Univerzita Karlova
Fakulta sociálních věd
Institut politologických studií
Diploma thesis project

ANT-Security Interface and the Current Information Crisis

Name: Alexander Downs
Academic advisor: Filip Vostal
Study programme: Master's in international security studies (MISS)
Year of project submission: 2020

Table of Contents

Acknowledgments

I became interested in counter-factual information as a security issue, in part, as a response to my own experience with it. I am, what some might consider, a recovering conspiracy theorist. A decade ago, I ventured down the proverbial rabbit hole of extremism. In retrospect, I embraced that ideology not because I wanted to be correct in my world view, but because I wanted everyone else to be wrong in theirs.

Fortunately, there are those who helped facilitate my transition from the person I was to what the alt-right would regard as, "a sheep". And I am grateful to be that sheep. They have my gratitude.

Tom Nichols; of the U.S. Naval War College, Harvard University Extension School, and formerly Harvard Kennedy School. He is responsible for fostering my interest in international security studies and informing me that Ron Paul is crazy.

Vít Střítecký, Deputy Head of the Department of International Security Studies at Charles University. He is significant for introducing me to concepts which underpin the study of security and technology, and that cyberspace was a domain into which the traditional tenants of security now extend.

Filip Vostal of both the Academy of Sciences of the Czech Republic and Charles University. Vostal has contributed as an enabler of my choice to embrace of interdisciplinary approaches to security studies which he has rightly characterized as intellectual promiscuity. His contributions toward this project have been invaluable. As advisor on this thesis project he has my thanks for his insights and patience.

The students with whom over the last 5 years I have been fortunate to teach International Relations and Sociology. Learning through their curiosity, criticism, optimism, and sometimes pessimism toward our world, has been profound experience

Finally, my family. Robert, Cynthia, and Jonathan Downs. Virginia, and Herbert Haynes. They gave their unconditional support to this endeavor, and to all my endeavors, even if they didn't always understand what I was doing, or why.

Abstract

We live in a world driven by fast technologies. The same technologies that make information more accessible have created a dilemma by which the same conduits have also enabled access to mass amounts of counter-factual information. It is the assertion of this thesis project that counter-factual information poses a growing risk to the security and stability in liberal democratic societies and warrants a proportional response. The body of work which follows will explore what I have characterized as an information crisis.

The information crisis, so presented, is a multi-faceted issue. It's constituent causes and outcomes concern both scholars of security studies and sociology. To address breadth of scope and immediacy of the crisis, the conceptual framework purposed in this project offers an interface between actor-network theory and security studies (ANT-security interface). Actor-network theory is a material-semiotic approach that preferences engagement with human and technological actants as an assemblage. Or, in other words, a network of relationships.

The first chapter will introduce the dimensions of the information crisis, providing relevant examples of how counter-factual information embodies a human, and societal security issue. It will delineate important concepts such as misinformation, and disinformation, and position them as the focal point of a research dilemma due to the scope and speed at which they have been enabled.

The second chapter will discuss the relevant reference objects within the information crisis and why they belong in the purview of both security studies and scientific and technological studies (STS). It will then introduce the conceptual framework of an ANT-security interface.

The third chapter will provide a practical example of the information crisis as an assemblage through the mainstreaming of far right, or alt-right revisionism, as facilitated by technologies in cyberspace. It will accomplish this through demonstrating the relationships between ideology, rhetoric, and the technologies which enable manipulation of information availability, amplification of misinformation, and the manufacture of disinformation.

By its conclusion, this thesis project demonstrates a conceptual framework capable of mitigating the scope and speed of the information crisis and provides a brief set of policy recommendations to be undertaken as both responsive countermeasures and as longer-term goals.

