EXTREMISM AND TERRORISM ONLINE: A MULTIDISCIPLINARY EXAMINATION OF CURRENT TRENDS AND CHALLENGES

Event Report
13-14 October 2014

Centre of Excellence
for National Security

RSiS
Nanyang Technological University
S. RAJARATNAM SCHOOL OF INTERNATIONAL STUDIES

NSCS
NATIONAL SECURITY COORDINATION SECRETARIAT

Event Report

EXTREMISM AND TERRORISM ONLINE: A MULTIDISCIPLINARY EXAMINATION OF CURRENT TRENDS AND CHALLENGES

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:
Navhat Nuraniyah, Joseph Franco, Jennifer Yang Hui, Nur Diyanah, Romain Quivooij, Yeap Su Yin, Priscilla Cabuyao

Editors:
Navhat Nuraniyah, Joseph Franco

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

CONTENTS PAGE

EXECUTIVE SUMMARY

Opening Remarks

In his Opening Remarks, Norman Vasu spoke about the importance of the Workshop theme as the Internet and social media continue to have a profound impact on how terrorist groups operate. He highlighted some examples of the increased utility of the Internet to terrorists of different religious and ideological backgrounds including Islamist militants and right-wing extremists. A major lacuna in online extremism research was the overemphasis on extremist activities and threats online, with little research on an individual's interaction with extremist ideas – both online and offline – as well as how such interactions contributed to the radicalisation process. Given the complexity of online extremism, a multidisciplinary examination that takes into account the dynamics and interconnections between the online and offline realms was, therefore, necessary. He concluded that the Workshop was a modest step to better understand the issue and formulate workable policy solutions.

Panel One – Current State of Play: Extremism and Terrorism Online

The first panel of the Workshop assessed the current state of play in online radicalisation. Departing from traditional studies that concentrated on content analysis of web pages, Anne Stenersen's presentation examined the actual learning process of terrorists who chose to use the Internet to manufacture explosives. The second speaker of the panel, Anne Aly, spoke on the interactive process by which messages embedded in terrorist propaganda are communicated and understood by individuals in their everyday lives. Thomas Koruth Samuel argued that online media has become a game changer for terrorists' violent narratives, allowing the message to reach a global audience in an unprecedented manner and scale. The final speakers of the panel, Navhat Nuraniyah and Sulastri Osman, analysed the extent to which the Internet was used in ten terrorist operations in Indonesia over the past decade.

Panel Two – Radicalisation over the Internet: Mechanisms and Processes

The presentations started with Kumar Ramakrishna discussing online extremists transition into real-world violence. The nuance between radicalism and extremism was also explored, and it was suggested that all forms of extremism should be unequivocally rejected. In the second presentation, Philipp Holtmann explored the role of allegiance pledges among terrorist groups like the Islamic State (IS). Pledges could provide multiple functions such as establishing virtual leadership and remote command-and-control. Omer Ali Saifudeen spoke of potential "tipping points" for online radicals to engage in violence. Omer cautioned against focusing solely on radicalising messages, and stressed that context as well as the combination of message, messenger and messaging were all important factors in the analysis of tipping points. In the final presentation, Michael Kenney underscored the limitations of online learning and knowledge-sharing by terrorists. Kenney distinguished between the abstract (techne) and practical (mētis) knowledge required to conduct attacks, and the difficulty of attaining the latter through the Internet. He stressed that real-world training remained indispensable, with active insurgencies acting as learning laboratories for terrorists.

Panel Three – Linking the Dots: Methodological Issues and Research Implications

The panel examined various methodological issues pertaining to existing approaches to online extremism research as well as discussed the relevant implications. All three speakers highlighted the important role of analysts in the planning and carrying out of data collection and the necessity of maintaining research integrity. Jeffrey Simon discussed the issue of 'lone wolf' radicalisation and the importance of including this subject in overall terrorism research. The presentation by Aaron Zelin explored the inherent biases and ethical concerns that analysts should be cognisant of when conducting data collection through social media. The final speaker, Carlo Pecori, discussed the need to fully understand how social media is used in the country vis-a-vis traditional media in order to gain better insights.

Panel Four – Social Media Analytics and Online Extremism: Cutting-edge Tools for Research and Intelligence Gathering

The implications of social media analytics tools in the study of online extremism and terrorism were the focus of this panel. The speakers addressed the issue from three different angles. The first presenter, Maura Conway, emphasised the value of 'big data tools' in gathering substantive empirical data. Despite the advantages provided by such tools, technical and ethical drawbacks might hinder the effective synergy between social science methods and computer science tools. The second panellist, Lisa Kaati, described the processes used to identify 'weak signals' of extremist behaviour through social media. Focusing her presentation on specific types of warning behaviour and profiling techniques, she underlined the promising potential of the proposed recognition methods. Shifting to the question of jihadist social media strategy, the third presenter, Nico Prucha, provided an update on the networked structure of the online activities of Islamist militants. To this end, he outlined the strategic communication mechanisms involved, stressing the highly adaptive nature of Islamist militants' social media strategy.

Panel Five – Countering Online Extremism

The speakers offered different perspectives on how to counter online extremism. Daniel Kimmage spoke on the initiatives of adversarial engagements undertaken by the United States government. The aim is to achieve three over-arching objectives: to contest the online space; redirect online conversations; and let the adversary know that there are alternative voices online. Speaking about online initiatives in Indonesia, Bilveer Singh noted that while such initiatives played an important part, it was essential to address existing grievances in the offline realm in order to deal with violent extremism. This last point was echoed by Elina Noor, who advocated for a structural, whole-of-society approach in countering violent extremism. She also argued that it was necessary to focus on educational initiatives, such as teaching the youth to critically engage with materials online. Several methods to combat online extremism and terrorism were also discussed. Max Boon spoke about the power of victims' and reformed terrorists' stories in educating and influencing the youth. Outreach activities such as trainings and workshops were also useful in this regard. Mehdi Knani argued that human rights, due process, and the rule of law should be observed when dealing with the issue of online extremism. Nur Azlin Mohamed Yasin discussed the significance of looking at root causes and direct enablers in understanding radicalised individuals and promoting the ideology of peace with the help of influential members of the community such as clerics, the media and youth leaders.

Moderated Discussion

The Moderated Discussion was intended to facilitate a frank exchange on how to move forward with policy and research initiatives on online extremism. Three main themes emerged in the discussion: the importance of effective counter-narratives; the role of civil society both online and offline; and the need to fill the gap in existing online extremism research. To develop a more effective counter-narrative, it was necessary to adopt a more nuanced approach in three key elements, namely, the message, messenger, and messaging. It was also important that new initiatives were developed to counter extremists' rebuttal of existing counter-narratives. With regard to the role of civil society in assisting in countering extremism efforts, public-private partnership and better communication between researchers and civil society were recommended. It was proposed that two major issues deserved more attention in terrorism research: empirical evidence on whether the Internet actually reduced extremism due to its role as a safe place for expressing extremist ideas; and reflexive discussions on methodological and ethical issues in online extremism research.

OPENING REMARKS

Opening Remarks
Norman Vasu, Deputy Head, Centre of Excellence for National Security (CENS), RSIS

Norman Vasu

Norman Vasu on behalf of the Dean, RSIS, welcomed all participants, speakers, and observers. The Workshop was organised by the Centre of Excellence for National Security (CENS), a constituent unit of the S. Rajaratnam School of International Studies (RSIS) at Nanyang Technological University (NTU) with the support of the National Security Coordination Secretariat in the Prime Minister's Office.

Vasu noted the timeliness of the Workshop topic as the Internet and social media continue to have a profound impact on how terrorist groups operate. He highlighted some examples of the increased utility of the Internet to terrorists of different ideologies. Al-Qaeda propagandist Anwar Al-Awlaki called for an army of "internet mujahidin" to fight on the media battlefront, which is apparently considered as "half of jihad". Right-wing radicals have also used online forums to spread their ideology, attract new recruits, and cement brotherhood among existing and new members through a virtual community. The Internet has altered terrorist modes of operation. The circulation of terrorist tradecraft online means that even lone-actors could get bomb-making instructions and virtual training through a simple Google search.

Despite the increasing attention to the phenomenon of online extremism, major lacunas in online extremism research were identified. For instance, the links between the Internet and radicalisation remain poorly understood. There has been much emphasis on extremist activities online and the threat emanating from them such that online extremist content or the online media itself is often depicted as the source of the problem, and individuals as passive recipients being brainwashed by online contents. Meanwhile, individuals' interaction with extremist ideas – both online and offline – and how such interactions influence radicalisation processes remain under-investigated. Given the complexity of online extremism, a multidisciplinary examination that takes into account the parallel links between what is online and what is offline was recommended.

Against this backdrop, the Workshop was a modest step to better understand the issue and formulate workable policy solutions. It aimed to provide a platform for policy practitioners and scholars to exchange ideas and tease out workable policy outcomes. In this regard, it brought together a genuinely multidisciplinary panel of experts not just from Singapore, but also from the UK, Australia, the US, Norway, Netherlands, Malaysia, Austria, and Sweden.

PANEL 1

CURRENT STATE OF PLAY: EXTREMISM AND TERRORISM ONLINE

Virtual Training: How do terrorists use the internet to learn bomb-making skills?

