Evolution of Warfare: Research Essay

Name: Vineet Posani

This essay will show how social media acts as a means for contemporary hybrid warfare. It ties into the discussion of a few different themes like the exchange of news and information, propaganda and social networking. This essay will reference two case studies to demonstrate the ways in which state & non-state actors utilize social media to engage time-tested propaganda methods to produce outcomes. Propaganda messages are distributed by engaging with a an already present ideology which is then boosted through a system of automated bot accounts to coerce that specific social media program algorithm to identify that message like something which everyone accepts and becomes popular for a certain period of time. Case study number one will focus on Russia the state actor and case study number two will focus on Islamic State (IS) the non-state actor where substantial evidence will be provided of how they have influenced social media for their own purposes. Force and influence shall proceed to be fundamental components in hybrid warfare for nations as they try and utilize social media more and more.[1] This essay will also address a couple of key questions: What part does social media play in hybrid warfare?, What is the weaponization of social media?, What are the strategic procedures in which state & non-state actors us to aid their political and military objectives while utilizing social media?, What are the

[1] Jarred Prier. "Commanding the Trend: Social Media as Information Warfare, Strategic Studies Quarterly, Air University Press. 2017. https://www.jstor.org/stable/10.2307/26271634.

possible impacts of it?, How can NATO with its allies help recognize and go against the evil operation of social media?[2]

Using social media as a tool for communication is extremely significant in today's world because it encourages and opens up more dialogue, contributes to the sharing of information and ideas, offers job opportunities through platforms like LinkedIn for example, allows people to share their daily experiences through platforms like Facebook & Instagram, allows people to post tweets on how they feel about certain things on Twitter and more. And while social media offers all these things, it also has a dark side to it as well. Because social media platforms are so open and engaging it reveals the weaknesses of everyone who use these platforms as well. Therefore, the cyber community has an unfettered atmosphere where anonymity offers more prospects to propagate extremist perspectives, cause deception, and produce misrepresentations by not showing who ever is responsible for the creation of that particular content. David Stupples states that, the strength of today's world is the fact that everyone is wired and connected and can interact with one another very quickly, but it also means that the spread of propaganda and trepidation could happen quickly which eventually causes panic.[3] So this means that anyone using social media platforms has the ability to influence the public's opinions on certain things to get the outcome that they want. It's added benefits are that it's free of cost and takes no time at all to gain a following as well. This has

[2] "Social Media As A Tool Of Hybrid Warfare". NATO StratCom COE: Riga. May 2016.

[3] David Stupples. "The Next Big War Will Be Digital and We Are Not Ready For It". The Conversation. November 26, 2015. https://theconversation.com/the-next-war-will-be-aninformation-war-and-were-not-ready-for-it-51218.

contributed to the utilization of social media in warfighting by countries & extremists factions. This is only increasing in contemporary times.[4]

Coming to hybrid warfare, it's safe to say that it doesn't have a unified meaning. It can however be described as type of warfare that is made up of many approaches like military and non-military, evident and secretive strategies, conventional & unconventional utilizing cyber & information warfare which targets at generating bewilderment and obscurity on what it entails, where it came from and what the purpose of these actions are.[5] Anyone can get involved in meaningful discussion revolving around non-military approaches involving information operatives, by stating that it's consistently been utilized at wartimes. "However, what makes modern warfare so different is the effects the information can cause to the development of the conflict, as audience perception of the outcome of the conflict matters more than the actual facts on the ground."[6] Combining the fact that there is hardly any limit on global boundaries geographically with the technological advancements like social media that have been put in place makes the public's inclusion in worldwide conflicts is increasingly fundamental. All audiences are able to currently engage with real time happenings while following internet news resources and communicate by means of social media. By this means, the struggle of having power and control over people's viewpoints and attitudes turned into a fundamental part of contemporary conflicts. As David Stupples predicts, "information warfare

[4] "Social Media As A Tool Of Hybrid Warfare". NATO StratCom COE: Riga. May 2016.

[5] Jan Joel Andersson. "Hybrid operations: lessons from the past". EUISS. October 2015. http://www.iss.europa.eu/ uploads/media/Brief_33_Hybrid_operations.pdf.

[6] "Social Media As A Tool Of Hybrid Warfare". NATO StratCom COE: Riga. May 2016.

that integrates electronic warfare, cyberwarfare, and psychological operations (PSYOPS) into a single fighting organisation will be central to all warfare in the future."[7] The Russian-Ukrainian conflict showed everyone that cyber-attacks has the ability to not solely mess up technical systems and procedures, but get inside people's heads and have an impact on their mindset regarding various issues. Small, primitive attacks which are aided by information procedures may also produce important communal & media awareness and as well emphasize the enemy's flaws and uncertainties. For instance, b0ltai.org which is a hacker group, made the public know about the Internet Research Agency's hacked e-mail communication in St. Petersburg in order to establish that this agency is actually a "troll farm" having Kremlin links. Another instance is a phone conversation between the US & EU government officials discussing Ukraine which got exposed and then went on social media. This can be viewed in two ways: 1) Trying to show that the security systems that are responsible for protecting Western administrative transmission lines are not good enough. 2) Humiliate Western officials and cause a rift amongst them while impacting people's perceptions through social media and misleading them.[8]

History has shown that there has been numerous instances where social media has been utilized to build and form society's perception on various issues, gain a following, organize army events and gather data for aiming reasons. Here's to a name a few: The Israel-Hezbollah conflict, the Middle East conflict, Syria & Ukraine, the 1999 Kosovo internet wars, the "Arab Spring" in Northern

---

[7] David Stupples. "The Next Big War Will Be Digital and We Are Not Ready For It". The Conversation. November 26, 2015. https://theconversation.com/the-next-war-will-be-aninformation-war-and-were-not-ready-for-it-51218.

