COLLABORATIVE RESEARCH ON COUNTERING EXTREMIST VIOLENCE

NEW INSIGHTS ON COUNTERTERRORISM ISSUES: CANADIAN FOREIGN FIGHTERS; ONLINE RECRUITMENT; AND THE FUTURES OF TERRORISM

February 26, 2016

Held in Ottawa, this one day workshop of the *Canadian Network for Research on Terrorism, Security and Society* (TSAS) presented updated findings from TSAS's three collaborative research projects funded under the Canadian Safety and Security Program (CSSP), led by *Defence Research and Development Canada*'s Centre for Security Science (DRDC CSS): the empirical study of Canadian foreign fighters; the emergence and evolution of violent narratives in online forum networks; and the future(s) of terrorism, 2015-2025. The agenda was, accordingly, divided into three hour-and-a-half segments, each encompassing a formal presentation by the researcher(s) and an open discussion held under the Chatham House rule.

Deliverable 2.1.3

The Puzzle of Radicalization: Insights from the Study of Foreign Fighters

Lorne Dawson (University of Waterloo)
[with the collaboration of **Amarnath Amarasingam** (Dalhousie University), **Alexandra Bain** (St Thomas University)]

In the opening session, Dr. Lorne Dawson presented an overview of the theoretical approach, methodology, and tentative findings that have emerged from his research conducted jointly with Drs. Amarnath Amarasingam and Alexandra Bain on the topic of Canadian foreign fighters.

He opened the presentation with a review of the broad scope of literature applicable to foreign fighters and the question of radicalization more broadly. His review emphasized that at the research's core is a problem of social action: a wide portion of the population may hold certain *grievances*, yet only a small minority of these individuals will engage in *social action* to promote their cause, and an even smaller minority will actually resort to *violence* in the same pursuit. While this problem is true in all social movement contexts, it is particularly acute in the case of terrorist radicalization: grievances do play an explanatory role in explaining why individuals turn to terrorism, but they are insufficient. This project aims to contribute to the radicalization literature by adding to our empirically-founded understanding of which factors best explain the process of radicalization that leads individuals to engage in foreign fighting. The researchers' qualitative approach presents an advantage over quantitative studies in this area, since it is better able to tease out the processes underlying observed correlations.

The project's approach is three-pronged. First, the researchers set out to develop—based on an analysis and synthesis of existing literature—a social ecology model of the foreign fighter phenomenon, encompassing the social conditions of "late modernity"; the immigrant experience; youth culture & rebellion; ideology; and group dynamics. Second, they drew on comparative dimensions with new religious movements and their corresponding literature to frame understandings of conversion and recruitment, commitment mechanisms, and causes of violence. Third, they have conducted qualitative interviews with foreign fighters; their family, friends and associates; as well as “wannabe” fighters and other online supporters. At the time of presentation, the research team had conducted field interviews of over 130 individuals (of all nationalities) across these categories—a significant augmentation of their original plan to interview approximately 40 Canadians. While some of these “interviews” are conducted in a conventional face-to-face manner (e.g., with parents of foreign fighters), and some were done on Skype, the majority of the interviews with the actual fighters in Syria and Iraq comprise extended social media dialogues, sometimes spanning months. This extended period of contact is often necessary to gain the individuals’ trust, and uncover interview content beyond the “party line” veneer.

While the research is still ongoing and unlikely to yield satisfyingly rigorous analysis for another year, Dr. Dawson presented tentative takeaways from the team’s current impressions of the data. He organized these findings into three, interrelated categories: background issues and radicalization; the role of the religio-political nexus; and the role of the online community.

Dr. Dawson presented two key ideas with respect to foreign fighters’ background issues. First, what seems to be emerging—although he acknowledges that this finding may be accidental, due to small sample size—is a bifurcation into two antithetical stereotypes. While some foreign fighters—almost all of whom are converts—are troubled youth from stereotypical broken families, engaging in activities such as drug abuse and petty crime, others appear to be the opposite: they come from “normal” families; are successful in school or work; and are described as good-natured, outgoing, and friendly. Research in new religious movements has found a similar bifurcation in recruits’ backgrounds, which also seems to parallel the typology of terrorist group joiners described by Petter Nesser (2010). The researchers intend to push their analysis further, to evaluate whether their foreign fighter sample truly falls into such “types” of individuals. While it is easy to focus on the “low-hanging fruit” of the first group (with individuals such as Damian Clairmont), it may be members of the second group (such as Salman Ashrafi) who are more influential.