Anne Stenersen, Research Fellow, Terrorism Research Group, Norwegian Defence Research Establishment (FFI)

Anne Stenersen

Anne Stenersen's presentation discussed how the Internet may assist terrorists in learning how to manufacture explosives. Based on a case study of the Al-Qaeda network, Stenersen observed that the Internet acts as a library for jihadist training manuals and a virtual classroom. However, the training manuals had seen low levels of usage due to the overload of information and the indispensability of face-to-face learning. Despite this observation, Al-Qaeda continued to use the Internet as supplement to real-life training as well as to encourage lone terrorists in achieving their goals.

Stenersen observed that the Internet acts as a library for Al-Qaeda training manuals, which can be stored and accessed by sympathisers. The sheer volume of the manuals represents a challenge to censorship and prevention of their distribution. In addition, the Internet also serves as virtual classrooms through functions such as chat forums. Al-Qaeda Internet strategy, however, has focused more on keeping an online library rather than running a virtual classroom.

From the 100 cases of jihadi inspired plots in Europe in the last 20 years, Stenersen found that there had actually been very few cases in which terrorists relied on online websites for bomb making skills. She suggested three reasons for this: information overflow, missing information, and the importance of face-to-face interaction for radicalisation and recruitment processes. The voluminous online content means that it is often difficult to ascertain the effectiveness of manuals without proper scientific and technical knowledge. Furthermore, the bomb-making manuals do not cover crucial information for the comprehensive making of explosives. The training manuals often contain limited detail about the preparation and final processes of assembly of explosives. Coupled with security and tactical concerns, these issues reduce the attractiveness of online bomb-making manuals.

In terms of radicalisation and recruitment processes, Stenersen was sceptical of Internet facilitation. For instance, many terrorists had been radicalised overseas. While there are exceptions to the rule, she observed that "home radicalised" individuals often differ from those radicalised abroad. Acting alone, their operations are often emotional rather than strategic and preferring simple weapons due to the spontaneous nature of the attacks.

Stenersen believed that Al-Qaeda is aware of the limitations of the Internet in terms of its appeal and therefore prefers to use the Internet as supplement to real life training rather than replace it altogether. Since 2010, the organisation's strategy has been to encourage lone-wolf terrorists to launch low-scale attacks to inspire terrorist attacks all over the world. While such limitations are often viewed as weakness, Sternersen argued that Al-Qaeda uses online tools to reach sympathisers in the hope of recruiting new members and promoting the jihadist cause.

In closing, Stenersen noted that shutting down jihadist websites or removing materials is counterproductive because denying such materials would only increase A-Qaeda's status and make the websites more mysterious and thereby attractive. She also noted that jihadist ideological contents comprise far more than bomb-making manuals. A graver concern is the manner in which Al-Qaeda attempts to radicalise youths online by promoting a culture of solo terrorism.

Brothers, Believers, Brave Mujahideen: Focusing attention on the audience of violent jihadist preachers
Anne Aly, Research Fellow, School of Media, Culture & Creative Arts, Curtin University

Anne Aly

Anne Aly saw the Internet as a critical tool for the dissemination of terrorist messages. Most research on jihadist websites, however, focused on the kind of messages being spread via the various media platforms, falling short of understanding the reason for the appeal of certain messaging to some people and not others. The theories also assume a passive audience uncritically consuming violent messages. To address this gap in understanding, Aly approached the study of audiences from three-level analysis to develop understanding of the interactive process by which messages that are embedded in terrorist propaganda are communicated and understood by individuals in their everyday lives.

Aly stated that the Internet is a critical part of the terrorist repertoire. While not innovative, terrorists are opportunistic in using the online platform to learn, influence, organise and inform their supporters. The Islamic State's media campaign, for example, is comparable to some of the world's largest multinationals with usage of the social media, publication of e-magazine *(DABIQ)*, and creation of opinion leaders, all in 200 languages. The websites' usage of master narratives that employ systemic and heuristic techniques, for example, has been well-documented.

The impact of online master narratives, however, has been less clear. Aly noted that studies on the impact of jihadist websites on their audience largely relied on the silver bullet model of communication, which assumes a passive audience with no real understanding of how messages are received and interpreted. The theory also does not provide an understanding of the context for interpreting the messages. Therefore, despite the heavy usage of the internet by terrorists, little is known about the actual import of online radicalisation. While there is much empirical evidence that the internet is a public space to find support for ideas, evidence for the escalation of radicalisation or promotion of self-radicalisation has not been proven.

Aly proposed a theory to gain more complete understanding of the audience interaction with the Internet. The media uses and gratification theory notes four primary needs that can be fulfilled in the usage of media: information; personal identity (involving confidence, identity and value reinforcement); social interaction (personal relationships, imagined community provided by the Internet); and entertainment (to escape and relieve tensions). She noted that the categories are not mutually exclusive and a particular online material can serve more than one need.

In moving forward, Aly suggested that policymakers need to look at three key areas to better understand the impact of jihadist websites: the message (what the websites are trying to convey), the medium (the reason for the appeal of the message for some people), and the receiver (to look at how they interpret the message and what they do with it).

The Perfect Storm: The Terrorist Message and the Online Media
Thomas Koruth Samuel, Director, Research and Publication Division, Southeast Asia Regional Centre for Counter-Terrorism, Ministry of Foreign Affairs, Malaysia

Thomas Koruth Samuel

Thomas Koruth Samuel observed that the online media has been a game changer for terrorist narratives, allowing the message to reach the global audience on an unprecedented scale. Thus, terrorist messages combined with delivery through online media, have created the environment necessary for online radicalisation. Policymakers will therefore need to find ways to counter terrorist narratives in cyberspace.

Samuel observed that terrorists have always been engaged in a battle of narratives with the authorities. Terrorists have put forth a narrative that explains their background, their justification and rationale for violence. This compelling message is focused on three premises: violence is the only way; violence is effective; and violence is acceptable.

While terrorists' message was both captivating and powerful, it remained at the fringes of society, impacting only a few. Samuel stated that online media has changed the rules of the game, providing terrorists' message with a potent delivery tool to reach a far greater audience in comparison with traditional media, which was limited in its reach and accessibility to terrorists. Several characteristics of online media contribute to these benefits.

Samuel first noted that online media, with its myriad tools, facilitates numerous ways (audio, visual, first person narration, discussion) to cater to various intellectual and emotional levels of different persons. This characteristic widens their pool of recruits to include far more diverse audience. Next, the usage of online media provided high return on investment, being user-friendly and requiring low resources in terms of expertise, funds and time. Another characteristic was that online media allows lone individuals to connect with like-minded people at a global level. This circumvents the need for individuals to be physically present at a certain time and space to be radicalised and indoctrinated.

Samuel also remarked that online radicalisation may take place without the fear of reprisal from authorities. Terrorists tend to exploit the difficulty in policing the Internet. For example, the majority of those advertising their actions on online media in Iraq and Syria remain unpunished. Similarly, one characteristic benefit of online media is the flexibility and convenience. Samuel noted that individuals are in control of their own level of radicalisation online. Additionally, online media allows terrorists to view the activities of other terrorists and subsequently replicate and duplicate successful strategies and techniques. The Internet thus provides valuable platform for terrorists to compare notes, learn from each other and avoid common pitfalls. Another characteristic Samuel observed was how the Internet acts as a repository that keeps alive the memories of deceased terrorists such as Moner Mohammad Abu Salha aka Abu Huraya with their images, videos, and statements. Finally, Samuel noted that the anonymity of the Internet allows terrorists to remain anonymous while carrying out their activities.

In conclusion, given the importance of the cyberspace in terrorist repertoire, Samuel advised that policymakers learn from terrorists' experience in online radicalisation when countering narratives in the online space.

Evolving Terrorist Uses of the Internet in Indonesia
Navhat Nuraniyah, Associate Research Fellow, Centre of Excellence for National Security (CENS) & Sulastri Osman, Independent Researcher, Jakarta

Navhat Nuraniyah

Sulastri Osman

Navhat Nuraniyah and **Sulastri Osman** examined the evolution of terrorist usage of the Internet through ten case studies in Indonesia. Their presentation evaluated the impacts of Internet use on operational success and attempted to answer the question of whether the Internet had significantly influenced terrorist operations in Indonesia.

The speakers noted that terrorist usage of the Internet should be viewed in the context of a rapidly advancing Indonesia, especially in the technological arena. Beginning in 2002, the Internet had played a role in terrorism cases in Indonesia. Imam Samudra, one of the perpetrators of the first Bali bombing in 2002, was also the pioneer of online extremism in Indonesia who conducted a failed cyber theft and made the case for jihadist usage of the Internet in his book.

Since then, online communication had been used in the planning and preparation phase of terrorist operations. The Internet also makes an ideal platform for establishing extremist presence and for the propagation of extremist narratives. Recently, for example, the Internet has been utilised for the propagation of Syria jihad narratives, which was framed as a sectarian war between Sunni and Shia and as part of the Final Battle. The Internet therefore represented an interactive and embedded form of communication for Indonesian jihadists, whereby the popularity of jihad by the pen and the rise of "jihobbyists" ensured that online media remained attractive for extremists over the years. Furthermore, the realisation of the ineffectiveness of mere violence as a way of gaining support caused Indonesian extremists to turn to the creation of their own jihadist world news agencies, which seek to shape public opinion through the Internet.

The Internet has also been used as a weapon by Indonesian terrorists through website hacking and defacement to issue threats that were combined with real world terrorists operations. For example, the Indonesian Armed Forces (TNI)'s website was defaced by the East Indonesian Mujahideen (MIT) group in 2013 in a bid to challenge authorities that were involved in counterterrorism operations.