1. Dimensions of an Information Crisis

Following the 2016 election cycle in the United States, a non-profit cyber monitoring firm called PropOrNot published a report reflecting their investigation of some 200 websites. The sites in question reached 15 million Americans. The content presented by the sites garnered over 213 million views via social networking platforms (Timberg 2016, np). "Social media sites have surpassed print newspapers as a news source for Americans: One-in-five U.S. adults say they often get news via social media, slightly higher than the share who often do so from print newspapers (16%) for the first time since Pew Research Center began asking these questions" (Shearer 2018, np). The content which concerned PropOrNot's investigation were distinctive, because they did not originate in the United States, but rather in Russia (Timberg 2016, np). A large portion of Americans were exposed to information that may not have reflected what was true for them, but rather what somebody else wanted them to think.

The investigation which follows is the culmination of an interesting and concerning journey. Interesting due its current relevance. Concerning due to the ominous effects which the consumption of flawed or untrue information may have on our communities and the institutions which govern them. To illustrate another such example, on June 28th Washington Post columnist Margaret Sullivan emphasized a disturbing correlation. Population samples in the United States who obtained their daily information primarily from Fox News have been remarkable for accelerated transmission of the SARS-CoV-2 virus. Sullivan suggests that Fox' obfuscation of emerging information pertaining to the seriousness of the virus, particularly during the key window for containment in early March 2020, has allowed it to flourish in ways that might otherwise have been preventable. The phenomenon, she proposes, has not only exacerbated a public health crisis but has also contributed to political and ideological one at the highest levels of government. She writes,

"beyond the risks the general public faces from consuming this nonsense and misinformation, there's the fact that the president himself has been picking up these same ideas and using them to steer policy. Instead of tapping experts in the medical and scientific community — many of whom are on the government payroll — he has chosen to educate himself by watching right-wing news outlets" (Sullivan 2020, np).

The correlation between the information we consume and virus transmission, which Sullivan advocates, is based in part on an April 2020 study published in Harvard Kennedy School's *Misinformation Review.* The survey study revealed that while familiarity with the virus was high (ninety-six percent knew about the virus), there were at least three levels of variance with respect to how respondents regarded the virus. The first revealed variance in the levels of factual vs. obfuscated information the respondents had encountered. The study revealed low levels of information about lethality and prevention, coupled with high levels of misinformation. Secondly, along party lines, Democrats and Republicans differed when surveyed about the perceived lethality of the virus. The third variance accounted for associations between media exposure and information/misinformation accounting for both ideology and political party. (Jamieson 2020, 4-5). The Harvard study posits that consumption of information through the medium of social networks and "conservative media use (e.g., Fox News) correlated with conspiracy theories including believing that some in the CDC were exaggerating the seriousness of the virus to undermine the presidency of Donald Trump" (Jamieson 2020, 1). Based on the conclusions of the Harvard study, it is evident that both the source of information, as well as confirmation bias with respect to party and ideology, has had significant bearing on how survey respondents have reacted to the SARS-CoV-2 virus.

The term cognitive dissonance, attributed to social psychologist Leon Festinger, alludes to the uneasiness we feel when two ideas (or behaviors) appear to contradict one another. Festinger's work made significant inroads toward explaining why people, both individually and on a group level, find it so difficult to change their minds or admit fault. "The minute we make a decision – I'll buy this car; I will vote for this candidate; I think COVID-19 is serious; no, I'm sure it is a hoax – we begin to justify the wisdom of our choice and find reasons to dismiss the alternative. Before long, any ambivalence we might have felt at the

time of the original decision will have morphed into certainty" (Aronson & Tavris 2020). If we extrapolate this model to account for the influence of today's information cycle on our behavior and decisions, and then consider the myriad sources of counter-factual information at our fingertips, we observe the makings of what I will henceforth refer to as an information crisis.

Information has always been, and continues to be, a key factor to the health of a society. In choosing to use the phrase "health of a society", that is to refer both to the literal sense of the word health; as the public health crisis in the United States is currently being exacerbated by misinformation, but also in the functionalist sense. The health of society can also be characterized in the answers to such question as: Are we able to make informed decisions about elected leadership, and the form or function of both civic and international institutions? Are we able to accurately appraise the sources of our societal issues and the means through which we can ameliorate them? We are currently witnessing an increase in the proliferation and consumption of counter-factual information, however. The consequence is a decline in the overall health of our societies in a functional sense, and in doing so hastening the need address the crisis from both an academic and practical standpoint. If we want to explain the world around us, we need the research tools with the capacity to explain what's going on, and in the case of the current crisis, we need them sooner rather than later.

