigning and state-backed information operations. In Indonesia, hashtags are critical in gaining more clicks, and people avoid flame wars by using re-tweets instead of their twitter accounts to discuss political issues. In democracies, it is increasingly important to distinguish between narratives that are legitimate criticisms and those associated with foreign interference.

Distillation

- Foreign interference needs to be well-defined and take into consideration what a specific country regards as acceptable and unacceptable activities by external actors. Political communication in democracies are evolving, and there is a need to distinguish between narratives that are legitimate criticisms and those associated with foreign interference.

- Social media companies have more insights into user data than what they publicly acknowledge. There should be continuous efforts to persuade these companies to prioritise addressing disinformation on their platforms instead of only focussing on profits. Inadequate efforts by social media companies risk mainstreaming disinformation and delegitimising credible news sources.

- Better critical thinking skills and media literacy are needed to enhance public resilience against disinformation. The public should be educated on how the social media landscape operates differently in various countries and regions. More legislation may not improve cooperation with social media companies or enhance public resilience against disinformation.

- There should be more conversations between the government, media, hoax busters and the broader civil society in promoting media literacy. These conversations are necessary in a post-truth world where the lack of public trust

results in fact-checkers and the media being perceived as government propaganda tools.

Panel Four: Tactics, Technology and Future of Online Falsehoods and Influence Operations

Getting Real About the Deepfake Threat

Tim Hwang, Lawyer and Researcher, and the Former Director of the Harvard-MIT Ethics and Governance of AI Initiative

Summary: Deepfakes are a growing concern due to advancements in artificial intelligence (AI) and its subset - machine learning (ML). However, the threat of cheap fakes remains. Cheapfakes are useful for propagandists who are pragmatists, and AI may not understand the context to create believable content. Furthermore, technology to detect Deepfakes is also improving.

- Deepfakes are dramatic, but their ultimate impact may be limited. Focussing on deepfakes may distract us from the underlying issues that affect society. Furthermore, deepfakes have their

limitations despite improvements in ML. A technical understanding of how deepfakes work can support analysis of its threat and how to counter it.

- Cheapfakes remain as a threat given three arguments. Firstly, propagandists are pragmatists. They would expend the lowest amount of effort to spread disinformation if it fulfils their objectives. There may be less need to use deepfakes if cheap fakes are sufficient to achieve their goals of spreading chaos in society.

- Secondly, AI has improved substantially, but it cannot understand the context. AI may improve the puppets but not the puppeteers. The use of media forensics to investigate contextual clues in video content can aid in identifying deepfakes. Human input and strategy, therefore, remains necessary to create and spread credible falsehoods.

- Thirdly, researchers are improving the means and methods to detect deepfakes. Advancements in deepfake detection may be keeping up with advancements in

deepfake creation. Large quantities of data are needed to create credible deepfakes. The lack of quality images may hamper the quality of deepfakes, thus, making them easily identifiable.

- The anxiety over the threat of deepfakes may be larger than the actual impact that the threat poses. Deepfakes are not new and existed since the computer market introduced the Photoshop software back in the 1990s. Instead of focussing on the image of deepfake, it may be more important to focus on the person behind the image and the cognitive and social factors that make people susceptible to falsehoods.

Deviant Mobs of the Internet: Tactics, Techniques and Procedures

Nitin Agarwal, Jerry L. Maulden-Entergy Endowed Chair and Distinguished Professor, University of Arkansas at Little Rock

Summary: Trends in disinformation campaigns include cross-platform orchestration and the use of niche platforms, coordination and exploiting blogger

communities, and algorithmic manipulation. Techniques to identify disinformation include collective action theory, cyber forensics, identifying affiliations across networks and coordinated clickbait, and colour theory based detection.

- Trends in disinformation include cross-platform orchestration and niche platforms like Tik Tok; coordinated click baits and exploiting blogger communities in flash-mob style; and algorithmic manipulation to manipulate search results and content ranking. Social media organise individuals into groups, groups into crowds and crowds into mobs. Botnets behave like communities when they demonstrate coordination and complexity in their behaviour.

- Social media companies should be more proactive in building collaborative networks of practitioners, researchers and policymakers. Media literacy programmes and more dialogue on cybersecurity and cyber diplomacy can support efforts to counter disinformation. Tools such as blog-trackers and YouTube-trackers can

monitor, track and identify influential online content and behaviour that are indicative of disinformation.

- Online deviant groups use botnets, commentator mobs, blog farms, coordinated clickbait and algorithmic manipulation to amplify their disinformation campaigns. Collective action theory can support the analysis of how online deviant groups operate. The theory provides a model for understanding how groups coordinate themselves in online platforms. Current efforts to counter disinformation that use this theory include the active tracking of anti-West, anti-EU, and anti-NATO online groups.

- Cyber forensics can help in the extraction and analysis of metadata such as web traffic tracker codes, email addresses, IP addresses, contact details, names under which the domain is registered and other digital signatures. The process of identifying affiliations across blogs and social media platforms can improve the understanding of how influential networks

are and how they operate across platforms.

