National Defence Défense nationale

Canadian Forces College

Collège des Forces Canadiennes

THE WEAPONIZATION OF INFORMATION AND ITS USE THROUGH SOCIAL MEDIA

Major Stephen Wyatt

JCSP 45

Exercise *Solo Flight*

Disclaimer

Opinions expressed remain those of the author and do not represent Department of National Defence or Canadian Forces policy. This paper may not be used without written permission.

PCEMI 45

Exercice *Solo Flight*

Avertissement

Les opinons exprimées n'engagent que leurs auteurs et ne reflètent aucunement des politiques du Ministère de la Défense nationale ou des Forces canadiennes. Ce papier ne peut être reproduit sans autorisation écrite.

Canada

CANADIAN FORCES COLLEGE – COLLÈGE DES FORCES CANADIENNES

JCSP 45 – PCEMI 45
MAY 2019 – MAI 2019

EXERCISE *SOLO FLIGHT* – EXERCICE *SOLO FLIGHT*

THE WEAPONIZATION OF INFORMATION AND ITS USE THROUGH SOCIAL MEDIA

Major Stephen Wyatt

INTRODUCTION

Information has always played a key role for both militaries and governments alike as it relates to strategy and the processes followed in decision making. As a result, in years gone by what often occurred when militaries marched off to war, or governments were stalled in political negotiations, was he who was able to gain access to vital information quicker was often better suited to leveraging the information gleaned to their advantage. That early access to information often provided the opportunity to gain a marked advantage over your adversary which than facilitated the ability to make a decisive decision ahead of one's adversary and achieve the desired outcome. Today there can be no doubt that this still very much holds true only the difference now is the need to wade through massive volumes of readily available information to determine which pieces are relevant, although perhaps more germane, which pieces can be best employed (accurate or not) to best suit one's purpose. Never before has it been as easy as it is today to gather information related to essentially any topic and tailor it to suit one's purpose. Militaries, governments, interest groups, individuals, all have access to the resources required to extract information from all parts of the world, and it is now a greater struggle to protect information and prevent its distortion or inappropriate use. It should also be mentioned that this is a challenge faced globally, and that many countries are struggling with how to best protect, and defend, against informational attacks from across all domains. David Patrikarakos wrote in his book *War in 140 characters - how social media is reshaping conflict in the twenty-first century* - "I was caught up in two wars: one fought on the ground with tanks and artillery, and an information war fought largely through social media. And, perhaps counterintuitively, it mattered more who won the war of words and narratives than who had the most potent weaponry"[1]

[1]David Patrikarakos, *War in 140 Characters* (United States of America: Basic Books, 2017), 4.

This paper will look to explain how adversaries are employing information operations to influence populations, alter and shape narratives, incite and recruit supporters, as well as some of the methods which have been employed to fund and equip them. More specifically, it will be discussed how information is being weaponized and employed by our adversaries through social media. Social media has changed the way information is presented and delivered drastically over the course of the last 15 years or thereabouts. And while it provides unique and incredibly beneficial functions for modern day living, it also has a dark side which is easily exploited and used regularly for nefarious purpose. It is these ill intend purposes that we will examine throughout the paper.

THE THREAT

As discussed during the introduction social media plays a crucial role in today's modern battlefield. Information whether true or false is shared around the world at a rate of speed never before seen. Social media platforms such as Facebook, Twitter, and Instagram (to name a few) provide opportunities for both individuals and groups to broadcast information instantaneously to millions of viewers worldwide with little to no oversight or validation of the information being presented. What this could then facilitate is the spread of false information, whether by accident or intention, the consequences of which may not be fully realised at the moment of transmission. Alternatively, perhaps the consequences are fully realised and the spread of information was intentional in an attempt to shape a narrative, or alter facts, in order to distort the truth. This has the potential to pose a significant threat to Canada (and its allies) which we will now exam.

