Spring 2019

The New Geopolitical Space in the Information Era: A Neuroscientific Approach to National Security

Naomi Silverstein

The New Geopolitical Space in the Information Era

A Neuroscientific Approach to National Security

By Naomi Silverstein

Spring 2019

School of International Training (SIT)

Geneva: International Studies and Multilateral Diplomacy

Dr. Elizabeth Meur, Ph.D.

Dr. Gyula Csurgai, Ph.D.

University of Michigan, Ann Arbor

Biopsychology, Cognition and Neuroscience (BCN)

Political Science

Abstract

Cognitive Warfare, is the interdisciplinary use of technology and an understanding of the brain's natural processes to influence opinion and behavior. Also known as sharp power, these methods are more technical and accurate than Cold War-age propaganda, and more personal than typical information warfare. With tools like disinformation and big data, outsiders have the ability to exploit vulnerabilities, manipulate belief formation and disseminate a chosen narrative on the grand scale. Examples of events that utilized cognitive warfare to influence sentiment include the 2016 U.S. Presidential election, Russian annexation of Crimea, and the UK's vote to withdraw from the European Union – the chosen case study for this paper. This paper will form a comprehensive analysis of the psychological factors at play and the components unique to the current Information Era to describe what make cognitive warfare so effective. The morality of sharp power is a big question but one that will not slow the world's ambition for technological innovation and neuropsychological discovery.

Acknowledgments

Thank you Dr. Meur for being a wonderful advisor and guiding me through this process. Your advice was instrumental in planning this paper.

I would like to thank my professors who supported my peers and me throughout this semester, Dr. Csurgai and Dr. Matilla. Their lectures, review sessions, office hours, etc. all contributed to my education and the success of this paper.

I also thank Aline Dunant and Christina Cornes for their logistical assistance and making sure my stay in Switzerland was so wonderful.

A special thank you to my incredible host family! Thank you for graciously welcoming me into your home for these three months.

I would also like to thank all my classmates here at SIT for always supporting one another and creating a healthy, inquisitive environment.

Of course, a huge thank you to my parents and siblings for supporting me and allowing me to take part in this amazing program.

Table of Contents

Introduction

The concept of war has changed dramatically over the course of human civilization. The line between war and peace used to be indicated with rituals, proclamations, and marked uniforms. Conventional armies with combatants were responsible for all aspects of the hostilities: observation, decision-making, combat, diplomacy, and so on (A. Vautravers, personal communication, 11/04/2019). Guerrilla warfare was an innovation that allowed smaller groups to compete with the shear mass and strength of the traditional armies of the developed world. Militaries had to transition and learn how to combat decentralized and small-scale surprise attacks. Now, the world is again in a time of transition. The combination of technological innovations and neuroscientific discoveries has led to a new reality with never before seen threats and vulnerabilities.

The Information Era began in the 1960s, and with it arose information warfare. Society quickly learned that accumulating data allowed for increased insights and efficiency. Likewise, the internet furthered globalization and allowed for both faster and broader distribution of information. However, as technology evolves, so do the threats. The digital world revealed entirely new weapons that militaries have been perfecting ever since their benevolent discovery. Data can be analyzed to reveal and take advantage of vulnerabilities, and the internet can be used to spread disinformation without regard for the truth, thus, largely polluting the information pool.

Geopolitics is the method of determining strategies and analyzing political power with an emphasis on the overlap of disciplines. These include the obvious current political dynamics, but also population demographics, geography, natural resources, history, economics, and security issues. The new inclusion of neuropsychological functions in geostrategy gives rise to a new geopolitical space that can be controlled and influenced: the brain. Amazing advances have

occurred in neuroscience and psychology in recent decades that allows for a solid understanding of the systems that correspond with information processing and belief formation. With this knowledge, outsiders can ascertain which messages would be most effective on the audience and how to focus persuasive messaging at the systems' most vulnerable points. This intentional exploitation of the brain's natural processes to influence perceptions and corresponding behaviors is called *cognitive hacking* – echoing the unauthorized access and hacking of computer data system.

Combining new knowledge of neuroscience and brain functions with new technological capabilities reveals not only a new method of combat, but an entirely new battlefield – one that lies within the public's mind. Militaries and other outsiders seek influence over the thought process because it allows them to subconsciously sway public opinion and perception of both domestic situations and global events. If correctly manipulated, they can even predict and guide actions and behaviors to benefit their own interests. This is called Cognitive Warfare. The tools of cognitive warfare include an understanding of the brain's natural processing pathways, disinformation campaigns, internet and technology, and social networks and the media (Waltzman, 2017). Consistent with humans' desire for accurate categorization to understand their world, this new manner of leveraging influence is also referred to as "sharp power." This term is in opposition to hard power – blatant threats and shows of military force to coerce agreeable behavior – and soft power – the attraction a country garners through various forms of aid, cultural ideals, etc. that develops into dependence and manipulated compliance with the donor's interests (Walker, 2017). Sharp power is the academic's attempt to characterize the techniques that take advantage of psychology, the media and the public's influence on national

policy trajectory (more so influential in democratic nations) in order to “pierce, penetrate, or perforate the political and information environments in the targeted countries” (Walker, 2017).

Democratic societies are ideal targets for sharp power and disinformation campaigns due to free speech culture and generally laissez-faire internet policies. For this reason, the conversation is often framed in a way that vilifies authoritarian regimes like China and Russia and victimizes the United States and other Western nations. While engaging in these external efforts, authoritarian governments are also well equipped to control their own population’s dialogue through domestic disinformation campaigns and strong censorship.

The rise of sharp power capabilities is not exclusive to governments and militaries. Private companies also recognize value of strategically targeting messages to more efficiently and effectively achieve a goal. Describing themselves as “political consulting” firms, they utilize personal data acquisition and analysis to determine exactly who and how to target with persuasive messaging. In this sense, they serve as the military strategists in the battle for cognitive influence. Contractors purchase these firms’ services, thereby digitizing and modernizing the traditional mercenary.