The body of work that follows, contributing to the completion of a master's degree in international security studies, responds to the unique circumstances surrounding the contemporary spread of counter-factual information as both a security issue, and a social one. The investigation will approach the predicament with four central assumptions. (1) A crisis indeed exists, and we must be concerned with its impact on electoral democracies. (2) The crisis stems from access to misinformation, disinformation, and is distinctive due to its connection with cyberspace as a facilitator. (3) The role of technology creates a unique research dilemma but also an opportunity for interfacing between security studies and science and technological studies (which is typically abbreviated STS). (4) This interface must be used to inform future policymaking and other practical solutions to the crisis.

1.1 A Crisis Exists

If we take the term crisis to mean a point at which events have reached a critical and decisive phase, the simple answer is yes, we have a crisis. The results of the *Harvard Misinformation Review* speak for itself. There is demonstrable evidence that sympathy for counter-factual information, when coupled with cynicism toward established knowledge, has helped accelerate a multi-dimensional public health risk that will also have far reaching economic and political ramifications. And this is only one manifestation. In his book *The Death of Expertise: The Campaign Against Established Knowledge*, Tom Nichols observes "anti-intellectualism is itself a means of short-circuiting democracy, because a stable democracy in any culture relies on the public actually understanding the implications of its own choices" (Nichols 2017). The information crisis at hand indeed has a unique impact upon societies rooted in modern liberal-democratic values. The cases selected to illustrate the crisis will pertain to the United States, where its effects have been acutely demonstrable, but may also apply in the UK, the nations of the European Union, and other electoral democracies. What makes electoral democracies particularly vulnerable to information crises is the close relationship between public opinion and policymaking. Holding sway over the former, may in short order, have direct consequences for the latter.

In struggling democracies or authoritarian societies, the relationship between information and policymaking differs in part because the linkage between public opinion and governance may be tenuous. That is not to say the veracity of information is unimportant outside democracies. As we observed from the Arab Spring uprisings of 2010-11, the sharing of information via social networks helped facilitate collective action that in the cases of Egypt and Tunisia, resulted in regime change. Rather, information in established democracies is crucial due to the *expectation* of its role in policymaking. Consent of the governed, the rule of law, and rights of minority populations; all these potential limits to power require transparency. Access to, and exchange of information is a key facilitator in this process. In democracies, it embodies the rule, rather than the exception to the rule. The relationship between information, the public, and policymaking can also be a paradoxical one though. While democracies require an informed electorate to function as intended, one of their hallmark traits; the freedom of speech and expression, also serves to

safeguard environments where misinformation and disinformation may circulate unimpeded.

1.2 Misinformation, Disinformation, and Technology

This leads to the second central assumption, pertaining to misinformation, disinformation, and technology (specifically cyberspace) as the principle facilitator. The distinction between misinformation and disinformation is important, as both are forms of counter-factual information which have helped instigate the current information crisis, and both will be discussed at length. Beginning from a position of self-reflection, we as people are instinctive receivers of information and are inclined to accept it. "Traditional models of information [behavior] seem to suggest a normative conception of information as consistently accurate, true, complete, and current," causing us to neglect "whether information might be misinformation (inaccurate information) or disinformation (deceptive information)" (Karlova & Fisher 2013, np). While misinformation may be characterized as "concealment, ambivalence, distortion, and falsification," it may also be information that is incomplete. Because we have a normative disposition to accept what we have been conditioned to regard as informative, misinformation may also appear to be current, true, or even accurate, meeting all our instinctive prerequisites for what we accept as fact (Karlova 2013 citing Zhou & Zhang 2007, np).