The speakers noted that the Internet is also used in the instrumental sense in Indonesian jihadist websites, which contain tradecraft materials such as online bomb recipes. However, online tradecraft manuals are less popular among the experienced operators who prefer to supplement such manuals with real training camp. The manuals therefore appeal more to amateur jihadists, aiding their journey towards radicalisation. In addition, social media serves the function of networking for the purposes of recruitment and supporting real-time operations for terrorists in Indonesia. In 2014, Indonesian and Malaysian fighters for the militant group Islamic State (IS) networked over Facebook and formed a military unit in Shaddadi, Syria. Financial fraud and theft had also been conducted to facilitate online fundraising for the purpose of supporting terrorist operations.

The speakers observed that a new generation of Indonesian terrorists arose in 2010, all belonging to the youth category. Many of them are freewheeling individuals as opposed to the previous generation, which was characterised by operating within close-knit networks. The Internet supports and buttresses their operations, linking them up to the global jihadist networks without intermediaries. The new generation terrorists' motivations have also changed, with ideology taking a back seat. The first contact and recruitment modes have changed as well, with evidence of first contact made online, but real world nodes of interactions such as schools, alumni networks, religious study classes and prisons remain central for actual recruitment. Small cell dynamics are therefore still important to the process of radicalisation and eventual engagement in terrorist operations.

Discussion

In the discussion session, a participant wondered about the role of kinship and ideology in face-to-face versus online radicalisation. One speaker believed that ideology is as crucial in online radicalisation as offline. Another noted that online radicalisation is not always ideological, although it does represent a dimension. In the preliminary case study of terrorist usage of the Internet in Indonesia, the relationship between kinship and ideology is multi-faceted. Planning took place online through the consultation of online manuals and using the internet to identify targets, but real-life meeting is still crucial to the process of radicalisation. One panellist observed that there are regional and contextual differences in terrorist cases that involve the

Internet. In Muslim countries, physical ties are crucial in radicalisation processes. However, for the cases in Western countries, there had been reported cases of second generation Muslims who were radicalised without coming into contact with members of the community. The internet fed the knowledge seeking impulse of young Muslims in Western nations by providing answers to Islamic rulings and interpretations on different issues. A speaker agreed that the Internet provided more than just ideological justification for violence by consciously playing on the emotions of its audience. Their impact is therefore beyond logical arguments. Some cases of radicalisation involved being introduced through very emotional video. Internet is therefore a supplement to real life networks in the process of radicalisation.

PANEL 2

RADICALISATION OVER THE INTERNET: MECHANISM AND PROCESSES

Radicalisation over the Internet: Radicalism, Extremism and the Transition to Real-world Violence
Kumar Ramakrishna, Head, Centre of Excellence for National Security (CENS), RSIS

Kumar Ramakrishna

Kumar Ramakrishna started his presentation by highlighting how radicalisation is often an organised exercise of "talent spotting" by terrorist groups. Individual pathways to radicalisation may differ, but often involve deliberate acts by charismatic personalities. Ramakrishna opined that this aspect of radicalisation has remained salient as the evolution of jihadist groups such as Al Qaeda point to the "democratisation" and decentralisation of their network structures. Nonetheless, Ramakrishna stressed that there is a distinction between radicalism and extremism, the former posing challenges to the status quo through relatively peaceful means such as elections and protest actions.

Extremism on the other hand, is entirely different, for its adherents deem violence a legitimate tool in the pursuit of their goals; either as active perpetrators or passive facilitators. In this context, it can be argued that non-violent extremism can act as "safety valve", allowing the expression of dissent without a group or individual's direct conduct of violence. Ramakrishna argued that while there is some distinction between non-violent and violent extremists, both perspectives are only set apart by time; non-violent extremists would be more correctly seen as "not-yet violent" extremists. "Tipping points", as referred to by other terrorism researchers, can bring about behavioural changes. Common indicators of the emergence of tipping points include the expression by extremists of narratives of dehumanisation and retaliation against perceived opponents.

For example, the case of Muhammad Syarif of Jamaah Ansharut Tauhid (JAT) showed how violent extremism emerged from the non-violent extremist milieu. Syarif was reportedly prompted to violent action after exposure to the counter-culture narratives of JAT founder Abu Bakar Bashir.

Policymakers should therefore be aware of the threat of extremism, whether non-violent or violent. Ramakrishna recommended that all forms of extremism should be resisted to disallow the emergence of spaces for jihadist groups. It would not suffice to undertake kinetic approaches to terrorist groups. The larger extremist milieu should be neutralised to prevent the emergence of individuals like Syarif. In addition, governments and other stakeholders should also focus on better identifying tipping points. He underscored that there are multiple potential tipping points, which require holistic and comprehensive approaches to identify and address.

Pledges of Allegiance in Online Radicalisation Processes
Philipp Holtmann, Research Associate, Terrorism Research Initiative

Philipp Holtmann opened his presentation by citing how pledges of allegiance made by individuals or groups to entities like Islamic State (IS) was an exercise in "virtual leadership" and can provide a degree of "remote command-and-control (C2)". Another key characteristic of pledges is that they reinforce each other and can act as symbolic rites of passage.

Holtmann cautioned however that it remained unclear whether pledges are operationally relevant. He referred to how an Algerian group supporting IS seemed to take

orders from the latter, which led to the beheading of a French hostage. It was also highlighted how pledges of allegiance of various groups to IS have started an apparent "competition of pledges", which can be seen as the struggle of subordinate groups to establish links with IS. After outlining these trends, Holtmann described the various uses of the pledges. Pledges can be seen as a way to endorse the legitimacy of or directly "elect" a figurehead into positions of power. Another function of pledges is to act as indicators of subordination of command. Pledges can also be used as a marker for the peak point of radicalisation. A more abstract function of pledges is to act as demonstration of commitment to what is purportedly a greater Islamic cause.

The emergence of pledges as a part of jihadist iconography is a fairly recent phenomenon and can be considered an "organised marketing". From 2004-2006, members of Al Qaeda in Iraq (AQI) started making pledges to Al Qaeda Central, mostly though writing. Today, the primary method of making pledges has transitioned to online space, with social media acting as the main conduit for expressions of support to IS. Social media-delivered pledges can take multiple forms, ranging from recorded "pledges of investiture" to comments made on jihadist-posted YouTube videos. "Selfie" photos and Twitter pledges also have been used to make pledges. What binds these disparate methods is the apparent openness of IS, specifically its media strategists, to experiment. The goal for IS strategists is to use pledges as a nexus for attaining legitimacy and remote C2.

IS' thrust to legitimise itself should inform any initiatives to counter the effects of pledges. Holtmann recommends that questions be raised over the electoral function of pledges in order to undermine the leadership of IS "caliph" Abu Bakr al-Baghdadi. Presenting contrary narratives to positive images foisted by al-Baghdadi's supporters for instance must be sustained.

Getting Out of the Armchair: Potential Tipping Points for Online Radicalisation

Omer Ali Saifudeen, Lead Analyst, National Security Research Centre (NSRC), Singapore

Omer Ali Saifudeen

Omer Ali Saifudeen began his presentation by stressing that while the Internet may pose new challenges for radicalisation, lessons can be drawn from the pre-Internet age. He recalled how mass hysteria and panic resulted from Orson Welles' "War of the Worlds" broadcast. The incident demonstrated that the confluence of message, messenger, and messaging could lead to profound consequences. What online space provides is freedom of action for armchair jihadists to thrive. The Internet is intrinsically biased toward the emergence and persistence of counter-cultures. Whether jihadist or not, the Internet acts as an alternative for the dissemination of narratives that contest those of mainstream media.

Online radicalisation can be considered as an example of attitudinal shift, following exposure and interaction with an alternative counter-culture. Attitudinal shifts, in turn, are seen in an individual's changing beliefs (i.e. cognitive rethink) that cast doubts on mainstream ideals and drifting away from traditional social anchors. Attitudinal shifts can lead to behavioural changes, through the influence of 'tipping points'. Omer stressed that stakeholders should not overtly focus on an individual's tipping points but rather on what can tip over the masses. Neither should it be assumed that the tipping points to violence are limited to irrational factors. Citing other researchers, Omer underscored the importance of assessing the persuasiveness of tipping points. "Jihobbyists", while passive online supporters of groups such as IS, can have an instrumental role in disseminating messages that could motivate more active individuals with the means and capacity to engage in violence.

Omer remarked that tipping points are not always attached to the prominence of the messenger. Even amateur jihobbyists, given a "sticky" message, can contribute to mobilising others to act. An example of a sticky message offered by Omer was practical details on how to travel to Syria, which were more widely spread than ideological tracts rationalising why an individual should go to Syria. Omer cautioned that while jihadists' messages, messengers and messaging can be ubiquitous; there is no guarantee of veracity. Stakeholders must be self-aware that terrorists and terrorist groups can lie and fabricate false information.

In conclusion, Omer made several observations. First, it was reiterated that getting people out of the armchair is highly context dependent. What tipped over extremists in Middle East conflict zones may be irrelevant to those in Western Europe. Second, while the goals of jihadists may appear irrational, their transition from cognitive to behavioural extremism is often marked by a degree of instrumental rationality. Finally, Omer argued that there is no one factor that causes a tip over into violence. The message, the messenger, and messaging can collude and converge to provide the triggers for violence.