This paper will provide a comprehensive analysis of the psychological and neuroscientific phenomena at play in cognitive warfare and how they are augmented with big data technology and factors of globalization. These concepts will then be applied to dissect the events leading up to the 2016 Brexit Referendum. Finally, this paper will gloss over recommendations for how both the general public and the government can defend against sharp power techniques.

Literature Review

A lot of literature exists that delves into the threat of cyber warfare and how hacking unauthorized information can harm groups. As cognitive warfare has gained recognition, some global security experts have completed analyses on the strategies employed by cognitive attackers, although they tend to focus on the technological aspects of the scheme or specifically on Russian manipulations.

Separately, psychologists and neuroscientists have researched the factors contributing to opinion and how people can be persuaded. Many have looked at the biological, evolutionary explanations for beliefs and behavior while others explore specifically how external factors like social media affect cognition.

Carole Cadwalladr is a journalist for The Guardian and thoroughly investigated the people and events behind the scenes of the 2016 Brexit referendum campaigns. Her work exposed the personal and business connections, policy loopholes, and technology that allowed the referendum decision to be influenced.

The objective of this paper is to form a thorough analysis that brings together the psychological factors that outsiders exploit to efficiently guide opinions and behaviors and the factors present in society that are new with the information era that allow manipulation on the large scale from abroad. These concepts will then be applied to a case study on the 2016 Brexit referendum.

Research Methodology

This research will utilize both qualitative and quantitative data to analyze the presence and effects of cognitive warfare and disinformation. Secondary, qualitative research includes online articles from trusted sources and peer-reviewed articles found through the JSTOR

database. Additionally, interviews with experts in the fields of global security, cybersecurity, and neuroscience serve as *primary* qualitative sources. These individuals were chosen due to their own relevant research or work experience. on the topic and This research also analyzes quantitative data collected by third-parties.

The ethical considerations of this research involve permission to publish and recognition of intellectual property from sources and interviewees. The study received verbal permission to quote the interviewees and ideas. The study followed all regulations regarding citing the sources for data and statistics.

Cognitive Hacking

Disinformation

Disinformation is the deliberate spreading of intentionally false messaging with the aim of misleading the target and obscuring the truth. This is in opposition to *mis*information which is not necessarily intentionally false information with a harmful purpose. The objective of disinformation campaigns is "not just to present an alternate version of reality, but rather to contaminate the information space" and compromise the public's ability to discern the truth (Mahairas, 2018). This puts forth the attitude that "no news source or narrative can be trusted," which pressures "the audience to connect with whichever storyline appeals to its pre-existing biases" – thus, leaving the public extremely vulnerable to cognitive hacking and propaganda.

Disinformation campaigns are not new and have been conducted for decades. Though the term entered English dictionaries only in the 1980's, in as early as the 1920's, Russia supported a special disinformation office that engaged in "Active Measures strategy" meant to "influence[] world events to achieve its geopolitical goals" (Mahairas, 2018). KGB Major General Kalugin

considered disinformation the "heart and soul of Soviet intelligence."

> "Not intelligence collection, but subversion: active measures to weaken the West, to drive wedges in the Western community alliances of all sorts, particularly NATO, to sow discord among allies, to weaken the United States in the eyes of the people of Europe, Asia, Africa, Latin American and thus prepare ground in case the war really occurs" (Mahairas, 2018).

Russia is far from the only military that recognizes the potential of disinformation and utilizes it to their advantage. If used strategically, disinformation has enormous potential for widening societal rifts, exacerbating internal discord and proliferating general feelings of mistrust and skepticism.

Cognitive Vulnerabilities

Disinformation preys on the *cognitive vulnerabilities* of its targets by taking advantage of pre-existing anxieties or beliefs that predispose them to accept false information (Waltzman, 2017). This requires the attacker to have an acute understanding of the socio-political dynamics at play and to know exactly when and how to penetrate to best exploit these vulnerabilities.

Cognitive vulnerabilities and the ensuing aggression or hostility when provoked is a result of evolutionary neuro-circuitry. Humans have always been a social, group-oriented specie. As with many other such species, acceptance into a group was necessary for survival. Self-preservation relied on group-preservation so anything unfamiliar was deemed a potential threat to the safety of the individual and the group – whether in terms of physical safety, competition for resources, etc. (Fields, 2016). Instinctive aggression developed as a self-defense mechanism in response to unfamiliar potential threats to group way of life. Humans undergo an unconscious and very fast assessment of threat level that leads to a reaction in the amygdala – a brain region critical for emotional learning and is often associated with attitudes toward race (Al-Rodhan, 2016).

This primeval aggression is wired into humankind's brain and has persisted into the modern world. Civilized society displays this aggression more commonly as "in group favoritism" and "out-group devaluation" (Al-Rodhan, 2016). This dynamic exists on every level of society with even the most inconsequential of dividing lines: family vs. not, wealthy vs. poor, white vs. black, Boston Red Sox vs. New York Yankees, and so on. On the global scale, this phenomenon is viewed as harmless nationalism. Rooted in a lack of understanding, individuals perceive unfamiliar others as a threat, thus they may denigrate the nonmembers as a form of self-defense meant to assuage personal anxieties. fMRI experiments support this in-group/out-group dichotomy. Studies have shown that the "mirror neurons" that are typically responsible for empathy are turned off when the brain perceives an out-group member, thus predisposing the subject to resist an emotional connection to the target (Al-Rodhan, 2016).