[8] "Social Media As A Tool Of Hybrid Warfare". NATO StratCom COE: Riga. May 2016.

Africa, etc. This has turned into the 'weapon of choice' for state & non-state actors. Thomas Elkier suggests 6 ways where social media is able to be utilized in order to help aid army procedures: 1) Targeting, 2) Intelligence Collection, 3) Cyber Operations, 4) Command & Control, 5) Defence and 6) Inform & Influence (Psychological Warfare). Everything listed here is able to be performed through social media irrespective of whether all of these have online or offline impacts. These actions are equally helpful and may frequently be performed in coordination with ground-based physical actions.[9]

Targeting – This activity utilizes social media to recognize possible targets to conduct army activities within the physical realm (focusing on geo-tagged photos or continuing talks online) and also to damage profiles on social media by means of hack or sabotage. For instance, in Libya, people used Google Maps and cell phones in order to chart government positions which had been given to NATO and subsequently utilized that information to recognize targets and capture them through air power.[10]

Intelligence Collection - This activity concentrates on the finding and the examining of information from social media platforms and its accounts. This involves subject matter and discussions. This can be done either openly or secretly. Numerous approaches can be taken to examine social media for intelligence collection purposes (like for example, craze, system, outlook, data examination, geo-, social, general, subject matter). These types of examinations may help target audience analysis (TAA) and help psychological warfare along with the choosing of targets for online and

[9] Nissen, Thomas Elkjer. "The Weaponization of Social Media". Royal Danish Defence College. Copenhagen. 2015.

[10] "Social Media As A Tool Of Hybrid Warfare". NATO StratCom COE: Riga. May 2016.

offline procedures. Overall, it's not impossible to obtain substantial data about systems, people and associated communications by using social media, therefore supporting anyone to learn more about the data atmosphere and circumstances surrounding a specific target group despite not being directly available. By researching thoroughly, social media may be a vital tool for circumstantial attention and as well to recognize any warning signs for a potential calamity in the time to come.[11] Particular challenges and constraints are present in the context of social media research. Moral considerations must be taken into account such as privacy breaches, data stream noise which is tough to distinguish from important data by utilizing computerized instruments and also the challenge of assessing the impacts of cyber conversations on happenings in the real world. For instance, the part which Twitter had to play for the Arab Spring uprisings is frequently exaggerated. Twitter acted as a turning point, although the potential of Twitter's impacts cannot be underestimated and must be approached with prudence. Twitter supported message distribution along with organizing activities, but these uprisings won't have occurred without the real circumstances on the ground. Media workers and advocates like civic journalists have been gradually utilizing "crowdsourcing" as a tool for fact-checking, exposing propaganda and recognizing changes within conflicts. Crowdsourcing is very beneficial in information warfare where it can expose truths by giving out the crowdsourced material to the public and doesn't have to be solely for intelligence gathering and examination. For instance, a collaborative venture which consisted of the Atlantic Council and Bellingcat could trace and give proof that Russian soldiers were present on Ukrainian soil by just gathering data from social media accounts of the Russian

[11] Nissen, Thomas Elkjer. "The Weaponization of Social Media". Royal Danish Defence College. Copenhagen. 2015.

soldiers, Google maps, media pictures and also crowdsourced data from observers.[12] Utilizing open-source inquiry, involving social media, this method facilitates the thwarting of propaganda and provide helpful aid for tactical communications requirements.

Cyber Operations – This can entail hacking social media profiles, changing profile information, or cause a social media platform to not be used anymore. These activities may be considered disrespectful or protective, depending on the situation, although the majority of social media cyber operations are naturally disrespectful. These could involve activities such as "Distributed Denial of Service (DDoS) website strikes, cracking passwords in order to obtain access and reveal e-mail, chat room and phone information, changing data on social media profiles or the incursion of files for the gathering of data. Activities like this try and restrict other people from engaging in dialogue, organizing events, have data access, or dispense messages for at least the short-term.[13] For instance, back at the start of January 2015, "CyberCaliphate" who was a hacker stated that he had links to Daesh and utilized Albuquerque Journal's Twitter page to publish contact numbers, detainment files, addresses, along with other private data that had been taken from a variety of

[12] Maksymilan Czuperski, John Herbst Eliot Higgins, Alina Polyakova & Damon Wilson. "Hiding in Plain Sight: Putin's War in Ukraine, Atlantic Council". October 2015, http://www.atlanticcouncil.org/publications/reports/ hiding-in-plain-sight-putin-s-war-in-ukraine-and-boris-nemtsovs-putin-war.