Bots, disinformation and foreign meddling in the digital space

Lukas Andriukaitis, Associate Director, Digital Forensic Research Lab (DFRLab), The Atlantic Council

Summary: Open-source intelligence can support democracy by tracking events, identifying and exposing online disinformation. Intelligence analysis tools include the use of geolocation, automated identification and analysis of fake social media accounts, software to spot bots that are attempting to sway public opinion, and identifying unnatural hashtags on social media.

- Open-source analysis has certain advantages such as (1) accessibility, (2) unclassified information that can be shared, and (3) the analytical methods can be imparted through training. In countries where there are imminent elections, open-source analysis happens alongside the training of journalists and

coordination with media outlets. Coordination with media outlets is necessary as their different ideological leanings would result in them framing news differently.

- Geolocation is an open-source tool that is useful for tracking conflict. Geolocation provides an understanding of where an event actually took place. Tools that complements geolocation, including mapchecking.com and cross-referencing data from satellite imagery, street views, photos taken by drones can help determine how many people were present during events such as protests.

- Open-source analysis can help discover "what really happened." Geolocation was useful in examining the events that occurred during the Syrian conflict. For example, the Russians denied it when the Syrian Observatory pointed to the presence of the Russian military at the area where an airstrike killed 53 Syrian civilians in 2017. What actually happened during the airstrike and where it happened was determined by cross-referencing

video images with maps and other social media data.

- Bots have both benign and malicious uses. Malicious bots can be spotted if they attempt to sway public opinion by making an issue appear more popular than it actually is. The DFRLab has developed 12 methods to spot a bot and its time of creation; and other ways to identify unnatural hashtags, and determine twitter reach and an authority score of tweets. These methods were used during elections in Malaysia, Mexico and Georgia.

Syndicate Discussions

Issue: Overplaying the threat of deepfakes.
The use of cheap fakes or "shallow fakes" is more prevalent than deepfakes in spreading disinformation. Cheapfakes can be effective in influencing people and are easier and less expensive to create. Nonetheless, deepfakes would increase in sophistication in the future. Firstly, better AI algorithms can lower the cost of creating deepfakes. Secondly, AI can make

doctored videos more effective by mimicking voice and pairing it with text.

Issue: Countermeasures against deepfakes. Most practitioners focus on technical solutions to counter deepfakes. However, it is crucial to address how cognitive and social factors determine the way people perceive deepfakes. Deepfakes may continue to have a psychological effect even after being debunked. Perpetrators who use deepfakes are nimble in their tactics; therefore, practitioners should keep up by developing both technical and non-technical solutions.

Issue: Effectiveness of bots during election periods. The effectiveness of bots in influencing election outcomes is debatable. Most of these bots – such as those that operated during the 2018 Malaysian elections – were of low level as they have few or no followers and are not interactive. These bots disseminate the twitter handles of random real accounts so that people receive notification that they are being pinged. These bots aim to amplify disinformation by spreading links to falsehoods to as many real people as possible within a short period.

Issue: Effectiveness of automated fact-checking. Over-reliance on automated fact-checking platforms might lead to the risk of the creation of black boxes. Machine learning (ML) works well in definite contexts such as the straightforward task of identifying pictures of specific animals. However, ML cannot effectively understand how different nuances and linguistic factors determine what is true. Therefore, how automated fact-checking platforms decide truth vs falsehood may be unclear.

Issue: Cyber forensics for determining information veracity. Cyber forensics can analyse and map the network connections between social media accounts and the content that these accounts share. The use of colour theory technique in cyber forensics enables the identification and comparison of dominant colour pixels in doctored videos against the original. Open source tools support cyber forensics in identifying and exposing disinformation.

Issue: More dialogues on cyber diplomacy to counter disinformation. Cyber diplomacy has

a role to play in countering disinformation. Dialogues between representatives and stakeholders for every state can support the development of norms and policies for online behaviour. Norms and policies are long-term solutions that underpin international rules to regulate the cyberspace. However, challenges abound as the Internet, like other global commons, are challenging to control.

Issue: Correlation between narratives and strategic objectives of disinformation. The narratives, rhetorical strategies and discourse that information operations use may not correlate directly with its strategic objectives. In understanding the objectives of disinformation, it is crucial to analyse narratives with the view of understanding how they complement a broader set of hostile activities. For example, the false narrative of Poland provoking World War Two has less to do with the war and more to do with obscuring the risk of dependence on Russian energy supplies.

Distillation

- Deepfakes are a concern as advancements in technology make them more sophisticated but cheaper to create. However, the continued prevalence of cheap fakes – such as photo-shopped visuals - makes it necessary to educate people on their risks and how to recognise them.

- The over-reliance on automated fact-checking platforms to counter disinformation can be problematic given the limitations of AI. The use of open-source tools can support cyber forensics in identifying and exposing disinformation. Cyber forensics can explain how influential networks are and how they operate across platforms

- The analysis of narratives in information operations should not happen in isolation but with an appreciation of how they complement a broader set of hostile activities. Overemphasis in narratives may distract practitioners from understanding the strategic objectives of disinformation.