This natural reaction to unfamiliar others can easily be exploited. Concerns regarding the outsider, though dormant, already exist so the disinforming messages need to only activate it. Successful disinformation campaigns not only activate, but "amplify existing divisive issues in order to further expand the space separating the targeted audience; thereby, making reconciliation between any two sides of a divisive issue even more difficult to achieve" (Mahairas, 2018). Disrupting society in this way harms the productivity of governments by forcing attention to irrational populist concerns and increasing polarization, thus estranging the officials who are supposed to solve problems and advance society.

Belief Formation

While the technical abilities are important in order to widely distribute the attack or to target a specific individual, the most important weapon is a keen understanding of the brain's processes. The brain employs many heuristics – or shortcuts – in order to absorb information and

maneuver the world faster and with less energy. The brain is constantly processing information and forming beliefs so these heuristics can be very helpful but also are a source of vulnerability. If the attacker understands these processing pathways, then they are capable of identifying interception points that will allow the attacker to affect the target's perception.

An individual's opinion on a certain topic is the amalgamation of multiple factors. Influence from parents and peers, group identification, and the portrayal of current event in the media can together lead to a belief. *Assimilation* is the tendency to interpret information through the lens of existing beliefs (Golman, 2016). The bias exists because people create mental *schemas* to help organize information about the world around them. These schemas affect interpretation, storage and recollection of information and allow for easier maneuvering in the world – thus influencing behavior. Festinger's *Cognitive Dissonance Theory* reveals humans' inherent desire for consistency, explaining the desire for new information to confirm existing beliefs (Harmon-Jones, 2012). This can also be linked to the ego in that altering an existing belief would require acknowledging that the previously held belief was wrong. Assimilation facilitates consistency but can also distort reality for the individual and influence new opinions. *Figure 1.* identifies the sources that influence an individual's opinion over a temporal dimension (Prier, 2017). This diagram illustrates that prior opinions influence the present relevant opinion directly and also the individual's perception of a current event – this is assimilation at work! The figure also identifies the most susceptible instances where attackers can focus their efforts to manipulate these prior opinions to their future benefit.

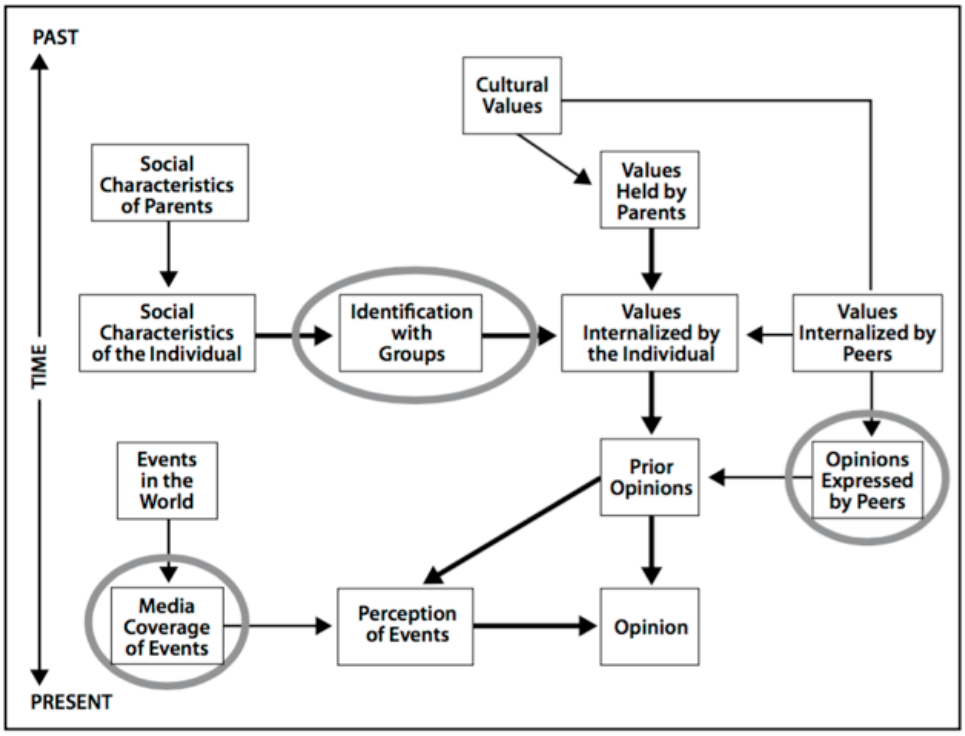

Figure 1. *Model of individual opinion formation. Bold arrows signify stronger influence on final opinions than thin arrows. Circles indicate points most vulnerable to penetration and exploitation. (Prier, 2017).*

The *availability heuristic* is the simplest tool used to influence the masses. Through this process, a concept is deemed more likely or plausible based on how immediately the subject is able to think of an example. This is generally based on how much contact the individual has with the concept and can be triggered by simply a vast volume of repetitive messaging. *Propaganda* is an obvious example of exploiting the availability heuristic. Repeated exposure to a specific narrative or piece of information causes easier retrieval and, eventually, acceptance of the information as truth. Targets are predisposed to accept messaging that appeals to pre-existing beliefs and anxieties so propaganda is often designed to work in accordance with cognitive vulnerabilities. However, even if the message is initially rejected by the target, continued exposure can succeed in normalizing the information until it is accepted. The availability heuristic is a tool that, by striving for normalization and easy retrieval, any attacker can use to

plant potentially harmful messages.

Captology

Internet & Globalization

Each generation yields new technology that furthers globalization and allows for both benevolent and malicious innovations. The introduction of air travel in the early 20th century immediately made the world much smaller and more accessible while also putting more of the world's population within reach of assailants. Likewise, the invention of the internet in 1983 and the World Wide Web in 1991 allowed for information sharing and collaborations between scientists, universities and institutes around the globe (A short history of the web, CERN). The commercialization of the internet in 1995 brought increased revenue, increased job opportunities and a streamlining of infrastructures. It also birthed *captology – Computers as Persuasive Technology (CAPT)* (P. Hérard, personal interview, 04/04/2019). Captology is the methods used by websites, mobile apps, video games, etc. to target behaviors in their audiences with the end goal of predicting and guiding behaviors. Many sources use these techniques to increase online traffic and profits; but, captology is not just a threat to one's wallet. It has broad applications and has the ability to influence societal attitudes, leading to changes in behaviors that can influence global events and politics.