[13] Nissen, Thomas Elkjer. "The Weaponization of Social Media". Royal Danish Defence College. Copenhagen. 2015.

databases.[14] Later that month, CyberCaliphate attacked the U.S. Central Command's (CENTCOM) Twitter account and delivered intimidating messages to the American soldiers. A few files had shown up as swell on CENTCOM's common Twitter feed. A Twitter message read: "American soldiers, we are coming, watch your back."[15] This attack may not have exposed any confidential files, but it still caused mental damage and acted as a cautionary signal showing that extremists won't be reluctant to utilize bad security systems and social media to spread their propaganda. Cyber operations which occur by means of social media may lead to real life consequences. An example can be the Syrian Electronic Army's hacker group who attacked Associated Press's Twitter account posting a fake tweet stating the White House was bombed and that the president was harmed from it. This single tweet alone led to a massive billion-dollar dip in S&P 500 index within 180 seconds.[16]

Command & Control – Utilizing social media for inner communications, data exchange, organization and action management. Utilizing social media in this aspect is significant for non-state actors like rebellious groups, specifically if they don't have a proper structure in place or are

---

[14] Armin Rosen. "A Self-Proclaimed ISIS Fan is Hacking Local News Outlets". 6 January 2015. http://www.businessinsider.com/ a-self-proclaimed-isis-fan-is-hacking-local-news-outlets-2015-1.

[15] "US Centcom Twitter account hacked by pro-IS group". 12 January 2015. http://www.bbc.com/news/world-uscanada-30785232.

[16] Peter Foster. ''Bogus' AP tweet about explosion at the White House wipes billions off US markets". 23 April 2013. http://www.telegraph.co.uk/finance/markets/10013768/BogusAP-tweet-about-explosion-at-the-White-House-wipes-billionsoff-US-markets.html.

disseminated over vast regions; social media may act as a medium of communication along with a way to organize their events. The utilization of social media however, by rebellious groups to organize their events, somehow reaches the intelligence community in the end.[17] This type of free composition is actually tough for conformist equipped forces to attack non-state actors' command & control systems. This is due to the fact that no central systems, intersections or physical targets are present in order to attack. This will lead to legal implications as well because these platforms are not part of the army. It's also possible to utilize social media as part of "swarming" tactics which is the dispensing of data in order to assemble and organize non-state actors with a general importance to connect to their particular targets. Social media helps actors to come together swiftly for campaigning which leads to security entities barely any time or no time to do something about it. This method had been utilized while the Arab Spring uprisings were happening. Iran had utilized this method like a counter-measure; a campaigning rally had been conducted from social media, but police forces came up against them once people had gotten together.[18] Because of certain policing problems, Daesh operates the majority of its command & control events through "closed" chat applications and gaming systems, but a fresh examination done by NATO StratCom COE recognized certain organization and assembly is being done on open platforms like Twitter too. The examination states that Daesh is including geo-locations for their own hashtags like "State of Homs" or State of Raqqa". This enables people to "disseminate target information to specific regions of the world and for any independent actor to share information within their region using

[17] Nissen, Thomas Elkjer. "The Weaponization of Social Media". Royal Danish Defence College. Copenhagen. 2015.

[18] "Social Media As A Tool Of Hybrid Warfare". NATO StratCom COE: Riga. May 2016.

a combination of Islamic State hashtags as well as geographic keyword tagging."[19] "State of Twitter" which is a hashtag is also commonly utilized in order to disclose certain procedures that are being done from Twitter and its strategic requirements and actions.[20]

Defense – Safeguarding social media websites and accounts on the system or technical stage. Activities as part of defense here may involve encryption, anti-tracking and/or IP-concealing software when linking it to social media. Not showing operational security gratitude and not having proper awareness of simple cyber-security led to the loss of numerous rebels' lives mainly in Syria.[21] Because of these circumstances, it's not shocking to know that extremist groups are utilizing encrypted messaging programmes in order to communicate with their supporters and cause more rebellion. For instance, PlayStation is actually considered to be a very contesting gaming platform for the regulation administration to trace.[22] Adding to that point, Daesh gave a

[19] Joseph Shaheen. "Network of Terror: How DAESH Uses Adaptive Social Networks to Spread its Message". 2015, p. 9-10, http://stratcomcoe.org/network-terror-how-daesh-usesadaptive-social-networks-spread-its-message.

[20] Joseph Shaheen. "Network of Terror: How DAESH Uses Adaptive Social Networks to Spread its Message". 2015, p. 9-10, http://stratcomcoe.org/network-terror-how-daesh-usesadaptive-social-networks-spread-its-message.

[21] Nissen, Thomas Elkjer. "The Weaponization of Social Media". Royal Danish Defence College. Copenhagen. 2015.