Panel Five: Reception of Online Falsehoods and Inoculation

The Psychology of Misinformation

Ullrich Ecker, Associate Professor, School of Psychological Science, University of Western Australia

Summary: Fighting misinformation is a multidisciplinary problem that requires a multi-faceted approach, including improving education, techno-psychological solutions, while at the same time recognising that there are valid societal factors that may explain why misinformation is consumed. The psychology of misinformation, among others, provides an insight into how misinformation influences reasoning, and it has to be studied to construct effective mechanisms to inoculate against misinformation.

- Misinformation may be subtle and can be attributed to a variety of reasons, such as a consequence of sensationalist reporting pouncing on a single point of failure,

impaired reasoning, overestimation of threats, reduced support for evidence-based policies, or having false balances in expertise.

- Misinformation continues to influence reasoning after corrections. Corrections may reduce misinformation impact, but they do not eliminate it. Known as the continued influence effect, corrected misinformation continues to influence reasoning and decision making even when the correction is clear, credible, repeated, and when the correction is believed and later remembered. The continued influence occurs even with 'neutral' misinformation where there is no motivation not to believe the correction.

- Corrections need to be designed carefully to maximize effectiveness. Studies show that refutations reduced false beliefs more than plain retractions a week after the misinformation. Correction effectiveness can be improved by seven measures:

    - First, refuting misinformation instead of retracting the misinformation. There

is a need to explain why misinformation is wrong and why it was provided/believed. This helps to discredit the source and expose the hidden agenda behind the misinformation. Alternative factual information should also be provided to help refute misinformation.

- Second, improving salience with target audiences. Using clear, simple language, fonts, and diagrams may better explain information. Myths should only be repeated once to achieve salience with audiences.

- Third, pre-exposure myth warnings. Warnings over myths can be made to prevent initial belief and obviates the need for retrospective re-evaluation.

- Fourth, graphical representations may help in understanding information. Graphs may facilitate information processing and retention by individuals. They may show specific and quantified evidence, which is harder to counter-argue.

- Fifth, source credibility. Using credible sources may make corrections more effective.

- Sixth, the use of affirmative language keeps individuals onside. Keeping conversations civil and taking the audience's worldview and motivations into account and affirming a person's values makes them more open to worldview-inconsistent information.

- Seventh, social norming. Injunctive norms should be used instead of solely using descriptive norms because it facilitates the acceptance of correction due to fear of social exclusion.

- Misinformation corrections can, however, only be part of the solution. Policymakers should be realistic about what corrections can achieve. Studies show that while corrections may effectively reduce misperceptions, these corrections may not change feelings, voting intentions, or behaviour.

- In the post-truth era, there is a need to improve education, techno-psychological solutions, and acknowledge societal factors. Improvements to education include fostering scepticism and improving critical/analytical thinking while exposing manipulation techniques to inoculate audiences to misinformation.

- Techno-psychological solutions such as automated fact checking and bot-labelling and revise algorithms, which seek to broaden filter bubbles and downgrade disinformation, may be leveraged in the fight against misinformation. The fight against misinformation should also attend to societal factors like the causes of inequality and discontent, declining trust in science and elites, and the fracturing of the media landscape. The solutions should also address the lack of regulation of social media platforms and political donations.

Best Practices in Combating Misinformation: Lessons from Experimental Research

D.J. Flynn, Assistant Professor, School of Global and Public Affairs, IE University

Summary: Misinformation can be found in many facets of life, including foreign policy, politics, and public health. There are three main challenges in confronting misinformation: first, how the use of motivated reasoning can lead to a 'backfire' effect; second, how people can foster distrust and increase scepticism about true claims in the process of debunking misinformation; and, third, the ability to increase the fluency of false claims.

- Misinformation can infect various issues and emerge in different places around the globe. Hence, the studies on disinformation focus on wide-ranging issues, including election year misinformation in India, Zika and yellow fever conspiracy theories in Brazil, vaccine safety misperceptions in Vermont, and policy misperceptions among American citizens and legislators. These

studies show that there is a significant proportion of the population that believes misinformation to be true.

- There are three main challenges in confronting misinformation: first, how the use of motivated reasoning can lead to a ‘backfire’ effect; second, how people can foster distrust and increase scepticism about true claims in the process of debunking misinformation; and, third, the ability to increase the fluency of false claims.

- Corrective information, when used on highly controversial issues, may cause people to become more confident in their misperceptions. When the corrective information is presented to an individual who believes strongly in the misinformation, they may counter-argue their points more forcefully. This may cause an entrenchment in their positions, thereby triggering a ‘backfire’ effect on the initial correction.

- Most recent evidence, however, shows that corrective information reduces

misperceptions about most issues, and it would be best practice to avoid partisan or ideological sources in corrections and employ trusted experts to provide corrections instead.