When we refer to the "weaponization" of information through social media what exactly are we referring to? TechTarget – an American company which offers data-driven marketing services- defines weaponized information as "a message or content piece that is

designed to affect the recipient's perception about something or someone in a way that is not warranted. The term implies a target and the intention to cause harm."[2] TechTarget then goes on further to say "the goal of weaponized information is bringing about a change in beliefs and attitudes and, as a result, promote behavior that serves the attacker's purpose. Attacks involving weaponized information are sometimes referred to as cognitive hacking."[3] While there are many open sources which speak to weaponized information and its definition, TechTarget's was selected intentionally as its reference to the identification of a "target" with the "intention to cause harm", and the "cognitive hacking" (cyberattacks which aim to manipulate peoples perception by targeting their psychological vulnerabilities) best defines the weaponized information which will be discussed throughout this paper. It is the harmful intent which our adversaries attempt to exploit as a means by which to bolster their cause, and shape narratives to suit their purpose.

Social media and its ability to disseminate information has "resulted in a qualitatively new landscape of influence operations, persuasion, and, more generally, mass manipulation. The ability to influence is now effectively [democratized] since any individual or group can communicate and influence large numbers of others online."[4] Information contained on social media sights is easily collected and sifted for content by both state and non-state actors. This is achieved either manually by less technologically savvy adversaries or through the use of algorithms and "bots" (software applications responsible for running automated tasks over the Internet) by more advanced opponents. Information is collected, collated to identify common themes (often loosely tied to truths or partial truths) and then used to send messages, shape or

[2]TechTarget, "Weaponized Information," last accessed 01 May 2019, https://whatis.techtarget.com/definition /weaponized-information

[3]*Ibid.*

[4]RAND Corporation, "The Weaponization of Information- the need for cognitive security," last accessed 01 May 2019, https://www.rand.org/content/dam/rand/pubs/testimonies/CT400/CT473/RAND_CT473.pdf

alter narratives of events which have occurred or are yet to occur, or in many instances generate fake news stories which though appear to be reputable are in fact a complete shame. "Users may be influenced by information provided to them by anonymous strangers, or even by the design of an interface. In general, the Internet and social media provide new ways of constructing realities for actors, audiences, and media."[5]

How it is done (Non-State Actors)

When considering the many methods information could be used to attack Canada and its allies we often consider the potential for kinetic attacks, or attacks that conventionally are more aligned historically with war-type actions. What about when the attack has nothing to do with weapons, soldiers, or the geography of a battlefield but rather is misinformation communicated through social media focused on destabilizing a country's economic stability?

Similar to bombing campaigns by allied forces during the Second World War focused on destroying German factories and industry, thereby damaging the German economy, could posting a message on Twitter which causes extreme economic fluctuations viewed in the same manner? Consider the events which took place 23 April 2013 when on-line hackers belonging to a group called "The Syrian Electronic Army", an organization known to support President Assad, hacked the Associated Press Twitter account at 1:07pm and sent a tweet saying "Two explosions in the White House and Barack Obama is injured". By 1:08 pm this tweet resulted in a significant drop to occur on the Dow Jones stock market which was not rectified for two minutes (1:10pm when the tweet was identified and confirmed as being false). In those less than three minutes the Dow dropped 150 points before beginning to rebound, resulting in a loss of

[5] *Ibid.*

approximately $136 billion dollars in equity market value.[6] While these actions were not directly attributable to President Assad or the Syrian military they were confirmed as having originated from a Syrian based group of non-state actors.