[22] Lily Hay Newman. "Intelligence Officials Have Named One More Enemy in the Paris Attacks: Encryption". http://www.

stern warning to their supporters of disregarding cyber-security, and they established a law which restricted its combatants from using the geo-tagging feature which Twitter has.[23] Daesh even created a virtual support assistant and private guidebook which offers recommendations on how to guarantee operational security virtually.[24]

Inform and Influence (Psychological Warfare) – This terminology connects with the spread of data in order to impact a target audience's viewpoints, feelings, faiths, principles, thinking, comportment, beliefs and drive. Using social media in this aspect goes in the direction of more towards accomplishing specific army consequences within the intellectual realm - form, notify, impact, exploit, reveal, weaken, endorse, cheat, force, discourage, assemble, persuade.[25] How to establish one's presence on social media may be done secretly like the establishment of official profiles, outlets, URLs, opinion leader remarks, etc. or in an open way like using false profiles, botnets and trolling. All of this may be utilized in any manner on social media. How to use all of this for a group's benefit depends on them individually in a conflict. There isn't any prediction from the NATO doctrine on the utilization of secretive procedures in order to have an impact on

---

slate.com/blogs/future_tense/2015/11/16/officials_say_digital_encryption_makes_anti_terrorism_efforts_more_difficult.html.

[23] Joseph Shaheen. "Network of Terror: How DAESH Uses Adaptive Social Networks to Spread its Message". 2015, p. 9-10, http://stratcomcoe.org/network-terror-how-daesh-usesadaptive-social-networks-spread-its-message.

[24] "Social Media As A Tool Of Hybrid Warfare". NATO StratCom COE: Riga. May 2016.

[25] Nissen, Thomas Elkjer. "The Weaponization of Social Media". Royal Danish Defence College. Copenhagen. 2015.

the people. Additionally, psychological operations (PSYOPS) may be utilized just for army procedures that are proclaimed by the North Atlantic Council. On another side, extremist communities and autocratic governments frequently show dissimilar principles and don't enforce any moral boundaries on the utilization of impactful actions (secret procedures as well). War isn't constantly proclaimed and the separation of "peacetime" and "wartime" is distorted.[26] Secret procedures like this that were executed from Russian forces happened recently against Ukraine, in which a huge chunk of data which involved propaganda and fraud and gossip spread throughout the web through counterfeit accounts.[27] While mentioning the various dissimilar objectives of social media dialogue, Dr. Rebecca Goolsby brings up "social cyber-attacks" which are intentional and assembled events put in place to propagate gossip, frauds and exploitative messages virtually in order to instigate apprehension in society. As tracing the people that are responsible for conducting cyberattacks is sophisticated, they stay hidden, concealing authentic individuals and computerized bot systems. Dr Goolsby illustrates the Assam, India case study in July 2012 which was when unauthentic photos and texts on the Muslim community were spread causing a vast chaotic emigration.[28] The Ukrainian conflict filled with cyber attack instances that had been

[26] "Social Media As A Tool Of Hybrid Warfare". NATO StratCom COE: Riga. May 2016.

[27] Jolanta Darczewska. "The Anatomy of Russian Information Warfare the Crimean Operation, A Case Study". Point of View. Centre for Eastern Studies. Warsaw. May 2014. http:// www.osw.waw.pl/sites/default/files/the_anatomy_of_russian_ information_warfare.pdf.

[28] Rebecca Goolsby. "On Cybersecurity, Crowdsourcing and Social Cyber-Attack". Washington: Wilson Center. U.S. Office of Naval Research, 2013. https://www.wilsoncenter.org/sites/

utilized to instigate apprehension. For instance, Pavel Astakhov in June 2014 opened his Instagram profile to claim over 7000 Ukrainian emigrants left Ukraine and went to the Rostov Oblast over the past day or so at that time. He also stated that the number went up to 8,386 the following day. Mass media in Russia publicized those figures, however Rostov Governor's headquarters went against it and stated that it didn't surpass 712.[29]

Russia are also known to be involved in other cyber attacks as well. The most famous one being the 2016 presidential election. In October 2017, the biggest social media companies like Facebook stated that at the time of the 2016 presidential election, Russian propaganda spread to around 126 million users. All this, which was to "let loose people's rally capability" created something new in terms of a long-standing aggressive approach meant to threat U.S. organizations and determination. By linking disinformation with cyber incursions as part of an information warfare operation, it clearly shows contemporary political warfare. Russian interference in the 2016 U.S. elections shows the cyber power which Russia use in order to get what they want. This isn't for potential future attacks on the population, but are more rather designed to change people's perceptions. Therefore this action requires a lot of recognition as an important case in the Russian cyber network. The reasoning behind the 2016 presidential election tampering by the Russians was to establish an extensive mental effect on the American people, while simultaneously showing

default/files/127219170-On-Cybersecurity-CrowdsourcingCyber-Attack-Commons-Lab-Policy-Memo-Series-Vol-1.pdf.

[29] "Rostov officials refuted information about thousands of Ukrainian refugees". 2014. StopFake.org. http://www.stopfake.org/en/rostov-officials-refutedinformation-about-thousands-of-ukrainian-refugees/.

their own people the crooked ways of democratic countries. Actions like this show how espionage's efficiency is used as an exploitative tool. Frequently labelled as "reflexive control" or "active measures", this espionage type attempts to have an impact on the enemy by having data power and exploitation helped by misinformation, procedures all done short of war. This procedure which ended with the tampering of the presidential campaign began in 2015 prior to when Donald Trump ran for president. Summer 2015 was when Russia began to distribute many phishing emails attempting to get people into clicking on those spiteful links.[30] When the Senate Testimony was happening, Thomas Rid documented that around 2.4% of the strikes had been effective in creating data.[31] Russia's violations hadn't been noticed up until when the New York Times claimed in June 2016 that two dissimilar Russian hacker factions named Cozy and Fancy Bear infiltrated the Democratic National Committee's (DNC's) computer networks.[32] It was all about observing the DNC's communications and as well withdrawing their data involving rival studies regarding Donald Trump. This data, while adhering to the principles of the KGB (Komitet Gosudarstvennoy Bezopasnosti) which is the English Committee for State Security, hub of overseas acumen and

[30] Benjamin Jensen, Brandon Valeriano & Ryan Maness. "Fancy Bears and Digital Trolls: Cyber Strategy With a Russian Twist". Journal of Strategic Studies. 2019. DOI: 10.1080/01402390.2018.1559152.