The hallmark of disinformation is its deceptiveness. Since the motivation for deception cannot be readily distinguished, disinformation offers an additional layer of uncertainly. Motivations for spreading disinformation may be "benevolent, such as lying about a surprise party, adhering to cultural values, demonstrating community membership, etc." But they may also be malicious, such as "manipulating a competitor's stock price, controlling a populace, ruining someone's reputation" (Karlova 2013, np). Thus, disinformation shares characteristics with both information, and misinformation. It may embody accurate, true, complete, or current data, spread anonymously for ulterior motives or purposes of subterfuge. To that point, misinformation is distinct because its source is clearly discernable while disinformation may be more likely when the source is not (Clark & Bryant 2020, np). While this may be an oversimplification, it provides adequate contrast between the Fox News host galvanizing support for President Trump through politicizing

the SARS-CoV-2 virus, and the Russian troll, or bot-driven account, amplifying similar misinformation under the auspices of being an average American voter. In either case, models of our behavior suggest that we have a penchant for regarding the information we consume with a relatively undiagnostic approach.

The information crisis as a security issue is a product of increasing and unprecedented access to misinformation, and disinformation, as they pertain to democratic institutions, and our socio-political processes. Decidedly, they both share conceptual space with propaganda, a human practice as old as our desire to persuade or influence our peers' thinking. The reason why now is the time for more rigorous examinations of our relationship with counter-factual information is due to its scope and means of delivery. Ideological competition has always been around but never applied on such a scale and with current levels of sophistication (Nestoras 2019, 2). The current information war, being fought largely across cyberspace, is distinctive due to factors that include but are not limited to speed, potential for anonymity, and unprecedented access to recipients who are predisposed to hold counter-factual information in the same esteem as fact. While the phenomenon has long been a grudgingly accepted biproduct of adversarial politics, its distribution potential and tangible results have increased measurably by exploiting the possibilities unlocked by 24-hour news cycles, abundant internet access, and participation in social networks. The current discord and politicization of the SARS-CoV-2 virus in the United States may be regarded as the predictable, though irrational conclusion to a decade under the influence of a maelstrom.

1.3 Research Dilemmas and the Case for Intellectual Promiscuity

The third central assumption of the investigation concerns the need for increased scholarly attention from experts in the social sciences. This is as much a focus for inquiry as it is an implicit recommendation from the body of work in general. A significant portion of the thesis is dedicated to promoting an interface between security studies and science and technological studies (henceforth STS). There has been a paucity of collaboration between the two fields in most meaningful ways, despite sharing a vested interest in the outcomes (or tangible results) of the information crisis and sharing an increasing number of mutual

reference objects. Reference objects are agents, artifacts, or trends which lend relevance to an inquiry or field of research. As phenomena in our world have become more interconnected, genres of research have necessarily expanded their purview to include additional reference objects. If one were a nineteenth century scholar of military logistics, the advent of the railroad would of course demand consideration of the train as a new and relevant reference object. The newfound ability to collapse space and time which the train facilitated would require new modes of thinking on the part of experts. The same thing is transpiring in the fields of security studies and STS. The information crisis presented here represents an area where emerging reference objects concerning both fields coalesce.

There are several dilemmas facing experts concerned with the information crisis as both a security, and social issue; not least of which are scope, and speed. When considering the information crisis as a dilemma of scope it is worthy to mention that a studies of disinformation as a product of foreign information operations, misinformation as a product and tactic of adversarial politics, or social networks as an emerging sociological phenomenon, all embody interesting and necessary avenues of research. They are germane to both security studies and STS as they illuminate actors and relationships which impact systems and institutions whose stability and function are significant. Our current information crisis, as facilitated through cyberspace, is an entirely holistic dilemma, however. Its inception owing to an assemblage that includes elements from each of the previously mentioned possible studies. An assemblage is a "patterned array of connections and composed of all manner of heterogeneous elements." (Michael 2017, 154).