- Correcting firmly held misperceptions can decrease people's confidence and increase their scepticism about all claims, both true and false. The experiment on providing corrective information about Zika and yellow fever in Brazil showed that corrections decrease belief in some false claims about Zika, like the ability of Zika to be spread through casual contact and genetically modified mosquitoes caused the Zika outbreak. These corrections, however, also decrease belief in several true claims, such as Zika being spread by mosquitoes, causes neurological problems, and increases the risk of microcephaly. Potential corrections should be tested rigorously to avoid unwanted spill-over effects.

- The correction of false claims may ironically make a claim more familiar, and in turn, reinforce the veracity of the claim

because of said familiarity. This becomes especially problematic when these corrections are framed as negations rather than affirmations because people are bad at processing negations. Over time, people will often remember false claims as true, and make their own connections contained in the negation. The best practice is thus to use affirmative language instead when presenting corrections.

Responding to Science Misinformation in A Post-Truth World

John Cook, Research Assistant Professor,
Center for Climate Change Communication,
George Mason University

Summary: Inoculation of populations against misinformation shows a strong positive change in consensus even when misinformation is presented to them. In contrast, when only facts and misinformation are presented to populations, there is still a probability of a negative change in the perceived consensus. There are three approaches to inoculation: first is a fact-based method, second is based on the use of logic,

and, third, use credible sources to inoculate populations.

- Inoculation of populations against misinformation warns of the threat of misinformation alongside the counter-arguments against the misinformation. For instance, with regards to climate change, there is a very strong consensus – ninety-seven percent – among the climate science community that global warming is real, it is bad, it is caused by humans, but there's hope.

- However, the Global Warming Petition Project, which purportedly received 31,000 American scientist signatories in its online petition, is trying to persuade populations that there is no convincing scientific evidence on greenhouse gases causing global warming. A closer examination of the petition project revealed a number of signatories on the petition are fictitious, including Charles Darwin and members of the Spice Girls.

- It is also of note that while 31,000 signatories seem like a large absolute

number, it only represents 0.3 percent of all United States graduates with a science degree, and most of these graduates do not have any expertise in climate science.

- The industry groups and organisations occasionally leverage misinformation about scientific data. A common tactic used by industry groups and organisations is to manufacture doubt about science through the promotion of “fake experts”. These “fake experts” are often spokespeople who convey the impression of expertise in a given area without possessing actual relevant experience. An example of this can be seen with the tobacco industry and the scientific evidence linking smoking with cancer.

- Logical fallacies are also a common way of spreading disinformation online. For example, a tweet purporting that the “safe” HPV vaccine caused paralysis in a teenager was debunked by a response citing data from large-scale scientific studies showing no link between the vaccine and auto-immune symptoms that cause paralysis. The response also called

out the tweet for its logical fallacies in mixing the concepts of causation and correlation.

- The use of parallel arguments may help populations understand misinformation better. Parallel arguments adopt the same logical structure as a misinforming argument but apply it in an absurd situation to demonstrate the false logic. For instance, late-night shows in the United use absurd comparisons in response to the misinformation perpetuated by the media and the Trump administration. The use of cartoons also helps to break the seriousness of the refutation and may make it more believable.

- Inoculation can also be done proactively, where inoculation prompts participants to generate pro- and counter-arguments actively. This has been used in classrooms around the United States and helps students recognise the techniques of science denial and teach students to name the fallacy that is being perpetuated.

Syndicate Discussions

Issues: There are multiple factors influencing individuals' receptivity to information. Individual emotions and social and cultural aspects affect the cognitive reception of influences depending on the target operations. Every target has its own characteristics. Influencers use different models/presentations for different groups. Usually, there are pre-existing cognitive biases that are exploited. It's harder to move people towards certain behaviour when their beliefs are contradictory. People have a desire to hold their attitudes and beliefs in harmony and avoid contradiction (or dissonance). One needs to think about the continuum of outcomes – from changing the belief to changing behaviour. For example, with regards to vaccination attitudes, while one can care about people's beliefs about the safety of vaccines, the high stake outcome is if one is convincing people who are sceptical about vaccination to vaccinate their kids. It is a behavioural outcome. It is important to nudge behaviour, not just belief.

Issue: Effects of information correction. Correcting misinformation on highly technical issues such as those related to science and medicine is likely to be met with greater receptivity. This is because people are more pliable on topics that they are less confident in. In comparison, it may be more challenging to correct people's misperception on "easier" topics like politics. Rather than mere information correction, it is also helpful to consider a particular group's general belief on a wide variety of issues in the hope of changing not only their attitudes but ultimately their behaviours as well.

Issue: Applying specific strategies for inoculation of the target audience. Applying inoculation theory for hyper-partisan individuals can assist in convincing sceptics on the issue of climate change. Messages to inoculate the public should be crafted in ways that resonate with the target audience. It is harder, however, to apply this for individuals who hold extremely fixed beliefs on a certain issue. Communicating with radical disbelievers can be achieved by framing messages in a way that takes their worldview into account, instead of being confrontational

and dismissive of their beliefs. In the instance of climate change deniers, affirming their values and decoupling science from their values enables them to feel heard and be potentially more receptive to counter-arguments.