[31] Thomas Rid. "Disinformation: A Primer in Russian Active Measures and Influence Campaigns". Hearings before the Select Committee on Intelligence. United States Senate. One Hundred Fifteenth Congress. 30 Mar 2017.

[32] David Sanger. "D.N.C. Says Russian Hackers Penetrated Its Files, Including Dossier on Donald Trump". New York Times. 14 Jun 2016.

local security forces of the U.S.S.R. may be utilized to either strengthen bigger impact procedures or to blackmail to get total control. The e-mails which had been stolen from Hillary Clinton's employees could possibly be seen as the most damaging data snatches, worsening a long-term concern revolving around the query of accumulated emails on Hillary Clinton's private home network. John Podesta's emails somehow managed to get stolen as well because of a typing mistake on an IT adviser's assistance in terms of not replying to a phishing email (illegal amended to legal). Cozy Bear were apprehended prior to them conducting procedures in unspecified White House networks, the State Department and more. Summer 2015 was when they began the infiltrating of the DNC and RNC (Republic National Committee) documents 44.[33] March 2016 was when Fancy Bear joined the party. All of these interferences simply shows the Russian cyber network's inept environment where more than one procedure has happened. Two factions aimed for the same targets, looking like as part of the same obligation while having no organization with the same guidelines. [34] Podesta's emails had been publicized during the same time as the Donald Trump's damning auditory recording of his capability to grab women struck the broadcasting networks. Data leaks that were very organized continued to the latter stages of the presidential election, showing a huge volume of partnerships amongst the data agents with Trump's campaign.

[33] Adam Greenberg. "Russia Hacked "Older" Republican Emails, FBI Director Says". Wired, 10 Jan. 2017.

[34] Benjamin Jensen, Brandon Valeriano & Ryan Maness. "Fancy Bears and Digital Trolls: Cyber Strategy With a Russian Twist". Journal of Strategic Studies. 2019. DOI: 10.1080/01402390.2018.1559152.

Russian involvement had actually been going on up until Barack Obama's and Vladimir Putin's G20 conference on Sep 5th in which Obama disapproved any more efforts from Russia to get involved in the American presidential election. All those dumps of data halted, however Russian hackers still managed to try and investigate more into state ranking election polling networks in order to find any flaws. It was in July 2016 when Hillary Clinton's campaign stated that Russia could be attempting to influence the presidential race.[35] It was on October 7th however when the Obama administration blamed Russia for tampering with presidential race.[36] A bilateral announcement had been conscripted; however the Senate Republics didn't apply their signatures to the common statement which would confirm their support in going against election tampering. This is because they believed it would favor the Democrats in terms of the election.[37] It wasn't however just the case of Russian involvement. It was also due to the leading contender supporting interferences along with dumps of data. Trump was actually relishing getting very close with WikiLeaks and it was a cause for concern.[38] Julian Assange, the founder of WikiLeaks, accused Hillary Clinton for this situation and supported the Russian administration and deciding not to

[35] Eric Lichtblau. "Computer Systems Used by Clinton Campaign Are Said to Be Hacked, Apparently by Russia". New York Times. 2016.

[36] David Sanger and Charles Savage. "U.S. Says Russia Directed Hacks to Influence Elections". New York Times. 2016.

[37] Kaveh Waddell. "Why Didn't Obama Reveal Intel About Russia's Influence on the Election"? The Atlantic. 2016.

[38] Patrick Healy, David Sanger & Maggie Haberman. "Donald Trump Finds Improbable Ally in WikiLeaks". New York Times. 2016.

publicly distribute any valuable Russian emails. Trump mentioned WikiLeaks around 164 times while his campaign was going on.[39] Combining dumps of data, spyware which aid in the release of it and finally Trump talking about all of this himself just show the control and dominance required to cause political warfare to be evil. At the Senate testimony, Clint Watts said, "part of the reason active measures have worked in the US election is because the Commander-in-Chief has used Russian active measures at times against his opponents."[40] Watts then stated that on numerous occasions, misinformation had been spread and intensified due to spyware where afterwards the Trump campaign echoed it all.[41] September 2017 was when Facebook publicized the fact they actually had business dealings worth around $150,000 with Russian operatives in terms of advertisements. Facebook admitted this after the House of Representatives interrogated them. A Russian troll farm was actually linked to these business dealings. It seems the purpose was to have an impact on important social matters like "Black Lives Matter". These advertisements lasted for nearly 2 years (June 2015 – May 2017). Right now, the Daily Beast figures that around

[39] Judd Legum. "Trump Mentioned WikiLeaks 164 Times in the Last Month of Election, Now Claims it Didn't Impact one Voter". Think Progress. 2017.