A second example to be discussed occurred as a result of an alleged insult spoken between a young Muslim boy and Hindu girl. In September 2013 in India's northern Uttar Pradesh state a young Hindu teenager returned home complaining of having been verbally harassed by a Muslim boy (also teenager) from a bordering village within the Muzaffarnagar district. Her brother and cousin wanting to seek justice for her visited the Muslim boy at his home and allegedly shot and killed him during the confrontation. The murder of the young Muslim boy obviously caused the situation to further deteriorate and the resulting actions which saw in the Muslim boy's family, and members from the surrounding Muslim community, attack and beat to death the brother and cousin. While it is very sad and unfortunate that three people would lose their lives over a verbal insult between two teenagers, the situation exploded into further violence when an individual from the Hindu community posted a video of two men being beaten and lynched online. While this video was actually three years old at the time (2010) and was not in fact the brother and cousin which triggered the event, the posting of this video served as the catalyst to insight further hatred and violence between the two communities. Armed protesters took to the street and began fighting, and massive demonstrations in surrounding Uttar villages sparked up; further assisted by warring politicians in both communities angling to garner support towards their campaigns as a result of a pending election. Schools and shops were closed, and hundreds of innocent people fled or had to be evacuated from their homes due to the growing violence on the streets. In the end 13 000 securing officers were dispatched to restore

[6]The Washington Post, "Syrian hackers claim AP hack that tipped stock market by $136 billion. Is it terrorism?," last accessed 30 April 2019, https://www.washingtonpost.com/news/worldviews/wp/2013/04/23/syrian-hackers-claim-ap-hack-that-tipped-stock-market-by-136-billion-is-it-terrorism/?utm_term=.5e1d6e7c0abe

order within the region, 31 people had been killed and over 100 individuals were charged with inciting violence. Police spokespeople also indicated that the attacks and violence witnessed in the street during this conflict were further fueled as a result of rumours spread via mobile phone and social media.[7]

Both incidents mentioned above speak to the cognitive hacking referenced in the TechTarget definition of weaponized information. In both cases the end results were directly related to the unprecedented speed and ability to widely distributed disinformation. A second key component to these cases was the disinformation author's correct assessment of the targeted audiences' cognitive vulnerability and the fact that in both instances they were able to play to the already existing fears and anxieties amongst the predisposed groups.[8] Attacks such as this are becoming common place on social media. A nation's ability to respond and/or protect itself from these forms of attack are tested and challenged on a daily basis as a result of the free flow of information across social media platforms. While these technologies have worked to improve life in many ways (causing many to wonder if we could ever go back to living in a world without these technological advancements) they are also very much responsible for a number of new and significant security threats we as individuals, as well as our nations, face today. Both of these examples serve as excellent tools to illustrate how effective a non-state actor can be at inciting violence, generating fear, and forcing governments to respond and expend significant time, money, and resources (and often lives) to counteract damages which have been done. In many instances these attacks are low-tech requiring very little technology, financial investment, or manpower, yet the outcome for individuals/families/special interest groups/nations can be

[7]Los Angeles Times, "An insult grows into violence in India; 31 dead," last accessed 30 April 2019, https://www.latimes.com/world/la-xpm-2013-sep-09-la-fg-wn-india-violence-death-toll-31-20130909-story.html

[8]RAND Corporation, "The Weaponization of Information- the need for cognitive security," last accessed 01 May 2019, https://www.rand.org/content/dam/rand/pubs/testimonies/CT400/CT473/RAND_CT473.pdf

disastrous, even deadly. “Interaction within the information environment is rapidly evolving, and old models are becoming irrelevant faster than we can develop new ones. The result is uncertainty that leaves us exposed to dangerous influences without proper defenses.”[9]

RUSSIA

No discussion on (mis) information operations or the weaponization of them, and social media, would be complete without addressing Russia and its tireless efforts to upheave global political discourse and sow seeds of mistrust within the international community. While these tactics were widely employed throughout the cold-war era and therefor in some respects are not new, the methods and audiences Russia is now able to reach, and influence, has grown exponentially as a result of social media and the opportunities it presents. While there are many adversary nations which employ social media to attack Western allied countries, no country is more overt and deliberate in their use of social media hacking than Russia. “The Russians see information operations (IO) as a critical part of non-military measures. They have adapted from well-established Soviet techniques of subversion and destabilization for the age of the Internet and social media.”[10] While the list of options and resources available to Russia is significant and as just mentioned spans decades of tradecraft and skill refinement we will look to exam a couple of methods Russia has most recently employed to further their nation’s influence through information operations using social media.