If we were to approach our information crisis in a traditional sense (from either a security studies or broader classical sociology background), we run the risk over over-territorializing. Or in other words privileging reference objects that are most typically associated with ones' area of expertise and in doing so, conceiving any number of correlative-based fallacies. If we were to follow just one key element of the current information crisis, such as the impact of Russian information operations on electoral processes in Europe and the United States, we would privilege a certain array of elements (such as the transference of Russian *realpolitik* views on foreign policy to the domain of cyberspace), and thus arrive at solutions that also overwhelmingly privilege security-based

thinking. By advocating for a more academically promiscuous, or "de-territorial" approach I will suggest potential solutions and countermeasures that reflect the information crisis as the more holistic and protean issue that it is.

A second research dilemma, the problem of speed, is thoroughly discussed by Filip Vostal of Charles University in *Accelerating Academia*. Vostal, who additionally contributed as advisor on this thesis project, observes that the collapse of time and space – as facilitated by the railroad in the previous example – that might have beleaguered military logisticians of the nineteenth century is having a similar effect of the social scientists of today. "Large chunks of social life have been migrating to the online world whose crucial modality is the one of immediacy." He continues, citing Gane, "Social relations, economic exchanges and even global events are now mediated by technologies that can operate at the speed of light from the digital circulation of big capitalist finance through to the 'real-time' reporting of global news and even the individual organization of personal relationships via mobile phones or email. Indeed, it is hard to think of an aspect of human existence that has yet to be touched by the fast technologies" (Vostal 2014, 174) (Gane 2006, 20).

These same fast technologies which are also facilitating our information crisis are proving a confounding variable for social scientists. Scholars in both security studies and STS are presently struggling with conceptual frameworks and infrastructure to address the very post-modern dilemmas of scope and speed. The impact of counter-factual information consumed *en masse*, as facilitated by fast technologies, is taking place in real-time. As it impacts our day to day behaviors, our voting tendencies, and thus our leadership, policymaking, and ultimately institutions, social sciences are left in coughing in the dust and struggling to catch up. We are left with the dilemma of publishing our research after the proverbial damage has already been done. Perhaps unsurprisingly, Silicon Valley and the advent of big data have turned information into profit, nearly in real-time. In doing so it has created another potential element for our consideration, which will be elaborated upon further in the first case study. Techniques which have paved the way for data-collection and generation in the realm of big data are also better equipped with "the now," and may be useful in replicating similar research as the *Harvard Misinformation Review* study (Vostal 2016, 174).

1.4 Proposing a New Framework

The fourth and final central assumption builds upon the third. One potential avenue for increased collaboration between security studies and STS lies in what I will characterize as an ANT-security interface. ANT, short form for actor-network theory, suggests viewing the interactions between humans and technologies as an assemblage, or web of relationships, as opposed to a hierarchical (or over-territorialized) analysis of correlations extended between actors and objects. By considering this alternative means with which to conceptualize our current information crisis, the investigation will advocate for more all-inclusive policy recommendations that privileges neither security-based thinking, nor social theory. This investigation proposes consideration of ANT as a conceptual framework for security studies scholars, as well as to inform future policymaking and practical solutions to the information crisis. ANT, as a conceptual framework, is related to the larger realm of material-semiotics, which is dedicated to making heterogeneous associations between an array of actors and arrangements. These could be human, non-human, organizational, or technological, (Michael 2017, 160).

It has thus far been established that an information crisis exists. It is the logical but problematic amalgam of several key input factors and has produced a problematic outcome. Of these input factors, we must consider that information in general has a normative effect on people. This is true irrespective of whether the information is factual or contains characteristics of misinformation and / or disinformation. People are thus susceptible to its effects. The discernable effect can be observed in the form of survey studies, as the *Harvard Misinformation Review* has demonstrated, and a number of those methodologies use to track cyber-behavior which subsequent case studies will further elaborate upon. The discernable effect in aggregate is detrimental, in a functional sense, to the health of electoral democracies and the institutions which they rely upon for stability. While our relationship with information may be innately part of our makeup as humans, cyberspace as a facilitator for disinformation has augmented the potentially harmful effects of the information crisis, thus establishing a new array for challenges for scholars. As it embodies a multi-faceted challenge, this thesis advocates an interdisciplinary approach to the crisis with an emphasis

on framing the phenomenon as an assemblage and embracing an ANT-security interface in the search for actionable countermeasures.