[40] Aaron Rupar. "Former FBI agent Details How Trump and Russia Team Up to Weaponize Fake News". Think Progress. 2017.

[41] Benjamin Jensen, Brandon Valeriano & Ryan Maness. "Fancy Bears and Digital Trolls: Cyber Strategy With a Russian Twist". Journal of Strategic Studies. 2019. DOI: 10.1080/01402390.2018.1559152.

23,000,000 people – 70,000,000 have seen those advertisements.[42] All these reports regarding possible Russian attacks had started since the concern raised in June 2016. Numerous sources showed the complex procedure and that it had all the signs of Russian interference, beginning with Cloudstrike that the DNC directed their attention towards. Many news companies like the New York Times put out numerous details on this matter. In Esquire (Men's magazine), Thomas Rid stated that investigators linked the main network's spyware aiming the DNC with a 2015 German Parliament attack.[43] The U.S. Intelligence Community examined the Russian procedures in January 2017 and came to the conclusion that their aim was to "undermine public faith in the U.S. democratic process denigrate Secretary [Hillary] Clinton and harm her electability and potential presidency."[44] The investigation recognized the drive with Vladimir Putin accusing Hillary Clinton on the fact that the Panama Papers had become publicized and those 2011 & 2012 Russian strikes. By the way, the Panama Papers are basically a sequence of data dumps that detects illegal banking techniques. Cyberbullying is tough, detrimental and takes up a lot of time. These Russian procedures began prior to 2016 and went on beyond the real vote. As there is no evident influence which may be spoken or written about in depth, the procedure most probably bolstered bad viewpoints on Hillary Clinton by Republicans and Bernie Sanders' supporters. Also, no poll got

[42] Ben Collins, Kevin Poulsen, & Spencer Ackerman. "Russia Facebook Fake News Could Have Reached 70 Million Americans". Daily Beast. 2017.

[43] Thomas Rid. "How Russia Pulled Off the Biggest Election Hack in U.S. History". Esquire. 20 Oct. 2016.

[44] Director of National Intelligence. "Background to Assessing Russian Activities and Intentions in Recent US Elections: The Analytical and Cyber Incident Attribution". 2017.

out which proved that the WikiLeaks case caused an increase in Trump supporters. The question to ask is however whether or not the hacks drove people to not vote for Hillary Clinton and vote for Donald Trump. It seems probable that many tactical errors contributed to Hillary Clinton losing the presidential race which involves barely focusing on the Rust belt, the lack of addressing people's concerns on immigration, the fact that her emails were under scrutiny once more and consistent gender discrimination.[45] So, not having a counter operation program which focuses on thwarting such activities had been a horrible error on America's part. Russia's main aim is just to create mayhem for their victims. In Russia's point of view, taking part in such activities only benefits them to a certain degree. This could involve in altering the U.S. government's direction, diminishing a potential president's power even prior to them taking office, etc. All of this only helps Russia in terms of Syria and Ukraine. Overall, if creating mayhem and confusion was Russia's initial aims then they definitely succeeded in that aspect.[46]

The next case study focuses on the Islamic State. The way they have used social media to make known of their propaganda is nothing short of remarkable. They have managed to gain more followers, grow their brand acknowledgement and propagated terror and horror throughout the world while exerting barely any struggle. It is actually the first group to ever use social media to

[45] Benjamin Jensen, Brandon Valeriano & Ryan Maness. "Fancy Bears and Digital Trolls: Cyber Strategy With a Russian Twist". Journal of Strategic Studies. 2019. DOI: 10.1080/01402390.2018.1559152.

[46] Benjamin Jensen, Brandon Valeriano & Ryan Maness. "Fancy Bears and Digital Trolls: Cyber Strategy With a Russian Twist". Journal of Strategic Studies. 2019. DOI: 10.1080/01402390.2018.1559152.

set out what they wanted to achieve. The Islamic State may utilize terrorism as their primary approach, but the way they conduct themselves is entirely different from any other terrorist or extremist group.[47] The dissimilarities are evident in all areas. To make progress on their goals, IS utilized communication methods which disseminated their propaganda through social media platforms in a wider community which satisfy their descriptions for people who could help them and for people who could be their enemies. Simply put, IS cyber fighters managed to mix propaganda with power and authority in order to carry out three points in one main point. This is how they did it: Firstly, IS showed the flaws and ineptness of the global society to go against them through the web and including directly on the battleground. Secondly, IS added horror throughout all mainstream media sources. Thirdly, which is the most significant, IS managed to gain new combatants to become members of their community whether be online or on the battleground.[48] The technique behind trying to get in contact with people on social media platforms like Twitter for example with just one tweet is dependent upon a system of correct retweets joined by bots and innocent people who use Twitter. IS may sustain a very powerful system of ardent followers, but their group size isn't that big and is disseminated very sparsely throughout the Middle East. So, IS has to manage the network and tamper with Twitter for any of their communications to flood the database. An advanced technique to make a bot system is an app known as "Dawn of Glad

[47] 26. Audrey Kurth Cronin. "ISIS Is Not a Terrorist Group,". Foreign Policy (March/April 2015). https://www.foreignaffairs.com/articles/middle-east/isis-not-terrorist-group.