One of the first key aspects which should be addressed is Russia’s stance on cyber and informational warfare. The original technique employed by the Soviets was through aktivnyye meropriyatiya (active measures) and dezinformatsiya (disinformation) terms which today are

[9] *Ibid.*
[10] *Ibid.*

more commonly understood than perhaps they were during the cold-war. The U.S. State department defines active measures in that they are "distinct both from espionage and counterintelligence and from traditional diplomatic and informational activities. The goal of active measures is to influence opinions and/or actions of individuals, governments, and/ or publics."[11] In February 2017 Russian Defence Minister, Sergey Shoigu, announced the creation (or rebrand) of what in 2015 was termed the Internet Research Agency into an Information Warfare branch of the Russian military. While details surrounding the number of personnel and exact mandate of this branch are kept closely guarded, Minster Shoigu is quoted as saying "the information operations forces have been established which are expected to be a far more effective tool than all we used before for counter-propaganda purposes. Propaganda should be smart, competent and effective."[12]

Russia also takes a very different viewpoint on information operations than do the West. General of the Army, Valery Gerasimov, Chief of the General Staff of the Russian Federation Armed Forces has indicated that war is now fought observing a 4:1 ratio of non-military and military measures. Russia views the non-military measures of warfare as including economic sanctions, both political and diplomatic pressure, as well as the disruption of diplomatic ties.[13] General Gerasimov further indicates that "the very [rules of war] have changed. The role of non-military means of achieving political and strategic goals has grown, and, in many cases, they have exceeded the power of force of weapons in their effectiveness."[14] It is also important to

---

[11]United States Department of State report, *Soviet Influence Activities: A Report on Active Measures and Propaganda*, (Washington, DC: Bureau of Public Affairs, 1987), viii.

[12]UPI, "Russia has a cyber army, defense minister acknowledges," last accessed 01 May 2019, https://www.upi.com/Top_News/World-News/2017/02/23/Russia-has-a-cyber-army-defense-minister-acknowledges/2421487871815/

[13]U.S. Army, "The Value of Science Is in the Foresight New Challenges Demand Rethinking the Forms and Methods of Carrying out Combat Operations," last accessed 01 May 2019, https://usacac.army.mil/CAC2/MilitaryReview/Archives/English/MilitaryReview_20160228_art008.pdf

[14]*Ibid.*

understand that Russia takes a much different stance on their employment of information operations in that they are not viewed (as we do in the West) as targeted, precision strikes when required, moreover, Russian information operations are viewed to be persistent and enduring, a state of continues activity "regardless of the state of relations with any government, while the Westerners see IO as limited, tactical activity only appropriate during hostilities. In other words, Russia considers itself in a perpetual state of information warfare, while the West does not."[15] This presents a very different mindset than that of Western nations and is one of the reasons Russia has been as successful as it has with many of their campaigns. In order to understand how Russia has been successful we must closer examine their processes.

Firstly, Russia has significantly resourced their information operations agencies such as the Information Warfare branch of the military. Supporting this branch are their vast intelligence networks and state-owned media outlets funded by the Kremlin such as Russia Today (RT) and Sputnik. "RT was originally launched with a Russian government budget of $30 million per year in 2005. By 2015, the budget had jumped to approximately $400 million, an investment more in line with the Russian view of the outlet as a [weapons system] of influence."[16] Before Russian trolls begin their information operations they will first conduct cyber warfare to hack and gather intelligence on whichever target they have selected. This information will then be passed to an organization such as Wikileaks who acts as a cut-out (a mutually trusted intermediary, method or channel of communication that facilitates the exchange of information between agents) which according to CIA former director Mike Pompeo "is a non-state hostile intelligence service