Second, interviews with family and friends have revealed that many foreign fighters are very good at keeping their radicalization process secret from the people closest to them. Family members frequently expressed their unawareness that the radicalization process was underway, but could clearly point to indicators (e.g. change in peer group, withdrawn nature, etc.) in hindsight, while offering deep reflection with respect to their causes. Peers were more likely to note obvious behavioural signs, but—as is characteristic of youth—would be inclined to treat them on a superficial level and dismiss them.

With respect to the religio-political nexus, the interviews have confirmed that most foreign fighters are converts, or Muslim-born youth “reaffirming” their dedication to Islam (which mirrors standard processes of adolescent conversion). But the literature is divided with respect to whether religion actually plays a meaningful role in the radicalization process. The interviews conducted thus far demonstrate that the Salafi-jihadist framework is crucial to these individuals’ understandings of themselves and their worldviews, and interviewers must treat it as a valid motivation in order to gain these individuals’ trust. The researchers find that it is not these individuals’ theological orthodoxy or knowledge that is necessarily important (indeed, the religion hypothesis is frequently dismissed because these individuals’ practice and knowledge of Islam is often abysmal), but their *religiosity*: their level of commitment, and the way in which they fuse their identity with the Salafi ideology. Simultaneously, however, religion is also used as a gloss in the interviewees’ discourse; they easily resort back to religious explanations for everything, even when other dynamics are truly motivating their behaviour.

With respect to the role played by the online community in the radicalization process, the Baqiya ("enduring") Community is more than just a simple network or forum for communication. It is a thriving online Salafi-jihadist community, where interactions delve beyond the political, into everyday personal matters and interactions. Evidence of these deep personal connections is found in the online community's response to the death of perpetrator Elton Simpson, in the 2015 Curtis Culwell Center attack in Garland, Texas. The immediate wave of response felt throughout the community encompassed the standard martyrdom discourse, but it also took on a tone akin to what would be expected in response to the accidental death of a high school quarterback: posts emphasized where they had med Simpson, what a "nice guy" he was, and other such personal sentiments. For radicalized and radicalizing individuals, online life is of incredible importance, and provides meaning to their "real-world" lives. The online world is of such immense significance that some view their online activities as a substitute for fighting abroad; they interpret—to the dismay of some fighters on the ground—the shutdown of social media accounts as a form of "online martyrdom": a mark of prestige.

Taken together, these findings point to six elements of the radicalization process. In the researchers' working hypothesis, individuals radicalized to becoming foreign fighters: (1) face acute (emerging adult) identity struggles, and are, for various reasons, (2) conditioned by a moralistic—rather than political or psychological—problem frame and (3) an inordinate quest for significance, to "matter," or to "have a purpose." These struggles are (4) resolved with a religious ideology, as well as a fantasy component. When combined with (5) the psychological impact of small group dynamics and charismatic leadership, the result is (6) identity fusion, whereby the individual loses his or her aspirations of autonomy, and effectively merges with a group and cause. On their own, each of the process's components are remarkably ordinary. However, through the way in which these elements interact, radicalized individuals end up in an extraordinary situation where they are willing to do extraordinary things to other people and themselves (i.e. carry out brutal acts of violence and willingly face death).

Deliverable 2.2.5

The Emergence and Evolution of Violent Narratives in Online Forum Networks

Martin Bouchard, Bryan Monk, Evan Thomas, and Philippa Levey (Simon Fraser University)

[with the collaboration of **Richard Frank**, and research assistance from **Sadaf Hashimi** and **Joseph Mei** (Simon Fraser University)]

This project on the emergence and evolution of violent narratives in online forum networks is the outcome of a collaborative team effort; a multidisciplinary collaboration underscored by this session's joint presentation by Dr. Martin Bouchard, and three graduate students: Brian Monk, Philippa Levey, and Evan Thomas. After Dr. Bouchard's introductory remarks, the presentation proceeded in three sections. First, Mr. Monk described the data collection system and process of sentiment analysis, used as the project's foundation. Second, Ms. Levey presented her qualitative, micro-analysis of how violent sentiment evolved in relation to the transition from adolescence to adulthood. Third, Mr. Thomas presented a macro-view of ISIS forums and the followers of ISIS online, focusing on the impact of opinion leadership and external events on forum participants.