Limitations of Learning Terrorism Online

Michael Kenney, Associate Professor of International Affairs, Graduate School of Public and International Affairs, University of Pittsburgh

Michael Kenney

Michael Kenney introduced his presentation by recalling how early studies of terrorists' use of the Internet warned of the emergence of online terrorism universities. However, he remarked that terrorism research at the time made premature, sweeping claims over the utility of virtual training camps. Kenney remarked that terrorism requires a significant degree of knowledge. He further stressed that nuances between the types of knowledge required for a terrorist attack is oft-ignored by researchers and policymakers. Kenney distinguished between the abstract, technical knowledge (techne) and practical, experiential one (mētis).

Acquiring techne is a straightforward process, usually obtained through reading manuals or material containing information on military techniques or tradecraft. The proliferation of terrorist manuals is not a new phenomenon; 19th century anarchist movements were known to have collated and distributed bomb-making plans. At present, Al Qaeda's *Inspire* magazine exemplifies how modern-day terrorists seek to disseminate operational knowledge to a broad field of supporters and potential recruits. The 2003 Madrid Bombings are often cast as the perfect example of the feasibility of building bombs from instructions downloaded from the Internet. However, Kenney argued that Madrid was far from a perfect case, pointing out how other bombs in the attack failed to detonate.

Madrid not only demonstrated the unreliable products resulting from Internet-DERIVED operational manuals but also the poor adherence to tradecraft by self-taught terrorist operatives. Perpetrators of the Madrid bombings were immediately caught by Spanish security services by failing in counter-detection skills. Kenney pressed on further that as a whole, terrorists' skills are exaggerated, citing how "shoe bomber" Richard Reid was just one in a long line of "dumb terrorists" who lack mētis. The combination of poor, sometimes wrong bomb-making instructions and the ignorance of basic tradecraft translate into the limited capability of online-educated terrorist to conduct successful attacks.

Thus, real world training still matters to acquire mētis. But even with access to actual terrorist training camps, terrorist operatives still are limited by operational contexts once they embark on actual missions. Kenney observed how skills in guerrilla warfare do not translate well to conducting an urban terrorist attack. Local knowledge remains indispensable as shown in the case of the 7/7 London bombers, whose successful targeting of England's iconic public transport system owed more

to their British upbringing rather than their actual training as terrorist operatives. Kenney also recommended that stakeholders be sceptical of terrorist materials found online, as their release can provide greater utility as propaganda. Factually questionable manuals, while posing little actual threat, can help jihadists in exaggerating their perceived mastery of terrorist tactics. Kenney concluded that the Internet may be a useful complement for radicalising potential recruits but may be of little utility for disseminating operational knowledge.

Discussion

One of the issues raised was how global media appeared to pay little attention to the atrocities of the Nigeria-based Boko Haram. The panel opined that IS captured the attention of policymakers worldwide through the jihadist group's more international goals, in comparison to the localised objectives of Boko Haram. To a question whether religiously-inspired extremism is a result of the intrinsic nature of various faiths, the panel remarked that such was not the case albeit religion often provides an exclusivist, us-versus-them discourse which can be exploited for legitimising violence. Extremism by repressive governments was next discussed, with the panel highlighting how states are becoming more aware of the imperative to reduce collateral damage and to use non-kinetic counterterrorism measures. Also discussed was the role of women in jihadist movements. Panel members observed that the recent advances of IS have opened a range of roles for female supporters—ranging from all-female fighting brigades in Syria to alleged jihadist brides.

PANEL 3

LINKING THE DOTS: METHODOLOGICAL ISSUES AND RESEARCH IMPLICATIONS

The Growing Threat of Lone Wolf Terrorism

Jeffrey Simon, President, Political Risk Assessment Company, Inc.

Jeffrey Simon

Jeffrey Simon's presentation emphasised the growing threat of "lone wolf" radicalisation and the issues that may be overlooked when lone wolves are excluded from terrorism analyses. Simon highlighted the need to include lone wolves in terrorism studies to better assess their types and motivations and to understand how they might be radicalised through the Internet, which can affect how and how fast they carry out terrorist activities.

First, Simon asserted that terror acts perpetrated by lone wolves have great impact; there is little difference in the impact of attacks launched by lone wolves and organised groups. In this regard, there is a need to also consider "lone wolves" in the definitions of terrorism. By working alone, there is no group decision-making process nor is there communication between group members. This makes it difficult for them to be captured and encourages them to be innovative in their methods of attack. Thus, there is no constraint on the level of violence, which could possibly heighten the level of danger.

Simon identified five types of lone wolves: secular; religious; single-issue; criminal; and idiosyncratic. Secular lone wolves commit acts of terrorism for political and/or ethno-nationalist objective while religious ones act in the name of their religion. Single-issue lone wolves act for a single cause such as animal rights. Meanwhile, criminal lone wolves are usually motivated by financial gain and do not have any political, social or religious objective. It is for this reason that criminal lone wolves are usually not considered terrorists. Lastly, idiosyncratic lone wolves involve those who are mentally ill or schizophrenic, who might also be radicalised on their own. Simon gave as examples the perpetrators of the 2009 Fort Hood shooting and the 2013 Boston Marathon Bombings.

Second, the information found on the Internet might encourage radicalisation. Materials such as sermons and bomb-making instructions are easily found, providing potential lone wolves with limitless opportunities to be radicalised. Simon cited Roshonara Choudry as an example; she had downloaded sermons of Al-Awlaki and was influenced to fight in the cause of religion. Different lone wolves would also undergo different online radicalisation processes, which can influence how fast they execute their terrorist acts.

Simon reminded in his conclusion however, that the Internet too can be used objectively by the law enforcement and authorities to learn about lone wolves' activities beforehand. There have been cases in which lone wolves share what they know or have planned online, which can be used in investigations or to prevent terrorist activities from being executed. Anders Breivik, for instance, had posted his manifestos online before executing his plans. Thereby, challenges persist in studying terrorism when lone wolves are not given as much attention as organised terrorist groups. More research is needed on the potential threats of lone wolf terrorist, impacts and damage that could be inflicted, and the role of the Internet in their radicalisation processes.

The Use of Social Media in Social Sciences: Methodological and Ethical Considerations

Aaron Zelin, Richard Borow Fellow, Washington Institute for Near East Policy

Aaron Zelin

Aaron Zelin delved into the methodological and ethical issues that analysts should be cognisant of when carrying out research. Most importantly, Zelin emphasised the need for researchers to reflect on their own biases and how these may affect objectivity. He introduced five key methodological and ethical issues to take note of when conducting research using social media: understanding data collection; representative sample size; data extrapolation; online conduct; and contact with subjects.

First, Zelin explained that researchers would have to understand and consider properly the manner in which they collect data through social media. Researchers place themselves within the operating space of all social media interactions, and would not want to influence or affect the data found online. Zelin advised researchers to be cognisant of the sources from which data is collected, by differentiating them into official and unofficial data. They should assess the credibility of content, as some sources might actually be bogus accounts or contain deceptive information to trick researchers.

Second, Zelin emphasised the importance of obtaining a representative sample when attaining data. For instance, researchers should take into account Arabic sites and sources, which are often excluded. When collecting data, researchers should also be mindful that high numbers of visit to a particular website do not necessarily translate into its popularity because some users might try to artificially increase traffic to these sites. Third, once a data set is produced, Zelin warned researchers not to extrapolate excessively from the data, such that it becomes misinterpreted. Again, this is to minimise bias when analysing trends in the data.

Fourth, the manner in which a researcher conducts him or herself online is vital. They should contextualise online content and be aware of their role when viewing such information. This includes being able to balance the different sides of information received, as to ensure they are not influenced by researchers subjectivity. Further, he emphasised the difference between knowledge and promotion when analysing data, in which researchers might inadvertently be exploited by jihadists to promote their causes when the former use extremists' information without caution.

Fifth, similar concerns exist when the researcher makes contact with subjects. Relationships with subjects may affect how the researcher views information and data, and again may lead to the promotion of the jihadist cause instead. Researchers should be careful of private conversations in order not to compromise themselves; one should analyse but not advocate. They should also take precaution when contacting recruitment or financial hotlines, and ensure that their research takes minimal psychological toll on themselves.

Zelin concluded by acknowledging some limitations in online extremism research. Researchers are specialists but not experts. Official accounts and data are not likely to be holistic; some information might be removed or lost, or simply not found online – thus researchers can only learn so much from social media platforms. Lastly, Zelin noted the importance of conducting follow-up research to keep the data up to date.

Understanding Social Media: Ground Truths and Impacts on Counterterrorism

Carlo Pecori, Program Manager, Institute for the Study of Violent Groups, University of New Haven

Carlo Pecori's presentation showcased the research that he had conducted on the use of social media in more than twenty countries. It was divided into three sections: the importance of understanding the uses of social media; latter developments in the research; and the results of the study.

Carlo Pecori

First, Pecori emphasised the need to fully understand how social media is used in the country in relation to traditional media before using it or conducting research on it. Of particular interest was how social media was used for reporting purposes in the event of violence in the country. This was inspired by the onset of the Arab Spring and Osama Bin Laden raid, amongst other things. In 2011, the Mexican drug cartel activities were used for his initial study to analyse if the events that were reported in traditional media were also reported in social media. However, this produced a low and inaccurate percentage of incidences. Pecori attributed this to a lack of understanding of how Mexicans use social media: putting the cart in front of the horse.

Thereby and secondly, Pecori re-designed his study to first learn how social media was used in different societal contexts. The research was conducted by engaging local social media experts and analysing how social media is used in comparison to traditional media outlets. This allowed him to take a step back in understanding how social media is being used in the first place.