Issue: Testing interventions before implementation. Random Controlled Trials (RCTs) to understand the psychology of human behaviour and misinformation, when conducted through online experiments, are often quick and methodological. However, it should be conducted in an ethical manner: researchers must always be cognizant of best practices and any potential spill over effects of the research.

Issue: The role of the government in countering disinformation. Many countries worldwide are pondering over the role of the government in countering disinformation. For the most part, it is generally agreed that the key function of the government is to provide collective welfare. Governments should, therefore, take active measures to combat disinformation. Free speech norms differ from country to country. Therefore, measures such

as content takedown may not be welcome in places where free speech is the defining norm. Governments can address disinformation through measures such as information campaigns.

Distillation

- Cognitive, societal, and algorithmic biases are exploited to spread fake news. It is important to build tools to raise people's awareness of these biases and help people protect themselves from outside influences designed to exploit them.

- Understanding the belief and value systems of a target audience can help increase the target audience's receptivity to the corrections of misinformation.

- Pilot testing through random controlled trials can allow for a greater understanding of messaging strategies needed to inoculate target audiences effectively.

- Training people to recognise disinformation is challenging. However,

research is fast advancing in the area of psychology and cognitive studies. Practitioners need to find ways to incorporate the results into intervention practices.

- Governments do have a role in countering disinformation by virtue of their mandate to provide collective welfare for their citizens.

Panel Six: Countering Online Falsehoods and Influence Operations

Countering Disinformation by Empowering Civil Servants

James Pamment, Director, Partnership to Counter Influence Operations, Carnegie Endowment for International Peace and Associate Professor, Lund University

Summary: Initiatives to counter disinformation cannot rely solely on technical solutions. Strategic communications professionals have become crucial in detecting malicious falsehoods, mitigating damage, and devising constructive responses. In this challenging and evolving field, building capacity among relevant practitioners in government and civil society should be a priority.

- A team at Lund University has been training governments and civil servants to counter disinformation. Training material is based on best practice underlined by scientific theory and includes activities

such as tabletop exercises. The training embraces an applied practitioner angle to ensure methods are actually used out in the field. Standard operating procedures (SOPs) are central to developing strategy, as civil servants are generally accustomed to working under such processes and routines.

- One project focused on the 2018 Swedish elections, and particularly communications professionals managing a Facebook page. The team developed a tool to help identify sophisticated multi-faceted foreign influence operations, which may involve false corroborations and bot-driven amplification.

- Following the March 2018 poisoning of a former Russian military officer in Salisbury, United Kingdom, the team developed a cross-government tool kit called Resist, which enabled large government departments to identify problems early and weigh risk when considering whether to counteract, while working in collaboration with a range of stakeholders relevant to the issue at hand.

- The team also engaged with the European Centre of Excellence for Countering Hybrid Threats (Hybrid CoE) in Helsinki to deliver election training. Sessions were held with roughly 50 individuals, including strategic communications professionals, electoral board representatives, security policy officials, and intelligence analysts. Through exercises, participants learned each other's strengths and weaknesses, issues regarding classification, and how to communicate information effectively across different sectors.

- Critical issues moving forward include balancing basic and applied research projects, given the requirement of tools to address immediate concerns. Much of the discussion around disinformation is still based on incidents from 2016, with limited analysis of current issues, which may only now be emerging. Effective collaboration is a further challenge. While governments and civil society often form productive relationships in the counter-disinformation space, technology companies may be

reluctant as they feel under threat from regulation and legislation.

Elves. Debunking vs. Own Success Stories

Giedrius Sakalauskas, Director, Res Publica

Summary: Debunking disinformation and calling out those seeking to spread strategic falsehoods are important, but they represent only part of an effective defence strategy. Responses should also employ the tactics of the instigator by using narratives. Engaging in the conversation armed with credible expert analysis or humour may have a greater impact than simply unveiling a fake story.

- Malicious actors are countering debunking efforts by undermining the integrity of the fact checkers and spreading disinformation in greater volume. On September 25, 2019, a WordPress blog falsely reported that 22 German soldiers operating under NATO desecrated graves at a Jewish cemetery in Lithuania. The webpage disappeared a few hours after the initial post, but the story, which featured doctored photos, had spread

widely on social media. On the same day, a petition emerged, seeking to remove German troops from Lithuanian soil. Lithuanian mainstream media outlets quickly reported the falsehoods, and the Foreign Affairs Ministry released statements confirming the news was false and likely part of an influence campaign. However, the problem is only the most 'newsworthy' hoaxes are picked up by the media for debunking.

- Developing counter-narratives may be a more effective defensive strategy. One pertinent case study involves the Ribbentrop Molotov Pact, a non-aggression agreement between Nazi Germany and the Stalin-led Soviet Union, which divided, occupied, and spread fear throughout Eastern Europe from 1939. Some in Kremlin use The Pact's anniversary to disseminate revisionist versions of history, such as the claim Poland started World War II. In response, Lithuanian civil society activists have published accounts from credible international historians and Russian opposition commentators.