Search engine optimization is the practice of maximizing online traffic to a particular website by ensuring its appearance near the top of a search engine's results list. The algorithms that search engines use to develop the results list can be manipulated in dramatic ways. Internet-based attackers are able to create thousands of automatic "bot accounts" to increase the number of clicks to a particular web page following a search. The search engine optimization algorithm

already in use perceives this increased traffic and will prioritize the web page by moving it higher in the results list for all subsequent searches of that keyword (Prier, 2017). In this way, attackers are able to push mass distribution of (dis)information to a broad audience – which, in turn, can trigger the availability heuristic and assimilation, later influencing opinions and behaviors.

Effects of Liberalism

Freedom of speech and of the press is an important liberty that is vital to democratic societies. A side effect of free speech on the internet is its correlation with the volume and type of disinformation presented to the public (S. Motte, personal communication, 01/03/2019). The United States prides itself on this liberty and is consequently more at risk of disinformation campaigns. (The English language's popularity around the globe is also a contributing factor). On the other side of this spectrum lies authoritarian regimes and those that greatly restrict and censor the internet.

Globalization creates a public good of knowledge, technology and information sharing that authoritarian regimes are able to free ride off of while maintaining their barriers. At the same time, these regimes have the ability to inject whatever information they want into exposed democratic societies. Christopher Walker, sharp power expert and vice-president of Studies and Analysis at the National Endowment for Democracy, aptly describes this dynamic:

> "Critical to their success has been their exploitation of a glaring asymmetry: in an era of hyperglobalization, the regimes in Russia and China have raised barriers to external political and cultural influence at home while simultaneously preying upon the openness of democratic systems abroad" (Walker, 2017).

These regulation differences greatly affect the narratives presented to the public. The semipermeable quality of authoritarian news agencies and internet gives the administration the

ability to shape discourse and guide public opinion with ease while the information pool in democracies is essentially a sitting duck at the disposal of any group seeking influence. Additionally, the fluid and open atmosphere in democracies makes detection of disinformation and malicious narratives difficult – even if identified, retraction may not be possible. In this way, disinformation campaigns targeting democracies benefit from the lag time before detection, during which time the public has already accepted the narrative, incorporated it into schemas and begun using it to process new information.

Another aspect complicating the regulation of cognitive warfare techniques is the liberal market economy and questions of sovereignty. A liberal market economy supports competitive innovation with the government's role only to ensure a fair and free market. This system gives private companies the liberty to do contracted work for anyone they please, including, for instance, a foreign government (S. Koch, personal communication, 10/04/2019). In a free market economy, the domestic government has no jurisdiction over a domestic company. This leaves the domestic country and government vulnerable to the tools developed possibly with their own investments.

Big Data & Social Networks

Social networks are an important contributing factor to captology and disinformation's success. Big data enables private companies to acquire a vast amount of personal information of millions of people. Artificial intelligence utilizes big data to identify these correlations and categorize people, thus creating a "mathematical representation of people" that are used to devise algorithms that effectively target categories of people with messaging they are predisposed to accept (S. Koch, personal communication, 10/04/2019). Social networks like Facebook encourage users to show their uniqueness by personalizing their profiles through follows, likes,

listed interests, etc. This all adds to the stockpile of data available. The data is then organized and people are categorized in order to create algorithms for how to most effectively target their messages. But what sort of information is exploited?

Of course, blatant political indicators are factored into these algorithms, but so are seemingly inconspicuous preferences. The music and fashion industries are extremely indicative of an individual's "populist political signaling" (Ferrier, 2018). The fashion industry was greatly weaponized in the United States' 2016 presidential election. Using data from Facebook, "political consulting" firm Cambridge Analytica found that preferences for American denim brands like Wrangler and Lee Jeans are correlated with mistrust and low levels of openness – these signaled that these individuals are more likely to engage with conservative, pro-Trump messaging (Ferrier, 2018). The mastermind behind this revolutionary operation, Christopher Wylie, notes that culture can be viewed as a "distribution of attributes" and that by "indulg[ing] in light stereotyping" they can accurately predict and guide behaviors (Ferrier, 2018).

FACEBOOK SUBSCRIBERS AND WORLD POPULATION STATISTICS
JUNE 30, 2017 - Update

World Regions	Population (2017 Est.)	Population % of World	FACEBOOK 30 June 2017	Penetration (% Population)	Growth 2010-2017	Users % of Table
Africa	1,246,504,865	16.6 %	**160,207,000**	12.9 %	809.9%	8.1 %
Asia	4,148,177,672	55.2 %	**736,003,000**	17.7 %	686.4%	37.2 %
Europe	822,710,362	10.9 %	**343,273,740**	41.7 %	111.8%	17.3 %
Latin America / Caribbean	647,604,645	8.6 %	**370,975,340**	57.3 %	444.0%	18.7 %
Middle East	250,327,574	3.3 %	**86,700,000**	34.6 %	641.1%	4.4 %
North America	363,224,006	4.8 %	**263,081,200**	72.4 %	166.5%	13.3 %
Oceania / Australia	40,479,846	0.5 %	**19,463,250**	48.1 %	67.8%	1.0 %
WORLD TOTAL	**7,519,028,970**	**100.0 %**	**1,979,703,530**	**26.3 %**	**282.3%**	**100.0 %**

Figure 2. *Chart via https://www.internetworldstats.com. (Demographic numbers are based on data from the United Nations Population Division. Facebook subscriber information comes from data published by Facebook.)*