In the following chapter, I will elaborate upon both security studies and actor-network theory. The chapter will consider how security studies grown intersubjectively to include a growing array of reference objects, and how those reference objects rightly apply to our current information crisis. It will then give some epistemological background with respect to actor-network theory, placing emphasis on material semiotics as a parent-concept, and performativity; "the ways in which practices produce particular realities" (Michael 2017, 162). The third chapter will operationalize the ANT-security interface broadly speaking by considering the growth and spread alt-right revisionism in cyberspace. The fourth chapter will further illustrate the concept of performativity with a case study about the role of big data, and big data brokers such as Cambridge Analytica, in the current information crisis. The thesis will conclude by recounting how both inherent case studies exemplify the emergent information crisis as well as a potential interdisciplinary approach to managing the crisis.

2. ANT-Security Interface: Theoretical and Epistemological Background

Science fiction writer Alastair Reynolds blithely summarized the spirit of this investigation. "Everything depends on everything else, doesn't it? That's interconnectivity for you – it's a bitch." His sentiment also underpins most central dilemmas which challenge scholars and policymakers at present time, as well as the principle elements concerned in this investigation. As it was briefly discussed in the previous chapter, this study adopts a multi-disciplinary approach to what it has characterized as an information crisis. A crisis indeed exists. Its causal origins insofar as human behavior is concerns comes from normative access to misinformation, disinformation, and is distinctive due to its connection with cyberspace as a facilitator. The role of technology creates a unique research dilemma but also an opportunity for an ANT-security interface which this chapter will discuss in greater detail. The purpose of this interface is to inform practical solutions to the crisis and provide conceptual flexibility to concerned scholars. Interconnectivity is

a crucial trait in how we characterize the information crisis, which this investigation will do at greater length in the third and fourth chapters. Interconnectivity is also inherent in the theoretic and conceptual framework that will be addressed in this section.

The past twenty years embody a period of accelerated change with respect to the pace at which we consume data. This holds true for the pace at which we process geopolitical concerns. Threat analysis and even the concept of security itself now necessitates the inclusion of a new reference objects. It also holds true for the social sphere, as the very means through which people (individually and on a group level) conceptualize their realities are in a state of unprecedented flux. In Vostal's *Accelerating Academia,* he notes (citing Rosa) "how certain temporal assumptions about the acceleration of social change and its ramifications may lead to articulation and development of new imaginaries, analytical apparatuses and conceptual languages intended to assist sociology in capturing social reality" (Vostal 2014, 170). This sentiment very much embodies the thought process by which my investigation came to regard a conceptual framework from the realm of STS as relevant to an emerging security issue.

To goal of this chapter is to characterize the development of an analytical apparatus that I will refer to as ANT-security interface. In doing so it is necessary to revisit the fundamental pillars of security studies and STS. Necessitated in part by the acceleration of change, each discipline has expanded to include a growing number of phenomena that appear relevant to each respective purview. The first section will focus on security studies. Demonstrating when applicable, how the answers to certain fundamental questions about security studies (as referenced by Buzan and Hansen in *The Evolution of International Security Studies)* dictate the inclusion of cyberspace as a domain, and concepts such as socio-economic or socio-political security, in the wider security studies apparatus. The second section will briefly revisit STS as the parent discipline whose critical turn fostered the emergence of ANT. It will also mention the brief, though meaningful moments of collaboration between security studies and STS, ultimately concluding that we must consent to flexibility. Merging relevant approaches from each field is a necessary consequence of a problem with the scope and speed of the information crisis. The final section will introduce the novel concept of an ANT-security interface.