Accounting for factors such as age and education level, Pecori studied the trends present in the various countries. Several results emerged: Facebook proved to be most popular amongst the social media platforms; Twitter is generally disliked in developing countries although commonly used by the educated elites; and that such trends were made possible by the increase of mobile device usage across the states. Social media is not generally seen as a trustworthy source of information relative to traditional media. There are, however, exceptions such as in time of political crisis and uncertainty. During the Syrian uprising, for instance, Facebook became the most popular source of information in the area, outgrowing the popularity of traditional media despite difficulties to get reliable Internet connection.

Pecori concluded by illuminating some hurdles when studying social media usage in various countries. Firstly, despite the difficulties involved in building relationships with local experts, such engagement is necessary to get reliable data on the ground. Secondly, there is no academic discipline that solely studies social media; the interdisciplinary nature of social media research invites more disagreements than agreements by multi-disciplinary experts on social media. Lastly, there are issues of privacy and safety when studying online material and investigating cross-border trends, of which researchers should be mindful.

Discussion

One significant point raised was if lone wolves who actively participate in discussions and learning online may not do so in reality. In other words, social media may empower lone wolves through the production of extremist and terrorist materials online, but they may not be as powerful in real-life. This was followed by another related point on how researchers can separate between lone wolves or radicals who create 'noise' and those who do not but may be most dangerous. It was argued that it would be difficult to differentiate between the two because although online platforms could be a force strong enough to encourage radicalisation, whether or not it translates to violent behaviour depends on the individuals and their particular contexts. Nevertheless, the information shared on the Internet might shed light on the tipping point when any radicalised individual may take action. Another question raised was if it was acceptable to use pseudonyms when conducting research. It was argued that it would generally be acceptable if the researcher only meant to collect information. However, it would be unacceptable when the researcher is conducting ethnographic studies as the ethical reviews board of many institutions would not usually allow such practices.

PANEL 4

SOCIAL MEDIA ANALYTICS AND ONLINE EXTREMISM: CUTTING-EDGE TOOLS FOR RESEARCH AND INTELLIGENCE GATHERING

Social Media Analytics and Online Extremism: The Pros and Cons of Employing Cutting-edge 'Big Data' Tools

Maura Conway, Associate Prof. of International Security, School of Law and Government, Dublin City University

Maura Conway

Maura Conway provided an assessment of the research potential of "big data" tools. She underlined the technological evolution of the Internet and the fact that Web 2.0 has significantly changed the online landscape of violent extremism and terrorism. Groups and organisations used to have an extensive control over their online presence, which is no longer the case. She mentioned that the interactive nature of contemporary social media practices has not been fully understood by counter-strategists, and stressed the need for empirically-based social scientific research in addressing three core questions: the possibility of online radicalisation; the role of online interactions and consumption of online violent and non-violent extremist content; and the contours of the process of online radicalisation. Despite widely shared assumptions regarding the central role of the Internet in radicalisation processes as well as anecdotes related to online radicalisation, she believes that this issue has not been adequately addressed due to the lack of substantive empirical data.

In this respect, "big data" is essential to support any theory related to online extremism and to develop effective counter-strategies. Despite the different definitions of big data, Conway argued that it is still possible to achieve a large scale data collection and analysis. Given that social scientists are not used to collecting and analysing very large amounts of online data, she contended that a close collaboration with computer scientists was the easiest option. This solution can prove effective as computer scientists have various tools designed to gather and analyse a large amount of information. In addition, the sprawling nature of Web 2.0 makes computing power indispensable for social scientists, as the presence of violent extremism online scene represent a massive flow of information which cannot be fully grasped.

Conway mentioned the provision of huge amounts of detailed data among the advantages. The possibility of obtaining full data sets such as a complete information on a whole online forum was equally underlined, thus allowing instructive overviews of particular online and social media platforms. However, these methods are subject to three kinds of restriction. First, there are interpretative limitations due to the risks of online deception and misrepresentations. The veracity of the information is questionable, especially in view of the phenomenon of online loss of inhibition. Second, technical restrictions exist as current analytics tools do not necessarily reflect the complexity of online landscapes. They must be applied with caution and their use may entail specific training for classifiers. Moreover, access to source codes of social media platforms can be limited, therefore entailing constant updates. Third, there are ethical restrictions, specifically the ambiguous online identities of some Internet users. In view of these elements, it was suggested that the best solution involved a combination of large-scale quantitative data description, analysis and visualisation, combined with thorough qualitative analysis. The capacity to achieve these steps across platforms was an ultimate goal that should be pursued.

Weak Signals for Detecting Lone Wolf Terrorists in Social Media

Lisa Kaati, Senior Researcher, Swedish Defence Research Agency (FOI)

Lisa Kaati

In her presentation, **Lisa Kaati** described the methods and techniques used by analysts to detect weak signals of extremist behaviours. She focused on the detection of warning behaviours on social media, especially on the basis of online textual elements. Recalling that the search for potential lone wolf terrorists on the Internet is an arduous task, especially given the widespread nature of the virtual extremist and terrorist landscape, she characterised a weak signal as an indicator that can take various forms, including the expression of radical views, the activity in extremist environments and specific warning behaviours. An isolated weak signal was characterised as less helpful than the combination of several weak signals that might indicate a clear intent.

Based on the definition and the typology of warning behaviours developed by other scholars, Kaati enumerated three social media-relevant warning behaviours: fixation, identification, and leakage. While the fixation behaviour is likely to be revealed by the frequency of certain words, the identification behaviour may involve a strong feeling of association with a group, a cause and/or a particular figure such as that of a warrior. The latter feature is frequent in the case of lone wolf terrorists. It may also entail a strong interest in military-related elements such as weapons and strategies, potentially coupled with a narcissistic vision of oneself. Additionally, leaked information is made of action verbs and semantic relations that reveal a specific intent. For example, the manifesto released by Anders Behring Breivik the day of the 2011 Norway attacks was a model of leaked information. However, the collection of these data is limited by the use of different social media platforms and the potentially numerous usernames of a single person.

Shifting to the issue of profiling techniques based on textual elements and additional information released on social media, Kaati underlined the variety of personal information which can be obtained through computer-based analysis: data such as age, gender, and psychological profile of a social media user can be gathered on the sole basis of a text published on the Internet. Moreover, specific techniques such as stylometric analysis and activity analysis may also be applied. These methods create a unique digital fingerprint through the application of specific auto-recognition techniques which involve elements such as the use of function words; the length of the words used; the repetition of letters; the specific use of digits; the punctuation, the spelling and the links of sentences. The application of these techniques on 'big data' is particularly productive in the cases of blogs and discussion boards, but its usage is more restricted on textually limited networks such as Twitter. However, the results achieved through an appropriate combination of different methods were said to be promising. Citing the high potential of online detection, Kaati concluded by mentioning several promising research areas, including cross-social media platforms analysis; the collection of online information related to real-life identities of social media users and the assessment of capabilities of online groups focusing on activities such as hacking and bomb-making.

Tearing Down Walls: Analysing, Tracking and Contextualising Jihadist Media Operations and Their Audience Impact

Nico Prucha, Fellow, Department of Near Eastern Studies, University of Vienna

Nico Prucha examined the nature of extremist presence and expansion on social media. He underlined the missionary role of jihadist online materials, whose primary objective is to spread ideology. Similar to the importance of a multilingual approach, the figure of the media extremist has long been recognised as central, especially since the killing of Osama Bin Laden. Citing a

Nico Prucha

document published on social media by extremist media activists in 2013, Prucha highlighted two elements: a strong awareness of the impact of media actions on the enemy and the crucial role of a polyglot approach in challenging mainstream media, which involves the use of subtitles in all possible languages. The uninterrupted flow of jihadist content and its constant reproduction, dissemination, reprinting and reframing are equally noteworthy. In view of these elements, the current state of online extremist mobilisation was highly effective and sustainable, especially due to the media activism of the Islamic State (IS).

Three significant shifts were identified: a highly resilient social media structure, especially on Twitter, which accounts for the continuous dissemination of online content; the particularly elaborate use of different hash tags, thus widening the target audiences to non-Arabic speakers; a cross-platform phenomenon which mixes the inter-connected use of different social media platforms such as Twitter, Google+, Facebook and YouTube. Mentioning the wide dissemination of videos by Twitter, Prucha demonstrated how essential the use of this network was for jihadist groups. He also mentioned that the exponential use of social media platform by jihadists in the Syrian/Iraqi context was recent, dating back to 2012-2013. In addition, he explained that the flow of foreign fighters has boosted an already strong Syrian mobile phone culture. Contents posted on official IS accounts tend to mingle violent and humanitarian dimensions at varying levels, depending on the audience targeted, thus illustrating a strong capacity for adaptation. In another example, the theological dimension tends to be deliberately minimised in materials aimed at Western audiences, in order to make the message clearer.

A parallel was drawn between the infrastructure of online extremist mobilisation and the concept of netwar outlined by John Arquilla and David Ronfeldt: the central role of highly-committed small units is coupled with a wide range of support networks, thus reinforcing the interconnectivity of accounts and contents, while ensuring a high level of adaptability and resilience. Moreover, the hybrid structure of social media such as Google+, which combines the characteristics of YouTube and Twitter, can be particularly helpful. Citing the methodology used to measure the impact of this online activism and to understand the dissemination mechanism involved, Prucha underlined the centrality of social media accounts characterised by Arabic and non-Arabic language skills, as these virtual hubs play a crucial role in expanding the outreach of Jihadist documents. Besides these multilingual structures, the languages used remain an essential distinct criterion as the messages conveyed are different from a language cluster to another. He concluded by underlining the fact that it is impossible to permanently delete jihadist materials from the Internet.