Along with data acquisition, the popularity of social networks like Facebook and Twitter allow for extensive dissemination of information. As of 2017, over a quarter of the world's population have Facebook profiles which inescapably exposes them to an inundation of targeted

advertising (*Figure 2.*). These advertisements may come from specific product companies or clothing stores recently browsed by the individual, but others have foreign origins with less benign intentions. For example, the Russian Internet Research Agency (IRA) influenced American sentiment regarding the 2016 presidential election through numerous avenues (Mueller, 2019). The IRA created Facebook accounts pretending to be both individual U.S. people and larger political activist groups and organizations. Over 3,500 advertisements purchased by the IRA promoted these IRA-controlled groups in the newsfeeds of their U.S. audience (Mueller, 2019). "In total the IRA –controlled accounts made over 80,000 posts before their deactivation in August 2017, and these posts reached at least 29 million U.S. persons and 'may have reached an estimated 126 million people'" – almost half of the number of North Americans on Facebook (Mueller, 2019).

The IRA's Twitter approach utilized many of these same techniques while also taking advantage of bot network optimization tools as described above. Through its bot network of over 50,000 automated accounts, the IRA tweeted more than a million times in the ten weeks leading up to the presidential election (Mueller, 2019). This strategy of automatic bot networks enables the IRA to create a sea of new influential content and also greatly amplify chosen information in the American public's newsfeeds.

Social networks greatly enhance an individual's accessibility. Profiles and online interactions make personal data instantly available for extraction, and the newsfeed allows for limitless penetration into the individual's consciousness. This process of data acquisition and then dissemination of strategic information allows the individual to essentially curate their own personal disinformation package. While this sounds lovely and personalized, the system is used

against the individual to influence perceptions and behaviors that serve the ultimate objectives of the aggressors.

Case Study: 2016 Brexit referendum

The 2016 referendum decision that the United Kingdom (UK) should separate from the European Union (EU) is regarded as one of the largest examples of right-wing populism in the recent developed world. A populist referendum is considered the best way to assess the attitudes of a state's citizenry and allow them to guide the trajectory of policy; but, in a democratic society, this proves to be a double-edged sword. The rise of privatized sharp power tools is a critical threat to democracy through their pervasiveness in "the spheres of culture, academia, media and publishing – sectors that are crucial in determining how citizens of democracies understand the world around them" (Walker, 2018).

The question of disassociating from the European Union begins with British nationalism. The cohesiveness of the EU relies on each member wholly identifying with the united group. However, the UK did not fully embrace this identity – apparent in its decision to keep the Pound sterling as its currency and reject the Euro. The requirement that some policy independence be relinquished to the EU aroused the belief that British identity and economic opportunity were threatened; or, at least, that the UK would be better off unencumbered by EU regulations (Fields, 2016). This concern for group-preservation began the in-group favoritism/out-group devaluation mentality and initiated the rejection of EU membership. This is the main pre-existing anxiety, or cognitive vulnerability, that was exploited by campaigners and political consulting firms.

The Brexit referendum campaigns and decision are disputed for multiple reasons. First, there are morality and legality concerns regarding the acquisition and use of personal data by

political consulting firms that were contracted by campaigns. Second, the UK exercises campaign collaboration restrictions that are meant to even the playing field between campaigns which some believe were violated. Third, many are concerned about foreign influence on the referendum decision via American billionaires in senior positions within the political consulting firms contracted by Brexit campaigns. This analysis will focus on the first concern.

Campaign Breakdown

As with all political votes, there were multiple campaigns on either side of the proposal. Generally, the "leave" side of the ballot was comprised of mostly right-wing conservatives while the younger, left-wing population leaned toward remaining in the EU. "Vote Leave" and "Leave.EU" were the two most prominent leave campaigns – the former targeted the middle England region with messages claiming better health services upon withdrawal, and the latter "target[ed] Ukippers and disaffected working-class Labour voters with images of queues of refugees" (Cadwalladr, Follow the data, 2017). Vote Leave contracted *AggregateIQ (AIQ)* to assist in data analysis, marketing and advertising – accounting for 40% of Vote Leave's campaign budget – while Leave.EU employed *Cambridge Analytica's (CA)* services (Cadwalladr, Revealed: the ties that bound…, 2018). *SCL Elections* is the parent company of Cambridge Analytica (for which Steve Bannon was previously vice-president); however, Cambridge Analytica and its owner Robert Mercer also owned the intellectual property of AggregateIQ (Cadwalladr, Revealed: the ties that bound…, 2018). This dips into the second concern marking the Brexit referendum. Given the firms' connection and their similarity and overlap of cognitive warfare techniques and to simplify the analysis, this analysis will not differentiate between the two companies and will address their actions as of a single source, referring to them jointly as "CA-AIQ."

Background & Data Harvesting

In 2014, Steve Bannon was editor-in-chief of Breitbart News Network and he established the London bureau with the deliberate intent to inject right-leaning, pro-leave discourse into the UK ahead of the 2016 Referendum. Immediately, this affects public opinion because it alters the information pool and amplifies particular political narratives. Bannon did not stop here.

Prior to Bannon's involvement or Robert Mercer's investments, SLC Group was proving itself elsewhere in the world. As a private contractor specializing in psychological operations ("psyops") – directing public sentiment through "informational dominance," manipulation and disinformation –, SLC was contracted by the UK's Ministry of Defense for counter-extremist operations in the Middle East, the US Department of Defense for work in Afghanistan, and also influenced more than 200 elections around the world including several Caribbean elections (Cadwalladr, I made Steve Bannon's…, 2018). It was around this time that SLC established Cambridge Analytica which used "'data modeling and psychographic profiling [classifying people into personality types] to … connect with people in ways that move them to action'" (Doward, 2017). In order to provide Cambridge Analytica with the data it needed, psychologist and owner of Global Science Research, Aleksandr Kogan, designed a personality quiz app that went viral and tricked 320,000 into granting access to not only their own Facebook profiles, but also those of all their friends (Cadwalladr, I made Steve Bannon's…, 2018). While those involved with this scheme were likely not intentionally breaking the law, this data harvesting was definitely not authorized.