2.1 The Evolving Concept of Security

The reason for beginning with a security studies perspective is simple. Security as a concept and security as established by interactions between reference objects is integral to this thesis. Furthermore, the information crisis is a security issue. Security as a concept embodies a wide range of possible definitions extending from simple mantras to philosophical and theoretical reflections. Insecurity as a concept may also lend itself to coloring our perceptions of security as space where "security is not." Associated applications of "security as logic" may extend to practices like coercion or deterrence. As an academic discipline, as well as in practice, security is continually transformed through processes of widening (through theoretical examinations pitting objectivity against intersubjectivity) and deepening (through assigning new reference objects to our understanding of negative versus positive security) (Karasek, Lecture, 2019).

As we widen our concept of security, new areas for concern and further protected values emerge. These range from the more traditional areas for concern, embodied by *realpolitik* and geopolitics, to include the more intersubjective societal, economic, and even environmental concerns. Through the lens of the former, more traditional approaches, security is regarded more so as defense and stability, or perhaps absence of instability. The latter, regarding security as interdependence, or institutionalization. More recently this scope has extended to human security and cyber security, demanding increasing intersubjectivity as we account for the social construction of security as a concept. As the areas encompassed by security concerns expand, we must consequently deepen the repertoire of refence objects associated with these areas. Widening of security to account for interdependence and institutionalization is relevant to this investigation because, as it has been previously stated, it is the form and sound function of our institutions that are under threat from a growing wave counter-factualism, resulting in cynicism against established knowledge.

The relevant validity and scope of security studies has been a topic of debate regarding what we consider to be reference objects. When we discuss reference objects in the field of security studies, they represent entities or phenomenon whose presence and between

whose relationships lend themselves to security as a concept. In the most traditional approaches to security studies, for instance, the state has been a primary reference object. The state as a principle reference object prioritizes the state as an actor in security related issues, thus making interstate (or international) security and relations, a primary focus of scholarship. In other words, if your main reference object for concern is the state, security-based thinking that privileges the state is likely to prevail. This is simply one mode of thinking encompassed by security studies, however. While our understanding of security is inextricably linked to the reference objects around which we are conceptualizing security, the array of relevant reference objects is expanding. Buzan and Hansen delineate four key questions in *The Evolution of International Security Studies.* These questions masterfully outline the central debates which have grown with, and out of, security studies. Their four key questions have also been crucial to the conceptual framework of this thesis, as we may justify a more protean approach to our current disinformation dilemma by accounting for recent changes in our perception and understanding of security studies.

The first question of Buzan and Hansen's fundamental questions pertains to whether security studies ought to prioritize or privilege the state as a primary reference object. "Security is about constituting something that needs to be secured: the nation, the state, the individual, the ethnic group, the environment…. Securing the state was seen instrumentally as the best way of protecting other referent objects" (Buzan and Hansen 2009, 10-11). Whether or not securing the state (or nation) is the most practical means for securing constituent reference objects, conceiving of *what* exactly requires security on a conceptual level is of primary importance from a policymaking perspective. If our information crisis constitutes an issue relevant to security studies, it will be helpful to formally establish to whom or to what is under threat. As it has been suggested, the social and institutional stability that underpins institutions in most liberal democracies now requires security on a conceptual level.

The second question posed by Buzan and Hansen leads us to consider whether security studies ought to account for both internal and external threats as key reference objects. The authors note that both (international) security studies and international relations "face mounting challenges from globalization to blur, or even collapse completely, the

inside/outside distinction" (Buzan and Hansen 2009, 11). There is some merit to these challenges. While there is certainly some ground for delineating between internal concerns such as economic problems and ideologically divergent "outside powers," this study will concern itself with how the internal and external are coalescing with respect to counter-factual information as a security issue. Our current crisis may be characterized as security challenge in both domestic and international spheres. Information operations as a malicious tool of rival foreign powers can be regarded as a matter of international security. These can manifest, for instance, as targeted disinformation campaigns. Security apparatuses in the United States and the European Union still struggle to fully reconcile with it as a new tool of great power politics, however. While they may constitute an outside threat in terms of origin, social networks and the inherent topography of cyberspace allows an outside threat to percolate and circulate within the domestic sphere. By considering the information crisis as its own assemblage, this investigation will advocate abandoning the old inside/outside tropes with respect to disinformation campaigns / information operations in favor of regarding them as a singular security concern.