Discussion

A participant enquired about the potential role of Muslim theologians and clerics in countering violent extremism. One of the speakers emphasised the necessity to challenge violent extremists whole-heartedly in the fields of religious authority and legitimacy. Another speaker underlined the central role of the media in amplifying the IS threat to the West, as well as a disproportionate amount of attention given to online violent extremists in Syria. Asked about the identification of relevant data in online radicalisation research, a speaker argued that the real issue involved was more about the methodology of data collection. The necessity to move from a middle level of analysis focusing on digital content to the study of online audiences was also highlighted. This would entail direct engagements with Internet users, focusing on issues such as motivations and reasons for online behaviour. On the usefulness of specific social media networks, it was argued that the research use of Facebook was both hampered by technical and ethical reasons. Twitter, on the other hand, was an easier platform to work with, given the openness of accounts and the accessibility of source codes. In conclusion, the evolving impact of social media was illustrated by the reference to YouTube, of which the radicalising influence in terms of online interaction seems to have diminished in recent years.

PANEL 5

COUNTERING ONLINE EXTREMISM

Countering Extremism Online: Adversarial Engagement in Dynamic Environment

Daniel Kimmage, Deputy Coordinator for Digital Presence, Center for Strategic Counterterrorism Communications, United States

Daniel Kimmage's presentation focused on the approach of adversarial engagement as a means of countering violent extremism online. He outlined the objectives of the approach, the challenges of managing a dynamic online environment and possible future scenarios that may unfold.

Online adversarial engagement methods are basically used to interrupt online interactive radicalisation processes. There are three overarching objectives: to contest the online space and provide alternative points of view in environments where violent extremists groups are able to distribute content without obvious impediment; introduce images, press reports and arguments in order to redirect the online conversations; and unnerve the adversary in providing alternative sources to push counter arguments and draw violent extremist groups into uncomfortable dialogue.

A number of operational challenges are present. In particular, the increasing diversity of social media platforms, the structure of violent extremist movements and the changing political context in many countries are important factors. Online platforms can be best characterised as a situation of "permanent impermanence"; this can be seen when managing data across many platforms and different levels of encryption that are built into the environment. Amid a dynamic online environment, a constant remains, namely the trade-off that more connectivity entails a less secure presence, a key consideration for government agencies.

Further complicating the process are fluctuations seen in the structures of violent extremists movements, with peripheral groups eclipsing previously established ones such as Al Qaeda. There are also regional differences; an example is the Boko Haram group which is deeply embedded in the context of northern Nigeria. This leads to a tension between the global framing of violent extremist movements and local politics. Lastly, the political context in the Arab region which is central to the movement has changed enormously. In an increasingly multi-polar world, this instability in the Arab region provides opportunities, especially for those with political revolutionary goals seeking to remake the fundamental order of societies.

Within this context, Kimmage saw three basic scenarios for future development: i) the golden age of radicalisation where violent extremists influences are spread effectively through medium such as peer-to-peer encrypted that are difficult to penetrate networks; ii) the beginning of a "long fade" where revulsion and resistance on online and social media to violent extremist ideology turns the tide of public opinion; and iii) the most likely scenario which is a combination of the first two scenarios in different parts of the world, providing a form of equilibrium.

While there is no certainty as to which of the scenarios will hold true, such conceptualisation allows for the identification and monitoring of trigger points and signs, which would better enable governments and law enforcement personnel to manage the challenges of online radicalisation. Looking forward, Kimmage noted that there is enormous potential for multi-disciplinary research in this area through the collaborative efforts of computer scientists, data scientists and regional experts.

Countering Online Extremism: A Perspective on the Indonesian case

Bilveer Singh, Adjunct Senior Fellow, Centre of Excellence for National Security (CENS), RSIS

Bilveer Singh

Bilveer Singh's presentation discussed the problem of online radicalisation and violent extremism and the ways to counter it from the Indonesian context. The presentation detailed the context of radicalisation in Indonesia, the current approaches taken by the authorities and the challenges faced in running an effective counter-radicalisation campaign. The presentation concluded with a review of the challenges faced in such endeavours.

Indonesia has had a long history of dealing with violent extremism, both in the physical domain as well as online. The Indonesian government has two broad-based strategies in place: a hard approach, which includes the formation of counter-terrorist operational units such as Densus 88 and a soft approach, which includes activities such as educational outreach and de-radicalisation efforts. However, the priority has been on hard approaches, with immediate results, rather than soft strategies where success is difficult to measure and achieve.

How is the idea of violent extremism sold online? Distinct from face-to-face human interactions, online activities are conducted through cyberspace. This has allowed violent extremist groups to disseminate ideas globally at very little cost, taking advantage of the vast stores of information online. These groups are also able to use the Internet to maintain virtual networks around the world and hide behind the cloak of anonymity where desirable. Further, said Singh, the spread of online violent extremism in Indonesia requires an in-depth understanding of the underlying historical, political, sociological, instrumental and governance factors that have drawn many towards the spread of violent ideology.

Countering online extremism requires a broad-based approach. This is pertinent in Indonesia given that its people are one of the top social media users in the world aided by the availability of cheap mobile and smart phones. To be effective, strategies will have to maintain a comprehensive counter-narrative that dismantles the underlying logic of the extremist narrative and make use of credible messengers and de-legitimise the message, morale and actions of the adversaries.

Singh noted that there are a number of approaches taken by the Indonesian government to counter the growing online threat. First are efforts made to take down sites which actively promote violent extremism. While this is effective as a short-term approach, in the long run many more sites will come up to replace the one that has been taken down. Second is the use of "black ops" tactics to contaminate existing sites. This requires much technical knowledge and funds. Third is by actively engaging in countering the narratives put forth by the extremists.

A number of key challenges are faced by the Indonesian government. A major stumbling block is the generational gap between policy-makers, a majority of whom are "digital migrants" unused to the fast paced changes of the online environment, and "digital natives", the younger generation of Indonesians who are tech-savvy as well as "message savvy"; they are thus able to manipulate the virtual dimensions in influencing others. In conclusion, Singh noted that the government needs to prioritise efforts to counter online radicalisation. There is a need to turn to the collaborative efforts of a good technical team as well as a cleric team in order to address the viral spread of extremist ideology.

Keyboard warriors: Realities of responding to virtual radicalisation

Elina Noor, Assistant Director, Foreign Policy and Security Studies, Institute of Strategic & International Studies (ISIS), Malaysia

Elina Noor

Elina Noor's presentation explored means to counter the appeal of virtual radicalisation through a structured, whole-of-society approach in responding to violent extremism online as well as offline. The presentation covered current measures in place to manage the threat of online radicalisation, operational challenges and concluded by proposing a number of solutions including educational measures that would promote critical thinking among the youth.

There is a range of current measures in tackling online radicalisation, from laws governing the cyber-domain to technical options and counter-narrative approaches. In terms of existing legislation governing the cyber-domain in the Association of Southeast Asian Nations (ASEAN) region, many are based on the interest of facilitating trade within the region, and are as such related more to data offences as well as the misuse of computers in general. As many of these laws are trade-driven, the key question to consider here is whether specific laws are needed to deal with online violent extremism. This is a question that law enforcement authorities are grappling with. In terms of technical measures, there are many options available including the removal of websites, filtering tools as well as the means to hide websites through the manipulation of algorithms and data analytics.

An important means of tackling online radicalisation are strategic approaches such as counter-narrative efforts, by the government as well as grassroots organisations. Online websites such as the United Kingdom-based Radical Middle Way aim to promote and propagate contemporary images of Islam that appeal to today's youth. The Religious Rehabilitation Group based in Singapore has also embarked on counter-narrative efforts online as well as offline. There has been an evolution in the past few years on how counter-narratives are conceived, to catch up and match the savvy messages of violent extremist websites.

However, the critical importance of language in counter- narratives and messaging should not be ignored. In particular, many have turned to the convenience of using terms such as mujahideen, jihadi and jihadists. Such terms are however, not clearly defined; may serve to validate the theological justifications used by extremists; and defiles the sanctity of the word jihad which has positive connotations for many Muslims through reduction of the term to a violent misinterpretation. Further, counter-narratives, especially messages that are propagated by government agencies, often come across as dry, contrived, reactive and not credible.

Noor argued that the bulk of the work in countering online radicalisation must be done offline. This is a more strategic, longer-lasting form of countering the threat. Efforts in this regard should include tackling the root causes of extremism and terrorism such as socio-economic causes that drive people towards violent extremism. In managing violent extremism that is predicated on ideological or a blinkered religious lens, education plays a key, preventive role. The education systems in many countries in the region do not prioritise critical thinking skills. The role of educators, parents and civil society organisations in promoting critical thinking is needed to equip the youth to question and challenge, especially in today's information age.

Victims' Voices: Going Online

Max Boon, Associate Fellow, International Centre for Counter-Terrorism, The Hague

Max Boon

Max Boon stressed the importance of victims' and former terrorists' voices in educating people about the destructive effects of terrorism. He highlighted this point by sharing his story as a victim of the 2009 Marriot Jakarta terrorist bomb attack. As a co-founder of Aliansi Indonesia Damai/Alliance for a Peaceful Indonesia (AIDA), Boon discussed the organisation's developing online presence that could complement its offline activities such as trainings and workshops. AIDA aims to empower, train, and mobilise victims and former terrorists in Indonesia through positive and constructive dialogue and never in destructive- and negative-based confrontation. Boon argued that the main aim of terrorists is not to inflict pain on the victims of their attack but to instil fear and chaos in the society. However, they do cause much direct pain by hurting and killing many innocent civilians and thus should be confronted with this reality. The dialogues are conducted with victims that terrorists could identify with, that is, fellow Indonesians preferably from the region where they came from and speaking the same language.