Targeted Messaging

Leave.EU's communications director, Andy Wigmore said "a Facebook 'like'… was their most 'potent weapon'" (Cadwalladr, Robert Mercer…, 2017). The artificial intelligence

used by CA-AIQ would receive inputs of mass amounts of "like's" (along with other data) and could then identify the "persuadable voters" and their cognitive vulnerabilities. For example, Cambridge Analytica would target overanxious and paranoid people with advertisements depicting immigrants swamping the UK (Cadwalladr, The great British Brexit…, 2017). The former Deputy Director of the University of Cambridge Psychometrics Centre, Michal Kosinski, found that "with knowledge of 150 likes, their model [of artificial intelligence] could predict someone's personality better than their spouse. With 300, it understood you better than yourself" (Cadwalladr, Robert Mercer…, 2017). This method of psychoanalysis is extremely effective. Not only does CA-AIQ recognize existing rifts and phenomena in society, but they encourage voters to self-identify with the cause through their aptly timed messages. This self-identification is key because it leads the voter to consciously acknowledge their agreement with the campaign, making them more likely to follow through and vote in that direction.

Figure 3. A sample of Facebook ads used by Vote Leave and BeLeave (another campaign that contracted AggregateIQ and connected with Vote Leave) that showcase the exploitation of voters' cognitive vulnerabilities. (Submitted to the UK Parliament Digital, Culture, Media and Sport Committee by Facebook as part of the Committee's inquiry into Fake News.)

The decision to exit the European Union was decided by a margin of just over 1.5 million votes, only 2.73% of the electorate (3.8% of voters). Given the data CA-AIQ had on tens of millions of voters, and the massive amount of targeted marketing and penetration into the public's consciousness they executed, its highly plausible that the Leave campaigns contracting of CA-AIQ led to their victory. It's also worth noting, that CA-AIQ were not the only sources distributing disinformation to ahead of the Brexit Referendum vote – along with monetary donations, 150,000 automated Twitter bots tied to Russia were disseminating messages about Brexit (Wintour, 2018).

It's important to remember that prior to its application in elections, these cognitive warfare techniques were contracted by militaries – they truly are war strategies. The tools contracted by militaries to control public opinions and behavior in some of the most volatile regions and conflicts in the world, are now being purchased by global elites to use on civilians to sway elections.

How to Defend

Dr. BJ Fogg, a Behavior Design expert at Stanford University, coined the term Captology in 1996. He was saw the potential of persuasive technology early on and predicted the ubiquity of technology that characterizes this era: "We are not just flesh and bones; we are now flesh and bones augmented with technology, and we will live the rest of our lives through technology connections, leveraging power" (Fogg, 2010). Persuasive technology is not disappearing and cognitive warfare is only increasing in pervasiveness and efficacy. In order to preserve individual autonomy and democracy, protective measures are vital.

General Public

Unfortunately, simply acknowledging errors and correcting the information does not erase the effects of disinformation and fake news. Once accepted, the disinformation is immediately integrated into schemas and used to maneuver the world and interpret new information. Subsequent falsification of information causes the breakdown of schema structure. It is then very difficult to re-interpret all information that was previously processed through that misinformed lens. While attitudes can change upon correction, the original information has lingering influences that prevent full rejection of the disinformation – the extent of these lingering influences varies based on the level of cognitive abilities of the individual (De keersmaecker, 2017).

Most of the time, disinformation presented to the public is never corrected or even detected. For this reason, the best defense the regular public has is awareness of the threat. Education on how fake news and disinformation campaigns design and target their messaging and how to identify a trustworthy source is the crux to remaining as objective as possible. The public needs to hold itself accountable and maintain a "critical distance" to the information. It is important not only to ask, "is this fake or not?", but also "why me? Why now? What are the consequences for this information to appear right now?" (S. Koch, personal communication, 10/04/2019). By constantly questioning the information presented and analyzing the context of it, the public is already able to greatly hinder its effect.

Governmental Responsibilities

While recognizing the importance of public education on the threat of disinformation, many are calling on the government to enact laws regulating internet usage and social networks. Facebook has been under fire for the past few years and has responded to these issues by

updating its privacy policies to obstruct the harvesting of personal data. Many people also have a problem with the algorithms used by many platforms that curate confirmative articles for the individual in their newsfeed. One idea is to legally require such platforms to alter their algorithms so that they also produce articles with opposing narratives – and, likewise, for news publications to offer varying perspectives (Wemer, 2019).

Global security expert, Dr. Alexandre Vautravers, compared the defense department mentalities of the United States and Russia. Noting the United States' affinity for acronyms and specific classification (evident in the US military's detailed separation of defense types), he claimed that the U.S.'s concern with specialization actually interferes with its ability to efficiently assemble information and achieve its goals (A. Vautravers, personal communication, 11/04/2019). He contrasted this with the Russian defense mentality which is much more unified in its denominations and thus is more cohesive in reaching its objectives. The interdisciplinary nature of cognitive warfare requires an integrated system of defense encompassing multiple branches of expertise.

Despite the best efforts of the public and national governments, the pace of technological innovation is so great that the current regulatory policies are antiquated and futile. In this era of hyperglobalization, "innovation is too transnational an enterprise, information too indifferent to borders, and civilization to interconnected for purely national solutions" (Patrick, 2019). Greater global collaboration is necessary in order to successfully regulate the technological and big data threats currently facing the world population.