Mr. Monk presented the project's technological component: a data collection system, developed by computer scientist-turned-criminologist Dr. Richard Frank. Mr. Monk illustrated how the system exploits the structure of online forums to efficiently extract relevant details from a massive quantity of data, walking workshop participants through an example of how the web crawler works. In the time since this tool was presented at last year's TSAS meeting, Dr. Frank replaced the originally-cumbersome, offline system, with a new web-based system that integrates a wide range of databases incorporating forums in areas beyond jihadism (including, for instance, right-wing extremism, hacking, and fraud). This new system is interactive, and allows the researchers to independently (i.e. without the aid of the computer science team) query all of the forums simultaneously.

The data collection system also incorporates "sentiment": a subjective classification for words. Using Harvard's *General Inquirer* lexicon as well as human-coded data sets, *SentiStrength* software gauges the positivity and negative of a supplied text, based on features of the language. For this project, the researchers used a scale configuration to sum sentences' sentiment scores, to give an indication of *how* negative or positive a post was (as opposed to simply the trinary indicator of whether it *was* positive, negative, or neutral). While sentiment constitutes a powerful tool, it is limited by its inability to take context into consideration (for instance, the sentence "That's great news that you're planning on moving to Syria to fight for ISIS" would receive a positive sentiment score, even though it is indicative of a preference for violent behavior). Future work can reduce this limitation by making manual adjustments (and subsequent machine learning) to establish context and thereby attribute negative values for certain terms (such as "ISIS").

Next, Ms. Levey presented her research about how sentiment developed in the online trajectories of forum participants, emphasizing the impact of transitions from adolescence to adulthood on the emergence of violent narratives. Drawing on life course theory's emphasis on trajectories and turning points, her qualitative study examined the evolution of 96 participants (48 minors, and a control group of 48 adults, all with a link to Canada, at least 1 year on the forum, and a minimum of 100 posts) across three forums: Ummah, ShiaChat, and Islamic Awakening. On this sample, she first conducted a pre/post analysis, comparing the test group's sentiment scores for posts written prior to their transition to adulthood (aged 18 and below) with scores for their posts written as adults (19 and up). Pre/post scores for both the minors and the control group of adults were statistically significant, demonstrating an increase in negativity over time. Second, Ms. Levey examined sentiment consistency for each individual, graphing variation in sentiment scores, aggregated over six-month blocks. Third, to validate the statistical sentiment trend classifications uncovered in the previous step and to gain a better appreciation of the transition to adulthood, she conducted a manual analysis of the posts made by the sample of minors.

Ms. Levey identified three broad themes that emerged from her research. First, the most extreme, violent users from the minor sample were few in number, and not well received by other forum participants. These extreme users exhibited a consistently negative sentiment: they both entered and exited the forum already expressing a fairly negative and violent sentiment, failing to sway others during their presence. Second, of the users who exhibited inconsistent sentiment, the majority were benign; their narratives evolved, but in ways that reflected a "normal" (i.e. non-extreme) transition to adulthood. Narrative evolution was also observed in a handful of "pseudo-extreme" individuals, so-named because their increasingly negative sentiment scores reflected their adoption of more negative subjects of conversation, not necessarily of more negative behaviours or views (i.e. they discussed such "negative" topics as martyrdom or suicide bombing, but they did not necessarily espouse support for these violent behaviours). Finally, it appeared that all users were relying on their respective forums as an outlet to alleviate stress and seek support or motivation for every-day, benign, issues. Overall, Ms. Levey's findings demonstrated that the majority of minors appeared quite resistant to, and able to identify, users of an extreme nature. This conclusion would assuage concerns that extreme individuals are inspiring, motivating, or indoctrinating youth in online forums.

In the final segment on this topic, Mr. Thomas presented his macro-level research on the impact of opinion leadership and external events on forum participants following ISIS online—that is, how these "interventions" affect the sentiment of content discussed on the forums, and the corresponding level of user engagement (i.e. their social network connectivity, measured based on how user content is quoted or referenced, directly or indirectly). To answer these questions, data was drawn from four threads selected for their extremist content and popularity on IslamicAwakening.com, monitored between September 2013 and June 2014. This period encompassed a range of on-the-ground, external, events—the Anbar offensive; al-Qaeda's formal denouncement of ISIS; the May crucifixions; and the Kurdish clash with ISIS in Kobani—as well as two shifts in the threads' network composition: a major increase in new users, as well as the entrance of Twitter personalities.