- Often the best narratives involve humour or sarcasm. A good example is the parody twitter account, Darth Putin, which posted photos showing the day “we celebrated liberating Poland from the Poles”. Lithuanian Elves have also conducted campaigns targeting “hostile propaganda outlets” such as Russia Today, in collaboration with counterparts in neighbouring nations. The strategy was to inundate the news outlet’s social media page with memes calling out the network’s misleading reporting of the Ribbentrop Molotov Pact anniversary, in particular.

- Foreign interference and disinformation campaigns present complex and difficult challenges, though democratic societies should ultimately hold the upper hand through openness and transparency, leading to more authentic narratives and credible arguments.

Simple Tools for Educators to Deal with Information Disorder

Kari Kivinen, Director, Helsinki French-Finnish School

Summary: The merging of social media and traditional news media has created a paradigm in which young people have become experts in the dynamics of online platforms while often lacking the critical judgement to discern impartial news reporting from prejudiced falsehood. In Finland, contemporary media literacy and fact checking is now taught in schools.

- Faktabaari is a non-partisan Finnish fact-checking service, employing social media tools to verify the information and ensure factual accuracy, particularly during public election debates. The organisation shares its fact-checking methods in schools to develop media literacy skills and raise awareness regarding disinformation. The goal is to have information literacy included in the national education curriculum. One problem is teachers are often reluctant to discuss social media with students because they feel young

people know far more about the subject. Educators require training, up-to-date material, and the involvement of media experts.

- A recent survey among Finnish youth revealed 94 percent of young people regard social media as a source of information on interesting subjects. A similar number believe the associated platforms are a source of happiness, while half thought they could lead to sorrow. The study found that while adults and young people engage with similar online tools, they use them in different ways. For example, students largely consume news media from unregulated social media sources instead of traditional outlets and have difficulty distinguishing proven fact from pseudoscience, or advertisement from a new article.

- Faktabaari uses a “traffic-light” system to divide published claims into three categories. Red denotes a clearly false piece of information, regardless of the poster’s motivation. A green light endorses a claim as factually correct, at

least in the particular context given. An orange/yellow light indicates partially true information, which cannot be regarded as completely accurate. This is common in the case of over-simplified representations of an issue.

- Another powerful tool is a simple checklist of questions to ask oneself before believing, liking, or sharing a piece of news. The procedure encourages users to think about who published the content, for whom it was intended, what the content is actually saying, why it was made, what is the basis of its message/information, and whether the associated pictures can be deemed authentic. The organisation believes this process has enhanced vigilance among young people online.

Syndicate Discussions

Issue: Understanding the objective of influence campaigns should be made a priority. Influence campaigns are usually about hard objectives rather than narratives or strategies. Narratives and strategies can both prove to be a distraction from the

ultimate goal of undermining a particular decision. Disrupting and countering the strategic objective of influence campaigns is vital.

Issue: Governance framework to tackle disinformation initiatives. Information operations are usually one aspect of influence operations. Toolkits such as the United Kingdom's RESIST framework (Recognise disinformation; Early warning; Situational insight; Impact analysis; Strategic communication; and Track outcomes) can be utilised to set-up best practices for counter disinformation planning. Such tactics include using online monitoring and surveillance to identify trends online for situational awareness. Additionally, Red-teaming scenarios may help test resilience. For instance, the Red-teaming exercises for the upcoming 2020 elections in the United States require participants (e.g., cybersecurity experts, technology companies) to develop strategies to manipulate the 2020 elections in various scenarios.

Issue: Building trust in government is an essential part of countermeasures. The government should not drive campaigns against its own people. The government can be seen as credible in information campaigns like “don’t drink and drive”, “don’t smoke”. However, to counter disinformation or avoid being seen as a propaganda machine, the government should build trust. The government has to work with NGOs, and wider civil society to build trust.

Issue: Measuring the success of a campaign against disinformation. While the grassroots-led campaign may not be able to measure the reach of their messaging as advertising companies can, they can take practical steps to respond to disinformation. For example, in Lithuania, a campaign called “Why Not Swastikas” was conducted in response to Walmart selling t-shirts emblazoned with swastikas. The campaign was deemed to be a success because international media featured it. After two months of active campaigning, Walmart stopped selling the offending t-shirts, showing that the efforts paid off.

Issue: Shared responsibility for media literacy between families and schools. It is difficult to distinguish where informal and formal education ends for children. In Finland, parents are considered as the first educators on media literacy. This is further reinforced when students enter the education system. Media literacy needs to be a shared responsibility between parents and schools. Educating children in media literacy is thus also a process of continuous learning. Finnish educators promote a participative learning model for Finnish students and adopt a facilitative role rather than an instructor role (e.g., through presentations, discussions, and peer-to-peer learning).

Issue: Fact-checking organisations may collaborate with schools in teaching media literacy. Media literacy should be included in the school curriculum to will help students spot disinformation. Schools can partner with fact-checking agencies in their efforts to boost digital literacy. For instance, a Finnish fact-checking organisation, Faktabaari (FactBar), adapts professional fact-checking methods for use in Finnish schools. The group believes

good research skills and critical thinking are key to countering disinformation.