[15]RAND Corporation, "The Weaponization of Information- the need for cognitive security," last accessed 01 May 2019, https://www.rand.org/content/dam/rand/pubs/testimonies/CT400/CT473/RAND_CT473.pdf

[16]P.W. Singer and Emerson T. Brooking, LikeWar (New York: Houghton Mifflin Harcourt Publishing Company, 2018),107.

abetted by state actors like Russia."[17]Once the information has been pushed through Wikileaks the Russian trolls than distribute the information across multiple social media platforms (Facebook/Twitter/Instagram) and reference the leaked information found on Wikileaks and RT. This message is then further communicated as a result of individuals who become influenced by the information presented to them (re: cognitive hacking). Russian trolls and bots then continue to retweet the messages of influenced individuals amplifying the misinformation momentum that has now gained traction on social media.[18]

How it is done (Russia)

A good example of these capabilities occurred in November 2015 after a trend gained momentum over Twitter as a result of protests occurring at the University of Missouri related to racial issues being experienced on campus. #PrayforMizzou began trending after a tweet was sent out claiming KKK members were conducting marches across Columbia and the Missouri (Mizzou) campus. One particular post from "Jermaine" (@Fanfan1911) stated that the police were marching in support of the KKK and that they had just beaten up his little brother. Images of a young black man who appeared to have been beaten were attached to the tweet. This information was picked up by other Twitter followers and the number of retweets moved into the hundreds. Jermaine and a number of other followers continued to tweet and retweet stores of KKK activities in Columbia which significantly increased the real time interest in this story as rumours spread like wildfire across social media. When this incident was later dissected it was discovered that the original tweet, and subsequent retweets, all originated from the same accounts which, upon further dissection, revealed themselves to be approximately 70 bots

[17]Strategic Studies Quarterly, "Commanding the Trend: Social Media as Information Warfare," last accessed 02 May 2019, https://www.jstor.org/stable/e26271629
[18]*Ibid.*

working in conjunction, spacing their retweets evenly and interspersed amongst tweets from actual followers. The bot tweets along with the tweets of actual followers resulted in thousands of retweets within minutes of the original post. The plot was deliberate and well planned so as to avoid the algorithms employed by Twitter aimed at identifying and catching bots. As intended, the result of this misinformation operation spurred outrage across the country and around the world. Russia's intent to spread fear and distrust within communities throughout the United States had worked. The narrative had been pre-established which allowed the trend to take root and support the establishment of the hoax. This incident resulted in an investigation into the events which transpired at the University of Missouri. It was discovered the original poster "Jermaine" whose online photo identified him as being a young black man had shortly after the event changed his online address from @Fanfan 1911 to @FanFan and his online photo changed to that of a German iron cross. Jermaine's younger brother who had been "beaten by the police", as it turned out a quick Google search of "bruised black buy" brought up the same image which had been attached to the original tweet. @FanFan's new tweets (now in German) also changed drastically and the messages posted were all anti-Islamic, anti–European Union, and anti-German Chancellor Angela Merkel. This persisted for a number of months, largely remaining focused on anti-immigration policies with Russian propaganda messages mainly dominating the narrative. In the spring of 2016 @FanFan's profile changed yet again, this time the tweets were published in English with the narrative being almost solely focused on anti-Obama and Clinton sentiment. Russia's anti-immigration narrative began to gain traction (another example of cognitive hacking) across Europe and was so effective that one Polish magazine devoted an entire issue to Muslim immigration in Europe titling their publication "Islamic Rape of Europe" (Polish newsweekly wSieci or "The Network).[19]

[19] *Ibid.*

This is just one of what at this point amounts to a multitude of identified Russia information operations which have taken place across the globe. “War Goes Viral” an article published in The Atlantic states that Putin’s intent “is not to make you love Putin; instead the aim is to make you disbelieve anything. A disbelieving, fragile, unconscious audience is much easier to manipulate. Active measures enable manipulation all focused on contributing to a breakdown of public trust in institutions.”[20]Just as Defence Minister Shoigu stated during his press conference announcing the creation of the Information Warfare branch, Russia’s stance on propaganda obviously still clings to the tenets of it needing to be smart, competent, and effective, and that nationally they work tirelessly to ensure that the outcome of their active measures influence opinions and/or actions of individuals, governments, and/ or publics. This coupled with the fact that Russia views itself as constantly being in a state of informational warfare is what makes them so effective, and dangerous, internationally within this domain.