[48] Jarred Prier. "Commanding the Trend: Social Media as Information Warfare, Strategic Studies Quarterly, Air University Press. 2017. https://www.jstor.org/stable/10.2307/26271634.

Tidings". IS cyber fighters made the app and keeps everyone informed regarding their events and mystical support with the people who interact with their app. Once people access the app, the make their profiles which connects to their Twitter profiles, and provides the app the ability to tweet using their profiles.[49] Afterwards, the app tweets again for the person once the main profile delivers an IS labeled tweet. As time passes, the hashtag produces sufficient responses to begin domestic trends. As the trend starts to grow, it's transmitted over trend-examining systems such as the account @ActiveHashtags.33 which is Arabic. It leads to more people getting aware of the hashtag throughout the area which will subsequently get retweeted by ardent followers along with various different bot profiles. Finally, it's all about the trend going worldwide**.**[50] International Twitter trends are like a blessing for IS. Had IS not prioritized the making and the stealing of trends on social media, they would've definitely gone undetected. It was in the 2014 FIFA World Cup when IS trend stealing was at its pinnacle. Combining the world's most popular sport with an event like the World Cup, it's not a shock to see #WorldCup2014 trending all over Twitter while the tournament was going on. There was a stage when each tweet that was a part of this hashtag was somehow connected with IS and not soccer. IS followers stole that trend. What's interesting is that, due to the popularity of that trend for fans and salespeople, Twitter didn't have the power to remove the trend and the propaganda IS spread afterwards**.** Currently however, IS are using social media far less. There could be two reasons for this: Firstly, IS no longer have control over Iraq and

[49] J. M. Berger. "How ISIS Games Twitter,". Atlantic, 16 June 2014. https://www.theatlantic .com/international/archive/2014/06/isis-iraq-twitter-social-media-strategy/372856/.

[50] Jarred Prier. "Commanding the Trend: Social Media as Information Warfare, Strategic Studies Quarterly, Air University Press. 2017. https://www.jstor.org/stable/10.2307/26271634.

Syria in certain territories, so they're modifying their approaches. Secondly, Twitter got rid of more than 600,000 IS-connected profiles which were made up of ardent followers, cyber fighters and more.[51] Moreover, Twitter has become more cautious regarding any propaganda coming from IS so they have managed to modify their platform to find any photos, videos or memes coming from IS.[52]

In conclusion, it's safe to say that from what this essay has demonstrated is, it is vital to properly differentiate between autocratic systems and democratic systems. The main difference is how the two systems look at information. Democracies give a lot of importance to collective rights of media and the public, freedom of speech and union. Autocratic governments however look at information like it's a danger to state power if it's permitted to just naturally happen at ease and as well like a social power tool if it's controlled and used skillfully. These governments interact a lot with monitoring, misinformation and suppression while utilizing the media with more instruments in order to have power and exploit data in the state's interests. In other words, democracy shows that the public control the information and in autocracy, the ones in power control the information. In order to flourish in the data sector, democracies must redesign the race so that they can profit from their own advantages and manipulate the weaknesses in the autocratic systems. This redesign needs to be parallel to growing the global democratic perception of information while adhering to

[51] Carleton English. "Twitter Continues to Wage its Own War against ISIS,". New York Post. 21 March 2017. http://nypost.com/2017/03/21/twitter-continues-to-wage-its-own-war-against-isis/.

[52] Jarred Prier. "Commanding the Trend: Social Media as Information Warfare, Strategic Studies Quarterly, Air University Press. 2017. https://www.jstor.org/stable/10.2307/26271634.

the strategies of the data race as well. This is what is fundamentally missing from the democracies' contemporary approach towards the information sector which results in giving the autocracies the edge where currently the global autocratic perception is in line with the strategies of information warfare. Democracies must be competitive with their own regulations and shouldn't just shape up a stronger community against autocratic information exploitation, but to grasp the edge in this race. This means to be clear, honest and multilaterally authorize data users and preserve freedom of speech to grow a worldwide information sector which upholds and intensifies the value of information globally. The ways in which this battle is combated is fundamental to see who will win this race.[53]

[53] Laura Rosenberger & Lindsay Gorman. "How Democracies Can Win the Information Contest". The Elliot School of International Affairs. The Washington Quarterly. 2020. P. 92, https://doi.org/10.1080/0163660X.2020.1771045.

References

- Aaron Rupar. “Former FBI agent Details How Trump and Russia Team Up to Weaponize Fake News”. Think Progress. 2017.

- Audrey Kurth Cronin. “ISIS Is Not a Terrorist Group,”. Foreign Policy (March/April 2015). https://www.foreignaffairs.com/articles/middle-east/isis-not-terrorist-group.

- Adam Greenberg. “Russia Hacked “Older” Republican Emails, FBI Director Says”. Wired, 10 Jan. 2017.