Distillation

- While the use of disinformation by foreign adversaries can threaten democratic processes in the target nation, democratic values are among a state's most fundamental safeguarding attributes in efforts to counter malicious falsehoods. The more open and transparent the national government, the more likely its citizens and observers abroad will believe and respect its narratives.

- The ultimate strategic objective of influence campaigns should be understood before devising countermeasures and countering narratives and strategies.

- As with any complex national security challenge, responses to disinformation campaigns require close multi-stakeholder coordination. Governments should ensure effective systems of integrating their many functions and clear

lines of communication among different agencies. Civil servants and educators should be supported by training initiatives to tackle disinformation.

- The importance of community-based, ground-up initiatives cannot be understated. Encouraging participatory learning for students can reinforce media literacy skills and initiatives more effectively than rote learning models.

- Media literacy must be a shared responsibility between the home and school and should be a continuous process. Fact checking organisations can partner with schools to enhance media literacy education.

Moderated Discussion (Closing Panel)

Chaired by: Shashi Jayakumar, Head, Centre of Excellence for National Security (CENS), RSIS, NTU [Singapore]

Speakers: Giedrius Sakalauskas, Director, Res Publica and Ross Tapsell, Senior Lecturer and Researcher, College of Asia and the Pacific, Australian National University (ANU)

Summary: The closing panel gave reflections on the key issues discussed during the workshop and proposed ways to move forward. The overarching argument of the closing panel suggested that while advances have been made in research on and governance of disinformation, given fast-changing developments, stakeholders from the policymaking and academic circles must work on the issue and solutions proactively.

- The disinformation phenomenon is a fast-evolving one. Since the 2016 U.S. presidential election, the issues of

concern have expanded beyond distortions, rumours, misinformation, and smears. Malicious actors are ramping up the game of state-sponsored subversion and foreign interference, becoming more sophisticated in terms of tactics. For instance, the Russian-sponsored disinformation has become more refined from the 2016 election to the 2018 mid-term election.

- Given the fast-changing developments on the ground, academic studies on disinformation have been proliferating. The so-called “fake news” issue has resulted in a renewed interest in media studies, with more researchers studying the phenomenon and numerous conferences on the topic worldwide. The research on detecting and countering disinformation advanced with the increase in capacity to study encrypted messaging platforms and the integration of psychology studies into disinformation studies.

- In the future, all stakeholders need to think about emerging campaigns in a proactive manner. Most are still considering the issue from the fallouts of the 2016 U.S. presidential elections, but other problems are quickly developing. Both research and policymaking need to stay one step ahead of the disinformation issue.

- For academia, there is an increasing link between disinformation research and investigative journalism. However, exposing disinformation practices could no longer be sufficient going forward. There is a need to integrate multidisciplinary perspectives from social media analytics and in-depth country studies to better understand how disinformation operates.

- Technology platforms need to better focus on how their platforms could be manipulated in future elections, going beyond measures like giving out grants for research. Policymakers also need to discuss more concretely what intervention measures, such as cyber

hygiene, media literacy, and critical thinking, entail in their respective countries. Some agencies like think tanks could be called upon to call out disinformation tactics in a much more direct fashion in the future.

Workshop Programme

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

Monday, 4 November 2019

0800–0900hrs **Registration**

Venue : Taurus & Leo Ballrooms Foyer, Level 1

0900–0910hrs **RSIS Corporate Video and Workshop Welcome Remarks** by ***Shashi Jayakumar****, Head, Centre of Excellence for National Security (CENS), RSIS, NTU*

0910–1010hrs **Panel 1: Online Falsehoods and Beyond: Influence Operations**

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

Speakers **The New Disruptive Media and Southeast and East Asia** by ***Markku Juhani Mantila,*** *Chief,*

Technical & Scientific Development Branch, NATO StratCom COE

Information operations and psychological operations - selected model by ***Kamil Basaj*****,** *CEO, INFO OPS Poland Foundation*

Russian and Chinese influence operations in Europe

by ***Veronika Víchová,*** *Head, Kremlin Watch, European Values Think-Tank*

1010–1030hrs **Networking Break**

Interactive Syndicate Discussions

1030–1130hrs

Syndicate 1

Venue : Capricorn A Ballroom, Level 1

Syndicate 2

Venue : Capricorn B Ballroom, Level 1

Syndicate 3

Venue : Pisces & Aquarius Ballrooms, Level 1

1130–1230hrs **Panel 2: Online Falsehoods and Influence Operations in Asia**

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

Speakers **Activism Trolled: Why Human Rights Groups Are Losing the Disinformation Battle Online** by ***Aim Sinpeng***, *Lecturer, Department of Government and International Relations, University of Sydney*

Tweeting through the Great Firewall by ***Tom Uren*****,** *Senior Analyst, International Cyber Policy Centre, Australian Strategic Policy Institute (ASPI)*

The Rumor Mill of Sri Lanka: Lessons in Countering Misinformation by ***Yudhanjaya Wijeratne****, Senior Researcher, LIRNEasia*