EXTREMIST GROUPS

On the other end of the spectrum when considering information operations and how they are increasingly becoming weaponized across social media platforms it is imperative that we discuss extremist organization such as ISIS, Al Nusra Front , Hezbollah, al-Qaeda and other such groups which have able to use social media to great effect in furthering their agendas internationally. Social media platforms provide the vehicle for extremist groups to spread their messages of hate, incite violence, call to arms, recruit foot soldiers, fund and equip fighters, etc. across the globe like never before. When you consider that in 2016 there were 3.4 billion internet users, over 500 million tweets were sent each day, 7 hours of YouTube video was uploaded each second in 76 different languages, and that there were over 1.7 billion active Facebook accounts it

[20]The Atlantic, “War Goes Viral- How social media is being weaponized across the world,” last accessed 02 May 2019, https://www.theatlantic.com/magazine/archive/2016/11/war-goes-viral/501125/

is no wonder that extremist groups are looking to take advantage of these opportunities which are readily available to all.[21]

One group which has benefitted greatly from social media is ISIS. Since its inception ISIS has been able to recruit over 30 000 fighters across 100 different countries in support of its self-declared caliphate. They have been responsible for lone-wolf attacks in Canada and the United States, suicide bombings throughout Turkey, Yemen and the middle east, terror attacks in Belgium, France and across Europe, all of which continue on today despite the tremendous losses sustained by the group as a result of the fighting in Iraq and Syria. One of the ways ISIS has been so successful in filling its ranks is through its use of "crowdfunding" via Facebook, Instagram, YouTube and PayPal. "By the time of the Syrian civil war and the rise of ISIS, the internet was the [preferred arena for fundraising] for terrorism, for the same reasons it has proven so effective for start-up companies, non-profits, and political campaigns."[22]ISIS has identified how (through PayPal) for $800 you can "equip a mujahid" with an RPG that he will require for battle in the same way you would sponsor or donate to a friend participating in an online charity run for cancer. Social media has expanded the networks available and extended the lines of communications to be able to reach out to potential fundraisers regardless of their location within the world. ISIS gained popularity through their posting of online videos, Instagram accounts where you could chat live with fighters as they conducted attacks throughout Syria and northern Iraq, and through their Facebook "vote" options where they solicited input on when and how to kill captured combatants as well as incent civilians. Some religious clerics went so far as to

[21]*Ibid.*

[22]P.W. Singer and Emerson T. Brooking, LikeWar (New York: Houghton Mifflin Harcourt Publishing Company, 2018),65.

message that believers could do their part in supporting the caliphate by pledging money online thereby fulfilling their religious obligations without having to actually engage in combat.[23]

How it is done (Extremists)

One of the best examples of when an extremist group has achieved success (almost infamy dependent on your perspective) was in 2014 during ISIS' military advance from Syria into northern Iraq. #AllEyesOnISIS is arguably an almost textbook example of how to mount an aggressive psychological operations campaign leveraging social media platforms to maximize the effect of information distribution. When ISIS made its move to leave Syria and begin their attack into Iraq they chose to do so taking to social media and laying out their battle plans as well as live streaming their advance. This allowed them to gather international support from global jihadi fans while having the added benefit of seeding terror in the soldiers of Iraq who were also able to watch ISIS' bloody and grotesque advance towards their positions. "Far from keeping their operations a secret, though, these fighters made sure everyone knew about it. There was a choreographed social media campaign to promote it, organised by die-hard fans and amplified by an army of Twitter bots"[24]The success of this hashtag, along with the smartphone app created, brought about an even greater success then likely ISIS leadership had originally envisioned. On Arabic Twitter it rapidly became the top trending hashtag being watched by fans, fighters, adversary militaries (Iraq) as well as civilians within the battlespace of ISIS' advance. ISIS was brutal in the attacks they launched, and the methods they employed in "dealing with" those that attempted to resist. Videos of beheadings, torture, and executions were uploaded daily as they conducted their vicious advance towards Mosul. Instagram and WhatsApp were the two primary sources employed by ISIS for gathering information on Iraqi soldier locations which was