Another objective of AIDA is to prevent young people from choosing the path of violent extremism. Through its outreach projects, AIDA brings a team of three to five victims along with a former terrorist and a religious leader to schools and villages where they share their stories. The former terrorists talk about the beginning, height, and end of their involvement in terrorism. The victims share their stories and show how damaging terrorism is, hoping to make young people realise that victims of terrorist attacks could easily be their family members or loved ones. Boon pointed out that the results of the outreach sessions have been very promising and thus AIDA plans to reach out to more communities and religious organisations

Boon also discussed the online measures that AIDA takes. AIDA's website and social media accounts feature newsletters, weekly updates, multimedia presentations, and profiles and interviews of several victims. The Facebook and Twitter pages of AIDA are also presented to the audience during school visits. As most stories in the media present the logic of the perpetrators, Boon explained that AIDA tries to present what these violent extremists actually cause and counter their narrative.

During outreach activities, the concept of peace is highlighted and an interactive dialogue discussing life's challenges and resilience is conducted. Boon is hopeful that AIDA will continue to make a difference in the views of young people in Indonesia.

Countering the Spread of Terrorism through the Internet: Perspectives from the OSCE

Mehdi Knani, Programme Manager on Countering Violent Extremism and Radicalisation that Lead to Terrorism, Organization for Security and Co-operation in Europe, Transnational Threats Department

Mehdi Knani

Representing the Organization for Security and Co-operation in Europe (OSCE), **Mehdi Knani** discussed the need for using a comprehensive and cooperative approach that recognises human rights, due process, and rule of law in countering terrorism. OSCE puts a

strong emphasis on the question of human rights and tries to help governments and stakeholders identify human rights-compliant solutions for terrorism. The organisation conducts policy workshops, training, seminars, and field research for governments, security agencies, businesses, and the public.

Knani explained that OSCE is dedicated to promoting non-punitive and positive approaches to fight extremism online as the risk of violating human rights and fundamental freedoms, especially the freedom of expression, freedom of the media, and the right to privacy, is very high. It is necessary to develop different, tailored, and targeted approaches for counter-terrorism solutions to be both human rights-compliant and effective.

Positive use of social media and alternative messages and trying to understand the intended audience are ways to ensure that human rights are recognised. In addition, promoting tolerance and non-discrimination as well as combating hate speech and crimes, though not usually labelled as direct solutions to terrorism, could contribute to the conduct of positive approaches to counter extremism.

Knani also pointed out that some governments have the tendency to violate the rule of law and due process when dealing with extremism. For instance, some states want to criminalise extremism without even defining what extremism is. In this case, it would be easy for governments to use counter-terrorism laws to merely stifle and silence political dissent. Therefore, it is essential to draw clear lines to ensure legitimacy, lawfulness, and effectiveness.

In sum, Knani recommends the following actions to counter online terrorism: defining precisely and clearly the scope for disciplinary action in accordance with human rights and the rule of law; devoting more time and effort in promoting the positive use of various online media; focusing on internet end-user empowerment and resilience by promoting internet literacy and raising awareness especially among the youth and also parents; combining online and offline approaches in a coherent fashion; and developing public and private partnerships involving the state, human rights organisations, business, and civil society.

Countering Online Extremism: Keeping up with the Changing Threat Landscape

Nur Azlin Md Yasin, Associate Research Fellow, International Center for Political Violence and Terrorism Research (ICPVTR), RSIS

Nur Azlin Md Yasin

For **Nur Azlin Md Yasin**, dealing with the root causes and direct enablers of radicalisation is a fundamental tool in keeping with the changing threat landscape. As extremism is both an online and offline problem, a holistic approach is required in order to face the changes and challenges. Root causes are factors that have contributed to a person's attraction to extremist materials. It pertains to one's past experiences (usually negative) and struggles in life. For instance, a person who is in need of an identity or has been discriminated against could be prone to radicalisation. Yasin added that people have biases in them that make them more susceptible to being affected by particular materials and messages. On the other hand, direct enablers include extremist materials and messages as well the instruments that entice followers such as ideologically related publications and websites.

Yasin also added that it is imperative to study what appeals to the supporters of extremist groups. Each group has a different kind of charisma and they attract many supporters. For instance, the supporters of the group Malaysian Fighters are presented with a credible Islamic façade. Also, the members share stories about their wives and families, which are very easy to relate to. Thus, they appear tolerant and legitimate when they are in fact violent.

When it comes to dealing with root causes and direct enablers, Yasin argued that the following have

important roles to play: international community and mainstream media; community centres; mosques; wider audience; governments; and parents and/or the family. The international community and mainstream media should be more direct and tough in identifying extremist materials as extremist—there is a need to "call a spade a spade". Also, there are people who doubt the reliability of mainstream media, which result in them turning to alternative news agencies that are usually replete with ideologies.

Community centres should propagate counter-ideologies through educational materials that target direct enablers of radicalisation. As most countries already have platforms and networks that can reach out to youths and various communities, this could be carried out effectively through the existing platforms. There should also be programmes that allow debates and dialogues. Mosques should be able to give sermons on identity, purpose, and meaning of life. Such sermons could resonate with those who are struggling with identity issues or searching for their path in life.

Apart from radicals, mainstream ordinary citizens, as well people who are anti-radicalisation should also be looked at. It is important to understand what makes people resist or oppose radical ideology. This could be a source of information and suggestions for targeting different audiences. To be sure, governments should assist in the promotion of moderation and the ideology of peace. However, they should understand their limitations to avoid besmirching the credibility of counter-extremist ideology materials. And lastly, parents and families play an influential role in the mind-set of young people and thus they should always be present in their lives.

Discussion

A question was posed on the approaches to better engage civil societies in tackling online violent extremism. A speaker remarked that one of the ways to approach civil society may be to engage them on issues which are of interest to them. This would depend on the context in different countries.

It was noted that there appears to be more people visiting extremists websites compared to mainstream websites and asked what would be needed to change the situation. It was suggested that government counter narratives will always have to play catch-up to extremist narratives; as such, critical thinking skills and an environment that promotes the questioning of sensitive topics such as religion are important means of preventing the spread of violent extremist influences.

A question was raised on how to define and measure the effectiveness of violent extremist countermeasures. It was stressed that an exact measurement of effectiveness is impossible to achieve, thus qualitative methods should be used. One way to measure effectiveness is by evaluating attitudes towards violence before and after outreach activities by conducting surveys and interviews. While measuring effectiveness is an important means of gauging the success or otherwise of particular programs, soft approaches in combating online violent extremism would generally need longer time spans in order to be effective.

MODERATED DISCUSSION

The moderated discussion was aimed to facilitate a frank discussion on how to move forward with policy initiatives and research on extremism and terrorism online. Several themes emerged in the discussion: utility of effective counter-narratives; the role of civil society both online and offline; methodological and ethical issues in terrorism research; and the gaps in online extremism and radicalisation research.

It was noted that an effective counter-narrative required three elements, namely the message, messenger, and messaging. With regard to the message, it is instructive that counter-narratives should not be reactive but rather focused on a positive message (i.e. promoting peace). A more nuanced approach in choosing the right messenger and messaging method could be done by engaging different types of ulama for different target groups. While moderate ulama might be widely accepted among the majority of Muslims, Salafi ulama might carry more weight when trying to dissuade individuals who have been radicalised. A focused target group is therefore crucial in counter-narrative.

The participants acknowledged the importance of a whole-of-society approach in countering violent extremism (CVE), as it was essential not to alienate the moderate majority in the effort to curtail the extremist minority. Spontaneous grassroots initiatives have been successful in some countries. Some civil society organisations that focused on online campaigns had worked with youth to make their campaigns more appealing to young people. In the offline realm, a local Muslim community in Germany had successfully reclaimed a mosque from an extremist group. It was noted that despite recent campaigns such as the #notinmyname campaign to counter Islamic State (IS) propaganda, grassroots initiatives are still limited due to funding shortage and lack of innovative ideas. The participants raised some practical solutions to these problems; including public-private partnerships; and a three-way communication between researchers, the government, and civil society. Private sectors should be involved to tackle funding problems. To improve the effectiveness of government policies and grassroots initiatives, such efforts needed to be informed by sound research.

One of the points raised regarding methodological issues was that former extremists often experienced "research fatigue", with some respondents having prepared scripted responses – thus posing a major challenge to the validity of interview-based research. It was recommended that researchers be more creative in coming up with new questions and fresh angles when interviewing former terrorists. Researchers are also faced with ethical dilemmas, one of which is balancing between researchers' interest in maintaining relationship with respondents and law enforcement concerns. While it was acknowledged that researchers are responsible for alerting law enforcement authorities when detecting a potential threat, complication might arise when the safety of the respondents' family is compromised. The participants agreed that such ethical issues and moral dilemma deserved more attention in terrorism research literature. Looking forward, some research gaps were identified, including the need for empirical research on whether online extremism might actually reduce violent extremism in the real world as the internet becomes a "safe place" for expressing radical and extremist views.