1230–1330hrs **Interactive Syndicate Discussions**

Syndicate 1
Venue : Capricorn A Ballroom, Level 1

Syndicate 2
Venue : Capricorn B Ballroom, Level 1

Syndicate 3
Venue : Pisces & Aquarius Ballrooms, Level 1

1330–1430hrs **Lunch**

1430–1550hrs **Panel 3: Elections and Information Manipulation**

Chair : ***Muhammad Faizal Bin Abdul Rahman****, Research*

Fellow, Centre of Excellence for National Security (CENS), RSIS, NTU

Speakers

Swedish Experiences of protecting an election by ***Fredrik Konnander****, Head, Counter Influence Branch, Global Monitoring and Analysis Section, The Swedish Civil Contingencies Agency (MBS)*

From Misinformation to Extremism: How WhatsApp Is Affording Radicalization in Brazil by ***David Nemer****, Assistant Professor, Media Studies Department, University of Virginia*

Drivers of election disinformation in Indonesia and Malaysia by ***Ross Tapsell****, Senior Lecturer and Researcher, College of Asia and the*

Pacific, Australian National University (ANU)

Understanding and Countering Online falsehoods and influence operations: the case of Indonesia
by ***Ismail Fahmi****, Founder, PT Media Kernels Indonesia*

1550–1710hrs **Interactive Syndicate Discussions**

Syndicate 1
Venue : Capricorn Ballroom, Level 1

Syndicate 2
Venue : Pisces Ballroom, Level 1

Syndicate 3
Venue : Aquarius Ballroom, Level 1

Venue : **Syndicate 4**
Libra & Gemini Ballrooms, Level 1

1710hrs **End of Day 1**

1830–2030hrs **Workshop Dinner (By Invitation Only)**
Venue : Aquamarine, Level 4

Tuesday, 5 November 2019

0800–0900hrs **Registration**

Venue : Taurus & Leo Ballrooms Foyer, Level 1

0900–1000hrs **Panel 4: Tactics, Technology and Future of Online Falsehoods and Influence Operations**

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

Speakers : **Getting Real About The Deepfake Threat** by ***Tim Hwang***, *Lawyer and Researcher, and the Former Director of the Harvard-MIT Ethics and Governance of AI Initiative*

Deviant Mobs of the Internet: Tactics,

Techniques, and Procedures by ***Nitin Agarwal****, Jerry L. Maulden-Entergy Endowed Chair and Distinguished Professor, University of Arkansas at Little Rock*

Bots, Disinformation and Foreign Meddling in the Digital Space
by ***Lukas Andriukaitis****, Associate Director, Digital Forensic Research Lab (DFRLab), The Atlantic Council*

1000–1100hrs **Interactive Syndicate Discussions**

Syndicate 1
Venue : Capricorn Ballroom, Level 1

Syndicate 2
Venue : Pisces & Aquarius Ballrooms, Level 1

Syndicate 3
Venue : Libra & Gemini Ballrooms, Level 1

1100–1120hrs **Networking Break**

1120–1220hrs **Panel 5: Reception of Online Falsehoods and inoculation**

Chair : ***Yi-Ling Teo****, Senior Fellow, Centre of Excellence for National Security (CENS), RSIS, NTU*

Speakers : **The Psychology of Misinformation** by ***Ullrich Ecker****, Associate Professor, School of Psychological Science, University of Western Australia*

Best practices in combating misinformation: Lessons from experimental research by ***D.J. Flynn,*** *Assistant Professor, School of Global and Public Affairs, IE University*

Responding to science misinformation in a post-truth world by **John**

Cook, *Research Assistant Professor, Center for Climate Change Communication, George Mason University*

1220–1320hrs **Interactive Syndicate Discussions**

Syndicate 1
Venue : Capricorn Ballroom, Level 1

Syndicate 2
Venue : Pisces Ballroom, Level 1

Syndicate 3
Venue : Aquarius Ballroom, Level 1

1320–1400hrs **Lunch**

1400–1500hrs **Panel 6: Countering Online Falsehoods and Influence Operations**

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

	Speakers :	**Countering disinformation by empowering civil servants** by ***James Pamment****, Director, Partnership to Counter Influence Operations, Carnegie Endowment for International Peace and Associate Professor, Lund University* **Elves Debunking vs. Own Success Stories** by ***Giedrius Sakalauskas***, *Director, Res Publica* **Simple Tools for Educators to deal with Information Disorder** by ***Kari Kivinen****, Director, Helsinki French-Finnish School*
1500–1600hrs	**Interactive Syndicate Discussions**	
		Syndicate 1
	Venue :	Capricorn Ballroom, Level 1
		Syndicate 2
	Venue :	Pisces Ballroom, Level 1

Syndicate 3

Venue : Aquarius Ballroom, Level 1

1600–1620hrs **Networking Break**

1620–1700hrs **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*

1700hrs **End of Day 2**

1830–2030hrs **Closing Dinner (by Invitation Only)**

Venue : Peach Blossoms, Level 5

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.