Conclusion

The scariest part about cognitive warfare and sharp power tools is that the public is being exploited and steered towards predesigned behaviors without their knowledge. The very existence of freewill is now compromised and democracy is greatly threatened. The man largely responsible for bringing cognitive warfare to where it is today, Chris Wylie, realized too late that when there is no "respect for the agency of people, anything [done] after that point is not conducive to a democracy. And fundamentally, information warfare is not conducive to democracy" (Cadwalladr, I made Steve Bannon's…, 2018). Data is the nerve of war, and "whoever owns this data owns the future."

But, is the use of data and behavioral analytics to guide marketing decisions that bad? When phrased this innocently, it's questionable. One Cambridge Analytica spokesman believes:

> "'There's nothing magical or Pied Piper-ish about it. It doesn't give us special powers over people. We're all trying to better use the behavioural sciences to do our work in more effective ways" (Doward, 2017).

Is he right? Is it all fair business competition? Should Russia and China be vilified for exploiting democracies' openness or is it simply the name of the game and a side effect of the West's choice of government?

While this paper focuses on the dubious uses of big data and algorithms, they are not just for those seeking influence power. With the Information Era, the world has begun to transition to *algo-governance*. This is an entirely new way to govern in which rather than relying on ideas and convictions, authorities recognize that data and algorithms can generate the most effective policies (P. Hérard, personal communication, 04/04/2019). Given the stalemates often afflicting democracies, algo-governance does not immediately sound like a bad idea. However, Wylie points out that "the company [Cambridge Analytica] has created psychological profiles of 230

million Americans. And now they want to work with the Pentagon? It's like Nixon on steroids" (Cadwalladr, I made Steve Bannon's…, 2018).

Despite hesitancies and questions of morality, technology will continue to progress. By the time laws catch up to regulate big data usage, everything will have already changed – again, leaving the government to play catch-up. There will be greater understanding of neuroscience and psychology, and it's likely that much less data will be necessary in order to make the same conclusions. "Cambridge Analytica is already a prehistoric company, … a prehistoric example that just gives an idea of what will be the modern use of data in the future … [when] every moment of your day, of your life, is data" (S. Koch, personal communication, 10/04/2019). It's both incredibly unnerving and also thrilling to imagine what will come.

Abbreviation list

AIQ = AggregateIQ

CA = Cambridge Analytca

CA-AIQ = This paper's reference to Cambridge Analytca and AggregateIQ indiscriminately

CAPT = Computers As Persuasive Technology

EU = European Union

IRA = Internet Research Agency (Russian)

Psyops = Psychological Operations

UK = United Kingdom

US = United States

Bibliography

Secondary Sources

EU Referendum Results. *The Electoral Commission*. Retrieved from https://www.electoralcommission.org.uk/find-information-by-subject/elections-and-referendums/past-elections-and-referendums/eu-referendum/electorate-and-count-information.

Wintour, P. (2018). Russian bid to influence Brexit vote detailed in new US Senate report. *The Guardian*. Retrieved from https://www.theguardian.com/world/2018/jan/10/russian-influence-brexit-vote-detailed-us-senate-report.

Vote Leave / 50 Million Ads. *British House of Commons – Select Committee on Digital, Culture, Media and Sports.* Retrieved from https://www.parliament.uk/documents/commons-committees/culture-media-and-sport/Fake_news_evidence/Vote-Leave-50-Million-Ads.pdf.

Harmon-Jones, E. (2012). Cognitive Dissonance Theory. *The Encyclopedia of Human Behavior, vol. 1., 543-549.* Retrieved from http://www.socialemotiveneuroscience.org/pubs/ehj_dissonance_encyclopedia_human_minda.pdf.

De keersmaecker, J. (2017). 'Fake news': Incorrect, but hard to correct. The role of cognitive ability on the impact of false information on social impressions. *Intelligence, Volume 65*. Retrieved from https://doi.org/10.1016/j.intell.2017.10.005.

Mueller, S. (2019). Report On The Investigation Into Russian Interference In The 2016 Presidential Election – Volume I of II. *U.S. Department of Justice*. Retrieved from https://www.justice.gov/storage/report.pdf.

Kim, M. (2014) The Everyday Psychology of Nationalism. *The Atlantic – Health.* Retrieved from https://www.theatlantic.com/health/archive/2014/03/the-everyday-psychology-of-nationalism/284188/.

A short history of the web. *CERN – Accelerating Science.* Retrieved from https://home.cern/science/computing/birth-web/short-history-web.

Jacewicz, N. (2016). Why Trump and Clinton Voters Won't Switch: It's in Their Brains. *Scientific American – Neuroscience*. Retrieved from https://www.scientificamerican.com/article/why-trump-and-clinton-voters-won-t-switch-it-s-in-their-brains/.

Fields, R. (2016). A Neuroscience Perspective on Brexit. *Psychology Today*. Retrieved from https://www.psychologytoday.com/intl/blog/the-new-brain/201606/neuroscience-perspective-brexit.

Al-Rodhan, N. (2016). Us Versus Them. How Neurophilosophy Explains Our Divided Politics. *World Economic Forum*. Retrieved from https://www.weforum.org/agenda/2016/10/us-versus-them-how-neurophilosophy-explains-populism-racism-and-extremism.

Walker, C. (2018). What Is "Sharp Power"?. *Journal of Democracy, July 2018, Volume 29, Number 3*. Retrieved from https://www.ned.org/wp-content/uploads/2018/07/what-is-sharp-power-christopher-walker-journal-of-democracy-july-2018.pdf.

Walker, C. (2017). The Meaning of Sharp Power: How Authoritarian States Project Influence. *Foreign Affairs – the Council on Foreign Relations*. Retrieved from https://www.foreignaffairs.com/articles/china/2017-11-16/meaning-sharp-power.