- Armin Rosen. “A Self-Proclaimed ISIS Fan is Hacking Local News Outlets”. 6 January 2015. http://www.businessinsider.com/ a-self-proclaimed-isis-fan-is-hacking-local-news-outlets-2015-1.
- Ben Collins, Kevin Poulsen, & Spencer Ackerman. “Russia Facebook Fake News Could Have Reached 70 Million Americans”. Daily Beast. 2017.
- Benjamin Jensen, Brandon Valeriano & Ryan Maness. “Fancy Bears and Digital Trolls: Cyber Strategy With a Russian Twist”. Journal of Strategic Studies. 2019. DOI: 10.1080/01402390.2018.1559152.
- Carleton English. “Twitter Continues to Wage its Own War against ISIS,”. New York Post. 21 March 2017. http://nypost.com/2017/03/21/twitter-continues-to-wage-its-own-war-against-isis/.
- David Sanger. “D.N.C. Says Russian Hackers Penetrated Its Files, Including Dossier on Donald Trump”. New York Times. 14 Jun 2016.

- David Sanger & Charles Savage. “U.S. Says Russia Directed Hacks to Influence Elections”. New York Times. 2016.
- David Stupples. “The Next Big War Will Be Digital and We Are Not Ready For It”. The Conversation. November 26, 2015. https://theconversation.com/the-next-war-will-be-an1information-war-and-were-not-ready-for-it-51218.
- Director of National Intelligence. “Background to Assessing Russian Activities and Intentions in Recent US Elections: The Analytical and Cyber Incident Attribution”. 2017.
- Eric Lichtblau. “Computer Systems Used by Clinton Campaign Are Said to Be Hacked, Apparently by Russia”. New York Times. 2016.
- Jan Joel Andersson. “Hybrid operations: lessons from the past”. EUISS. October 2015. http://www.iss.europa.eu/ uploads/media/Brief_33_Hybrid_operations.pdf.
- Jarred Prier. “Commanding the Trend: Social Media as Information Warfare, Strategic Studies Quarterly, Air University Press. 2017. https://www.jstor.org/stable/10.2307/26271634.
- J. M. Berger. “How ISIS Games Twitter,”. Atlantic, 16 June 2014. https://www.theatlantic .com/international/archive/2014/06/isis-iraq-twitter-social-media-strategy/372856/.
- Joseph Shaheen. “Network of Terror: How DAESH Uses Adaptive Social Networks to Spread its Message”. 2015, p. 9-10, http://stratcomcoe.org/network-terror-how-daesh-uses1adaptive-social-networks-spread-its-message.
- Judd Legum. “Trump Mentioned WikiLeaks 164 Times in the Last Month of Election, Now Claims it Didn’t Impact one Voter”. Think Progress. 2017.

- Kaveh Waddell. “Why Didn’t Obama Reveal Intel About Russia’s Influence on the Election”? The Atlantic. 2016.

- Laura Rosenberger & Lindsay Gorman. “How Democracies Can Win the Information Contest”. The Elliot School of International Affairs. The Washington Quarterly. 2020. P. 92, https://doi.org/10.1080/0163660X.2020.1771045.

- Lily Hay Newman. “Intelligence Officials Have Named One More Enemy in the Paris Attacks: Encryption”. http://www.slate.com/blogs/future_tense/2015/11/16/officials_say_digital_ encryption_makes_anti_terrorism_efforts_more_difficult.html.
- Maksymilan Czuperski, John Herbst Eliot Higgins, Alina Polyakova & Damon Wilson. “Hiding in Plain Sight: Putin's War in Ukraine, Atlantic Council”. October 2015, http://www.atlanticcouncil.org/publications/reports/ hiding-in-plain-sight-putin-s-war-in-ukraine-and-boris-nemtsov1s-putin-war.
- Nissen, Thomas Elkjer. "The Weaponization of Social Media”. Royal Danish Defence College. Copenhagen. 2015.
- Patrick Healy, David Sanger & Maggie Haberman. “Donald Trump Finds Improbable Ally in WikiLeaks”. New York Times. 2016.
- Peter Foster. ‘‘Bogus’ AP tweet about explosion at the White House wipes billions off US markets”. 23 April 2013.

http://www.telegraph.co.uk/finance/markets/10013768/Bogus1AP-tweet-about-explosion-at-the-White-House-wipes-billions1off-US-markets.html.

- Rebecca Goolsby. “On Cybersecurity, Crowdsourcing and Social Cyber-Attack”. Washington: Wilson Center. U.S. Office of Naval Research, 2013. https://www.wilsoncenter.org/sites/default/files/127219170-On-Cybersecurity-Crowdsourcing1Cyber-Attack-Commons-Lab-Policy-Memo-Series-Vol-1.pdf.
- “Rostov officials refuted information about thousands of Ukrainian refugees”. 6 June 2014. StopFake.org. http://www.stopfake.org/en/rostov-officials-refuted1information-about-thousands-of-ukrainian-refugees/.
- “Social Media As A Tool Of Hybrid Warfare”. NATO StratCom COE: Riga. May 2016.
- “US Centcom Twitter account hacked by pro-IS group”. 12 January 2015. http://www.bbc.com/news/world-us1canada-30785232.
- Thomas Rid. “Disinformation: A Primer in Russian Active Measures and Influence Campaigns”.
- Thomas Rid. “How Russia Pulled Off the Biggest Election Hack in U.S. History”. Esquire. 20 Oct. 2016.