LIST OF SPEAKERS AND CHAIRPERSONS

SPEAKERS

Anne Stenersen
Research Fellow
Terrorism Research Group
Norwegian Defence Research Establishment (FFI)
Norway

Anne Aly
Research Fellow
School of Media, Culture & Creative Arts
Curtin University
Australia

Thomas Koruth Samuel
Director, Research and Publication Division
Southeast Asia Regional Centre for Counter-Terrorism
Ministry of Foreign Affairs
Malaysia

Navhat Nuraniyah
Associate Research Fellow
Centre of Excellence for National Security (CENS)
S. Rajaratnam School of International Studies
Singapore

Sulastri Osman
Independent Researcher
Jakarta, Indonesia

Kumar Ramakrishna
Head
Centre of Excellence for National Security (CENS)
S. Rajaratnam School of International Studies
Singapore

Philipp Holtmann
Research Associate
Terrorism Research Initiative
Vienna, Austria

Omer Ali Saifudeen
Lead Analyst
National Security Research Centre (NSRC)
Singapore

Michael Kenney
Associate Professor of International Affairs
Graduate School of Public and International Affairs
University of Pittsburgh
United States

Jeffrey Simon
President
Political Risk Assessment Company, Inc.
United States

Aaron Zelin
Richard Borow Fellow
Washington Institute for Near East Policy
United States

Carlo Pecori
Program Manager
Institute for the Study of Violent Groups
University of New Haven
United States

Maura Conway
Associate Prof. of International Security
School of Law and Government
Dublin City University
Ireland

Lisa Kaati
Senior Researcher
Swedish Defence Research Agency (FOI)
Sweden

Nico Prucha
Fellow
Department of Near Eastern Studies
University of Vienna
Austria

Daniel Kimmage
Deputy Coordinator for Digital Presence
Center for Strategic Counterterrorism Communications,
United States

Bilveer Singh
Adjunct Senior Fellow
Centre of Excellence for National Security (CENS)
S. Rajaratnam School of International Studies
Singapore

Elina Noor
Assistant Director
Foreign Policy and Security Studies
Institute of Strategic & International Studies (ISIS)
Malaysia

Max Boon
Associate Fellow
International Centre for Counter-Terrorism
The Netherlands

Mehdi Knani
Programme Manager
Countering Violent Extremism and Radicalisation that Lead to Terrorism
Organization for Security and Co-operation in Europe
Transnational Threats Department

Nur Azlin Md Yasin
Associate Research Fellow
International Center for Political Violence and Terrorism Research (ICPVTR)
S. Rajaratnam School of International Studies
Singapore

CHAIRPERSONS

Norman Vasu
Deputy Head
Centre of Excellence for National Security (CENS)
S. Rajaratnam School of International Studies
Singapore

Damien D. Cheong
Research Fellow
Centre of Excellence for National Security (CENS)
S. Rajaratnam School of International Studies
Singapore

Shashi Jayakumar
Deputy Head
Centre of Excellence for National Security (CENS)
S. Rajaratnam School of International Studies
Singapore

Kumar Ramakrishna
Head
Centre of Excellence for National Security (CENS)
S. Rajaratnam School of International Studies
Singapore

Sulastri Osman
Independent Researcher
Jakarta, Indonesia

ABOUT CENS

The **Centre of Excellence for National Security (CENS)** is a research unit of the S. Rajaratnam School of International Studies (RSIS) at Nanyang Technological University, Singapore. Established on 1 April 2006, CENS is devoted to rigorous policy-relevant analysis of a range of national security issues. The CENS team is multinational in composition, comprising both Singaporean and foreign analysts who are specialists in various aspects of national and homeland security affairs.

Why CENS?

In August 2004 the Strategic Framework for National Security outlined the key structures, security measures and capability development programmes that would help Singapore deal with transnational terrorism in the near and long term.

However, strategising national security policies requires greater research and understanding of the evolving security landscape. This is why CENS was established to increase the intellectual capital invested in strategising national security. To this end, CENS works closely with not just other RSIS research programmes, but also national security agencies such as the National Security Coordination Secretariat within the Prime Minister's Office.

What research does CENS do?

CENS aspires to be an international research leader in the multi-disciplinary study of the concept of resilience in all its aspects, and in the policy-relevant application of such research in order to promote security within and beyond Singapore.

To this end, CENS conducts research in three main domains:

- *Radicalisation Studies*
  The multi-disciplinary study of the indicators and causes of violent radicalisation, the promotion of community immunity to extremist ideas and best practices in individual rehabilitation.

- *Social Resilience*
  The inter-disciplinary study of the various constitutive elements of social resilience such as multiculturalism, citizenship, immigration and class. The core focus of this programme is understanding how globalized, multicultural societies can withstand and overcome security crises such as diseases and terrorist strikes.

- *Homeland Defence*
  A broad domain researching key nodes of the national security ecosystem. Areas of particular interest include the study of strategic and crisis communication, cyber security and public attitudes to national security issues.

How does CENS help influence National Security Policy?

Through policy-oriented analytical commentaries and other research output directed at the national security policy community in Singapore and beyond, CENS staff members promote greater awareness of emerging threats as well as global best practices in responding to those threats. In addition, CENS organises courses, seminars and workshops for local and foreign national security officials to facilitate networking and exposure to leading-edge thinking on the prevention of, and response to, national and homeland security threats.

How does CENS help raise public awareness of National Security issues?

To educate the wider public, CENS staff members regularly author articles in a number of security and intelligence-related publications, as well as write op-ed analyses in leading newspapers. Radio and television interviews have allowed CENS staff to participate in and shape the public debate on critical issues such as radicalisation and counter-terrorism, multiculturalism and social resilience, as well as crisis and strategic communication.

How does CENS keep abreast of cutting edge National Security research?

The lean organisational structure of CENS permits a constant and regular influx of Visiting Fellows of international calibre through the Distinguished CENS Visitors Programme. This enables CENS to keep abreast of cutting edge global trends in national security research.

For more information about CENS, visit http://www.rsis.edu.sg/cens

ABOUT RSIS

The **S. Rajaratnam School of International Studies (RSIS)** was established in January 2007 as an autonomous School within the Nanyang Technological University. Known earlier as the Institute of Defence and Strategic Studies when it was established in July 1996, RSIS' mission is to be a leading research and graduate teaching institution in strategic and international affairs in the Asia Pacific. To accomplish this mission, it will:

- Provide a rigorous professional graduate education with a strong practical emphasis,
- Conduct policy-relevant research in defence, national security, international relations, strategic studies and diplomacy,
- Foster a global network of like-minded professional schools.

Graduate Education in International Affairs

RSIS offers a challenging graduate education in international affairs, taught by an international faculty of leading thinkers and practitioners. The Master of Science (MSc) degree programmes in Strategic Studies, International Relations, Asian Studies, and International Political Economy are distinguished by their focus on the Asia Pacific, the professional practice of international affairs, and the cultivation of academic depth. Thus far, students from more than 50 countries have successfully completed one of these programmes. In 2010, a Double Masters Programme with Warwick University was also launched, with students required to spend the first year at Warwick and the second year at RSIS.

A small but select PhD programme caters to advanced students who are supervised by faculty members with matching interests.

Research

Research takes place within RSIS' six components: the Institute of Defence and Strategic Studies (IDSS, 1996), the International Centre for Political Violence and Terrorism Research (ICPVTR, 2004), the Centre of Excellence for National Security (CENS, 2006), the Centre for Non-Traditional Security Studies (Centre for NTS Studies, 2008); the Temasek Foundation Centre for Trade & Negotiations (TFCTN, 2008); and the Centre for Multilateralism Studies (CMS, 2011). The focus of research is on issues relating to the security and stability of the Asia Pacific region and their implications for Singapore and other countries in the region.

The school has five professorships that bring distinguished scholars and practitioners to teach and to conduct research at the school. They are the S. Rajaratnam Professorship in Strategic Studies, the Ngee Ann Kongsi Professorship in International Relations, the NTUC Professorship in International Economic Relations, the Bakrie Professorship in Southeast Asia Policy, and the Peter Lim Professorship in Peace Studies.

International Collaboration

Collaboration with other professional schools of international affairs to form a global network of excellence is a RSIS priority. RSIS maintains links with other like-minded schools so as to enrich its research and teaching activities as well as adopt the best practices of successful schools.

ABOUT NSCS

The **National Security Coordination Secretariat (NSCS)** was set up in the Prime Minister's Office in July 2004 to facilitate national security policy coordination from a Whole-Of-Government perspective. NSCS reports to the Prime Minister through the Coordinating Minister for National Security (CMNS). The current CMNS is Deputy Prime Minister and Minister for Home Affairs Mr Teo Chee Hean.

NSCS is headed by Permanent Secretary (National Security and Intelligence Coordination). The current PS (NSIC) is Mr Benny Lim, who is concurrently Permanent Secretary (National Development) and Permanent Secretary (Prime Minister's Office).

NSCS comprises two centres: the National Security Coordination Centre (NSCC) and the National Security Research Centre (NSRC). Each centre is headed by a Senior Director.

The agency performs three vital roles in Singapore's national security: national security planning, policy coordination, and anticipation of strategic threats. It also organises and manages national security programmes, one example being the Asia-Pacific Programme for Senior National Security Officers, and funds experimental, research or start-up projects that contribute to our national security.

For more information about NSCS, visit http://app.nscs.gov.sg/public

RSiS
Nanyang Technological University
S. RAJARATNAM SCHOOL OF INTERNATIONAL STUDIES

Nanyang Technological University
Block S4, Level B4, 50 Nanyang Avenue, Singapore 639798
Tel: +65 6790 6982 | Fax: +65 6794 0617 | www.rsis.edu.sg