[23]*Ibid*.65
[24]*Ibid*.4

provided by Sunni supporters within Iraq. As the 1500 ISIS fighters neared Mosul, mounted in Toyota pickup trucks, and carry only their second-hand personal weapons, the 26 000 Iraqi soldiers as well as police began to abandon their positions and leave the city. Often leaving their weapons, vehicles and equipment in place for ISIS fighters to collect after they had gained entry and eventually control of the city. "Only a handful of brave (or confused) soldiers and police remained behind. They were easily overwhelmed. It wasn't a battle but a massacre, dutifully filmed and edited for the next cycle of easy online distribution."[25]So effective were the psychological operation mounted by ISIS in advance of their arrival to Mosul that the end result saw ISIS take control of the city with little to no resistance. Despite the Iraqi forces having more than 17 times the number of fighters than ISIS, in addition to the arsenal of American made Abram tanks, Black Hawk attack helicopters and 2300 Humvees (all of which were left in place for ISIS to capture) ISIS was able to declare a decisive victory in Mosul. ISIS was able to demonstrate it for the world to watch from the comfort of their homes, after barely having to lift a finger.[26]

The unfortunate reality of social media is that it does provide the opportunity for individuals and groups who wish to exploit its benefits for their perverse use to do so. It has demonstrated itself to be an incredibly effective tool for garnering international support from extremist fans, as a tool to help facilitate the funding, recruitment and equipping of extremist fighters, while also providing the venue to launch incredibly effect psychological terror campaigns. In 2016 alone, Twitter suspended 360 000 accounts which had been identified as being used to promote terrorism and violence. "Twitter [has become] a digital social media battlefield of some sort which is also a way of recruiting people. As we can see the extremist

[25]*Ibid*.6

[26]The Atlantic, "War Goes Viral- How social media is being weaponized across the world," last accessed 02 May 2019, https://www.theatlantic.com/magazine/archive/2016/11/war-goes-viral/501125/

groups are losing on the territorial front, so they're going to social media again and again to recruit the youth."[27] Within Canadian doctrine (The Future Security Environment) we have identified that we (Canada) and our allies are likely to continue to be engaged in dealing with the security threats these sorts of groups present in both domestic and expeditionary operations out to 2040. With this in mind there can be no doubt that the resources available to extremist groups through mass production and widely available technologies will undoubtedly become an even greater threat to us as these technologies and platforms continue to evolve and become further and further enhanced.

CONCLUSION

Information, and the degree to which it is available, is being collected, processed and made available at an explosive rate never before seen. This trend is likely to only increase as technology and the inter-connectedness of the global community continues to evolve and expand. No longer is the competitive advantage awarded to whomever gains access to information soonest, but rather who is best able to capitalize on the distribution of information across social media platforms. Unfortunately, the reality faced today is that the distribution of information does not even need to be factual, rather it just needs to appear as though it is.