Based on results from an interrupted time series regression, Mr. Thomas's central finding was that opinion leaders (in this case, the popular Twitter personalities) serve as a mediator between events external to online communities and the online reaction; external events do not, on their own, translate directly into changes in online behaviour. He observed that an external event produced the most dramatic change in forum content when accompanied by the presence of opinion leaders. In terms of group composition, these opinion leaders increased group cohesiveness: the presence of an opinion leader in the thread increased participation by the entire cohort, in a homogenous direction. This finding is of immense significance for designing and applying counter-narratives.

Taken together, the qualitative and quantitative components of this project underscore the importance of evaluating individuals' lifecycle transitions and corresponding variation in sentiment in the context of the broader online, social world in which they are embedded.

Deliverable 2.3.5

Futures of Terrorism: Technology Adoption and Fifth Wave Terrorism

Jez Littlewood (Carleton University)

In the workshop's final presentation, Dr. Jez Littlewood presented an overview of his findings from a project that analyzes how terrorism in Canada will evolve over the next five to ten years, with respect to 1) technology adoption by terrorist groups, and 2) possible trends in terrorists' ideological motivations. While he touched on both elements, the presentation emphasized findings with respect to the first category.

Dr. Littlewood described how Hollywood representations and media reports have inundated the public with the notion that terrorists are technologically sophisticated; a pervasive "technological determinism" frame has led most to believe that, because the technology is out there, terrorists will use it. However, the reality is that the vast majority of terrorism is overwhelmingly against local targets, using readily available, "low-tech" weaponry. Only half of terrorist incidents involve one or more casualty, and an incredibly small proportion results in mass (100+) casualties.

Dr. Littlewoods's project considers evolutions in three technological categories—the Internet, unmanned aerial vehicles (UAVs), and chemical, biological, radiological, and nuclear (CBRN) weapons—in relation to broader understandings of how groups innovate, learn, and apply knowledge, as well as developments in the broader technological arena. Ultimately, he argues, terrorists' technology adoption is simply a story of *people* adopting technology.

Nowhere is this ordinariness of terrorists' use of technology more evident than in the cyber realm. Cyber components—notably social media—are readily adopted by terrorists for the same reason that they are popular in the wider public domain: they are simple to use and easily exploitable. However, what is meant by "cyber terrorism" is highly ambiguous. Rather than observing the Internet used as a means of attacks (i.e. to actually result in harm to humans and/or property), we have continued to observe terrorists' use of the Internet in the same organizational functions identified by Gabriel Weimann in 2004: psychological warfare; publicity and propaganda; acquiring information and intelligence; fundraising; recruitment and mobilization; networking; sharing information; and planning and coordination. While some of these uses have advanced (e.g. movement to the Dark Web; changes in groups' command and control structures), their fundamental purposes have remained consistent. Terrorist groups' cyber capabilities have not evolved to such an advanced, persistent level that they would pose a real threat of attack to Canada. Such a level of threat would involve a significant investment of time and resources—and would require an immense improvement in terrorists' skills and capabilities—making it likely to remain unattractive and out of reach for most groups. In the future, groups will inevitably continue to exploit the Internet as a means of support for their activities, but we are unlikely to see it used as a means of attack in and of itself.

Similarly, while national security authorities have expressed concern over terrorists' use of UAVs for a number of years, we have not yet seen them take on any significant combat role: only one non-state group appears to have used UAVs in a combat function (Hezbollah's strike against Jabhat al-Nusra), but it is unclear whether the UAV itself served as a missile, or if it was fitted with a weapons system. Most reports of terrorist attempts to weaponize UAVs have been of questionable reliability, although there is some indication of real plots that would combine UAVs with weapons platforms. For the most part, terrorist use of UAVs has mirrored states' use of UAVs—only a small minority of which (contrary to popular belief) has been to employ a strike capability. Instead, UAVs have played a force-multiplying*, intelligence, surveillance, and reconnaissance (ISR)* function, supporting operations and attacks by non-aerial means. For terrorists, UAVs have also contributed a *prestige factor*: a certain demonstration of prowess which signals the group's technological sophistication for propagandistic ends. A more speculative possible terrorist use of UAVs would be for *disruption and deception* activities. From a deception or diversion standpoint, drones might be used to draw attention away from more important activities on the ground. For disruption, we could essentially see drones as harassment devices, either in isolation or in large numbers (i.e. swarming). While technology firms have been developing a drone swarming capability, and their attempts will inevitably shift from laboratory experiments to real world applications, this shift is unlikely to happen in the near future, and will involve an immense level of knowledge and skill beyond most terrorists' ability.