Evanoff, K. (2018). Governing the Next Technological Revolution. *Council on Foreign Relations – The Internationalist*. Retrieved from https://www.cfr.org/blog/governing-next-technological-revolution.

Patrick, S. (2019). Transformative Technology, Transformative Governance: A New Blog Series on the Future. *Council on Foreign Relations – The Internationalist*. Retrieved from https://www.cfr.org/blog/transformative-technology-transformative-governance-new-blog-series-future.

Ferrier, M. (2018). Christopher Wylie: "The fashion industry was crucial to the election of Donald Trump". *The Guardian*. Retrieved from https://www.theguardian.com/fashion/2018/nov/29/christopher-wylie-the-fashion-industry-was-crucial-to-the-election-of-donald-trump.

Wemer, D. (2019). How to Fight Disinformation While Preserving Free Speech. *Atlantic Council*. Retrieved from https://www.atlanticcouncil.org/blogs/new-atlanticist/how-to-fight-disinformation-while-preserving-free-speech.

Cadwalladr, C. (2018). "I made Steve Bannon's psychological warfare tool": meet the data war whistleblower. *The Guardian – The Cambridge Analytica Files*. Retrieved from https://www.theguardian.com/news/2018/mar/17/data-war-whistleblower-christopher-wylie-faceook-nix-bannon-trump.

Cadwalladr, C. (2017). Robert Mercer: the big data billionaire waging war on mainstream media. *The Guardian.* Retrieved from https://www.theguardian.com/politics/2017/feb/26/robert-mercer-breitbart-war-on-media-steve-bannon-donald-trump-nigel-farage.

Cadwalladr, C. (2018). Revealed: the ties that bound Vote Leave's data firm to controversial Cambridge Analytica. *The Guardian*. Retrieved from https://www.theguardian.com/uk-news/2018/mar/24/aggregateiq-data-firm-link-raises-leave-group-questions.

Cadwalladr, C. (2017). Follow the data: does a legal document link Brexit campaigns to US billionaire?. *The Guardian*. Retrieved from

https://www.theguardian.com/technology/2017/may/14/robert-mercer-cambridge-analytica-leave-eu-referendum-brexit-campaigns

Doward, J. (2017). Did Cambridge Analytica influence the Brexit vote and the US election? *The* Guardian. Retrieved from https://www.theguardian.com/politics/2017/mar/04/nigel-oakes-cambridge-analytica-what-role-brexit-trump.

Hérard, P. (2017). Victoire du Brexit et de Trump : la démocratie sous influence des Big data ?. *TV5MONDE*. Retrieved from https://information.tv5monde.com/info/victoire-du-brexit-et-de-trump-la-democratie-sous-influence-des-big-data-176999.

Hérard, P. (2018). Plateformes numériques et économie de la donnée : comment nos cerveaux sont-ils influencés ?. *TV5MONDE*. Retrieved from https://information.tv5monde.com/info/plateformes-numeriques-et-economie-de-la-donnee-comment-nos-cerveaux-sont-ils-influences-236786.

Fogg, BJ. (2010). Article: Thoughts on Persuasive Technology. *Persuasive Tech Lab at Stanford University*. Retrieved from https://captology.stanford.edu/resources/thoughts-on-persuasive-technology.html.

Prier, J. (2017). Commanding the Trend: Social Media as Information Warfare. *Strategic Studies Quarterly*, *11*(4), 50-85. Retrieved from http://www.jstor.org/stable/26271634

Kanwisher, N. (1989). Cognitive Heuristics and American Security Policy. *The Journal of Conflict Resolution, 33*(4), 652-675. Retrieved from http://www.jstor.org/stable/173995

Waltzman, R. (2017). The Weaponization of Information: The Need for Cognitive Security. *RAND Corporation*. Retrieved from https://www.rand.org/pubs/testimonies/CT473.html

Kosal, M., & Huang, J. (2015). Security implications and governance of cognitive neuroscience: An ethnographic survey of researchers. *Politics and the Life Sciences*, *34*(1), 93-108. Retrieved from https://www.jstor.org/stable/26372748

Boyte, K. (2017). An Analysis of the Social-Media Technology, Tactics, and Narratives Used to Control Perception in the Propaganda War Over Ukraine. *Journal of Information Warfare,16*(1), 88-111. Retrieved from https://www.jstor.org/stable/26502878

Teague, G., & Bartholomees, J. (2014). *U.S. ARMY WAR COLLEGE GUIDE TO NATIONAL SECURITY POLICY AND STRATEGY* (pp. 261-270, Rep.). Strategic Studies Institute, US Army War College. Retrieved from http://www.jstor.org/stable/resrep12023.22

Mahairas, A., & Dvilyanski, M. (2018). Disinformation – Дезинформация (Dezinformatsiya). *The Cyber Defense Review,3*(3), 21-28. Retrieved from https://www-jstor-org.proxy.lib.umich.edu/stable/26554993

McGeehan, T. P. Countering Russian Disinformation. *The US Army War College Quarterly Parameters, Spring 2018*, 49-58. Retrieved from https://ssi.armywarcollege.edu/pubs/parameters/issues/Spring_2018/8_McGeehan_CounteringRussianDisinformation.pdf

(2013). Muzaffarnagar: Tales of Death and Despair in India's Riot-Hit Town. *BBC News, 25 September 2013*. Retrieved from https://www.bbc.com/news/world-asia-india-24172537.

Golman, R., Loewenstein, G., Moene, K., & Zarri, L. (2016). The Preference for Belief Consonance. *The Journal of Economic Perspectives, 30*(3), 165-187. Retrieved from http://www.jstor.org.proxy.lib.umich.edu/stable/43855706

Primary Sources

(S. Motte, personal communication, 01/03/20190)

(P. Hérard, personal communication, 04/04/2019)

(S. Koch, personal communication, 10/04/2019)

(A. Vautravers, personal communication, 11/04/2019)