As mentioned earlier this is a challenge being faced by individuals and governments around the world, many of which do not hold themselves to the same ethical standards as do those from the West. This presents a significant challenge when trying to determine how best to defend against weaponized information intentionally being distributed throughout every facet of our daily lives. How best to defend against this issue would likely serve as an excellent topic to

[27]The Guardian, "Twitter suspends 235 000 accounts in six months for promoting terrorism," last accessed 02 May 2019, https://www.theguardian.com/technology/2016/aug/18/twitter-suspends-accounts-terrorism-links-isis

investigate in a subsequent research project. Holistically it remains imperative that information presented is rigorously scrutinized to determine its validity and that it not be assumed to be accurate at face value. Additionally, it is important to determine what we are comfortable with accepting as being the new contested threshold (as it relates to deliberate interference with regards to weaponized information) as the ability to conduct forensic analysis of all information being presented would be neither timely, nor feasible. Deliberate tampering in the affairs of nation states is now common practise whether that be through adversary states, non-state actors, or extremist groups and/or individuals. Understanding that this is the new reality and therefore determining how to deal with this eventuality will serve as best practice in our endeavour to prevent becoming victims to false information.

BIBLIOGRAPHY

Patrikarakos, David. War in 140 Characters. United States of America: Basic Books, 2017.

Singer, P.W, and Emerson T. Brooking. *LikeWar*. New York: Houghton Mifflin Harcourt Publishing Company, 2018.

RAND Corporation. "The Weaponization of Information- the need for cognitive security." Last accessed 01 May 2019. https://www.rand.org/content/dam/rand/pubs/testimonies/CT400/CT473/RAND_CT473.pdf

Canada. Department of National Defence. A-FD-005-001/AF-003, *The Future Security Environment*. Ottawa: DND Canada, 2014.

United States. United States Department of State. *Soviet Influence Activities: A Report on Active Measures and Propaganda*. Washington, DC: Bureau of Public Affairs, 1987.

Danish Defence. Royal Danish Defence College. *#TheWeaponizationOfSocialMedia – Characteristics_of_Contemporary_Conflicts*. Copenhagen, Denmark: Royal Danish Defence College, 2015.

The Washington Post. "Syrian hackers claim AP hack that tipped stock market by $136 billion. Is it terrorism?" Last accessed 30 April 2019. https://www.washingtonpost.com/news/worldviews/wp/2013/04/23/syrian-hackers-claim-ap-hack-that-tipped-stock-market-by-136-billion-is-it-terrorism/?utm_term=.5e1d6e7c0abe

Los Angeles Times. "An insult grows into violence in India; 31 dead." Last accessed 30 April 2019. https://www.latimes.com/world/la-xpm-2013-sep-09-la-fg-wn-india-violence-death-toll-31-20130909-story.html

UPI. "Russia has a cyber army, defense minister acknowledges." Last accessed 01 May 2019. https://www.upi.com/Top_News/World-News/2017/02/23/Russia-has-a-cyber-army-defense-minister-acknowledges/2421487871815/

U.S. Army. "The Value of Science Is in the Foresight New Challenges Demand Rethinking the Forms and Methods of Carrying out Combat Operations." Last accessed 01 May 2019. https://usacac.army.mil/CAC2/MilitaryReview/Archives/English/MilitaryReview_20160228_art008.pdf

Strategic Studies Quarterly. "Commanding the Trend: Social Media as Information Warfare." Last accessed 02 May 2019. https://www.jstor.org/stable/e26271629

The Atlantic. "War Goes Viral- How social media is being weaponized across the world." Last accessed 02 May 2019. https://www.theatlantic.com/magazine/archive/2016/11/war-goes-viral/501125

The Guardian. "Twitter suspends 235 000 accounts in six months for promoting terrorism." Last accessed 02 May 2019. https://www.theguardian.com/technology/2016/aug/18/twitter-suspends-accounts-terrorism-links-isis

The Guardian. “Polish magazine’s [Islamic rape of Europe] cover sparks outrage.” Last accessed 02 May 2019. https://www.theguardian.com/world/2016/feb/18/polish-magazines-islamic-of-europe-cover-sparks-outrage

Defense One. “Winning [LikeWar]: A conversation about social media and conflict with Peter Singer.” Last accessed 02 May 2019. https://www.defenseone.com/ideas/2018/10/winning-war-social-media-and-conflict-conversation-peter-singer/151806/