A final terrorist terrorist use of UAVs is *destruction,* future manifestations of which will likely involve miniaturized explosives. Given that we have already seen a range of such innovations in explosives (e.g. the shoe- and underwear-bombers, liquid bomb plots, explosives in headgear and laptops, etc.), it is inevitable that malicious actors will attempt to mount small, lightweight explosives to UAVs—although success in this arena will likely be dependent on advancements in the hobbyist community, where adaptations and improvisations are pursued for non-malicious ends. While we should anticipate some use of armed UAVs in the future—contingent on developments by hobbyists—we will see a more widespread use of UAVs by terrorists for ISR ends. Dr. Littlewood cautioned as well that state sponsorship has the ability to vastly augment terrorists' UAV capabilities.

For the final technological category, CBRN weaponry, the vast majority of terrorist groups currently pose no threat. While CBRN weapons have the ability to achieve mass destruction—if used correctly—and a small number of groups have clearly demonstrated an interest in CBRN technologies, their use thus far has been very basic, and with very low levels of success. Three outlying cases are: Aum Shinrikyo's 2015 sarin attack in the Tokyo subway; the 2001 anthrax letter campaign across the United States; and the Rajneeshees 1984 salmonella incidents in Oregon).

For assessments of CBRN's likely terrorist future, disaggregation is necessary. *Nuclear* terrorism is incredibly unlikely; it is too complex and too costly, and remains vastly beyond groups' scientific capabilities. If a nuclear state collapses, however, possible terrorist acquisition of its stockpiles would be a source of concern. *Radiological* terrorism is possible, but it would require a perpetrator who already has a strong grasp of the underlying science for effective deployment. To this end, radiological terrorism may attract an outlier perpetrator, or—more likely—an opportunist. While there have been many developments with respect to *biological* agents, advanced methods of delivery (e.g. aerosols) are beyond groups' capacity (although broader developments in science and technology may bring these methods more within reach). Such sophisticated techniques as genetic modification will continue to exceed—by far—non-state actor capabilities. *Chemical* agents are—and will remain—low-hanging fruit for terrorists. We are likely to see an increase in terrorists' use of toxic industrial chemicals, as well as chlorine. At least one group has recently used chlorine/mustard, and its demonstration effects will make successful use of these agents appear more attractive to others. In sum, CBRN use over the next five years is likely to be low-level, although lone actors may still be attracted to CB weapons (and toxins).

The above discussion predicts technology use through to 2020. Predicting to 2025 is far more difficult, particularly inasmuch as adaptations to new emerging technologies (e.g. 3D printing, artificial intelligence, On-Line learning, and simulations) as well as simple fixes may be developed to overcome current hurdles (e.g. fitting assault rifles to UAVs, designing swarming software and firmware, producing CB agents, or aerosol spraying devices). Adoption, proliferation, and use of sophisticated technologies will be far more likely in a world where such adaptations and simple fixes have been achieved, and where weapons available on illicit markets combine with new "plug-n-play" capabilities to allow for technological exploitation. The post-2020 emergence of a generation of technologically savvy individuals in their early 20s may accelerate these changes, as would an increased prevalence of disrupted spaces and safe havens.

On the topic of trends in terrorists' motivations, David Rapoport's "wave" theory suggests that we are nearing the end of the fourth, religious, wave. Although Dr. Littlewood considers that the religious wave is unlikely to wane over the next decade, religion's continued prevalence has not prevented him from thinking about what might come next. While Dr. Littlewood listed a range of possibilities for terrorism's "fifth wave," he highlighted two. First, an *anti-technology/neo-luddite* ideology could combine a range of broad (e.g. anti-surveillance;

anti-corporate) or specific (e.g. artificial intelligence; anti-genetic modification of humans or food) grievances. Second, we could observe a wave of *altruists* or vigilante groups, perpetrating political violence broadly in line with Western Liberal values. In this latter case, we may not be willing to label or acknowledge the violence as terrorism (as is arguably the case with current, anti-ISIS activities; the "good" foreign fighters). Ideology aside, the next wave of terrorism is likely to involve a resurgence of state sponsored activity—a so-called State Sponsored 2.0—particularly in the cyber domain.

Report written by Ms. Nicole Tishler (NPSIA, Carleton University)
at the request of TSAS.