Buzan and Hansen's third question for security studies pertains to whether we must extend security beyond the military sector and the use of force as a primary coercive tool (Buzan and Hansen 2009, 11). In most respects this question has already been answered. The present-day sectoral widening of security to account for the social, economic, environmental, and developmental spheres of security are all well established. We know from conflict studies and stable and wealthy societies are less likely to resort to interstate warfare. Thus, social and economic security are useful tools of conflict prevention. In absence of open conflict, military instruments become a secondary or even tertiary means for enforcing security. The scope of security studies has expanded to regard more intersubjective security concepts as essential, as opposed to being components of the idea of "force as security." This is an important development for security studies as it increasingly regards the effects and relevant reference objects of cyber and human security. During this investigation, the concept of cyber security vis-à-vis information operations and security as the health of a cohesive society crucial, as they are two spheres most immediately effected by the spread of counter-factual information.

The fourth and final question addressed by Buzan and Hansen pertains to "whether or not we should see security as inextricably tied to a dynamic of threats, dangers and urgency" (Buzan and Hansen 2009, 12). The traditional realist school related to security dilemmas almost exclusively as that which stemmed from "attacks, subjection, domination and – when pushed to the extreme – annihilation" (Herz, as cited by Buzan and Hansen 2009, 12). Structural violence, as it pertains to security and military-based thinking, embodies only a portion of present-day threat assessments analysis. Hybrid warfare, accounting for traditional use of force, as well as cyber warfare, and other subversive activities, signify an expansion of security studies' practical academic purview. We no longer consider the concept of "the attack" to the most immediate security concern. Threats can come in the form of economic warfare, malicious applications of economic statecraft, or other attempts to destabilize a given nation or society from the outside, or from within. Some of these threats are instigated with a long-term view and may develop more slowly.

In sum, we can conclude that based on Buzan and Hansen's guiding questions, security studies are a discipline well suited to investigate the nuances of our current information crisis and develop potential policy-based solutions that might provide countermeasures. Any cursory examination of how security studies has developed as a discipline over the last half-century reveals that it has adapted to accommodate the changing times, and with them the variables concerned. For this study, we can prioritize the following conclusions from Buzan and Hansen: (1) The sovereign state no longer holds a monopoly as the prime reference object for security studies. That which "requires security" now accounts for interdependency, social stability, and the wave of institution-building that has characterized the last century. (2) Our world is more interconnected than ever before and thus the distinction between internal and external threats has become increasingly tenuous. (3) The idea of security is intersubjective. Just as the state is no longer the prime reference object, the idea of "force as security," has also grown obsolete. Threats now hail from emerging domains such as cyberspace and require the requisite attention. (4) Structural violence and the threat of attack in the traditional sense is also outmoded. Information, and information operations now constitute a threat to our institutions and social stability.

During the past twenty years cyber security has gone from being a somewhat niche discipline to an indispensable facet of any security studies curriculum. As our appraisal of threat has evolved, cyber space demands the attention of experts in fields of government, the private sector, and beyond. Historically, when force-centric threat assessment was prevalent, traditional domains for consideration were regarded as the land, sea, and air. With the advent of intercontinental ballistic missiles, militarization of the high atmosphere, and the space race as defined by the Cold Wars, a fourth domain was added. Today, space has been joined by cyberspace as a fifth domain over which security-based thinking is conducted. And yet, cyberspace is fundamentally different from the other four domains. It is the only defense-based domain to occur outside of our three-dimensional world. Cyberspace is also accessible to a large proportion of people, regardless of their alignment or relationship to refence objects such as the state.

For the sake of demonstrating some of the fundamental contrasts between cyberspace and the other four domains, let us consider a typical tool of engagement such as a missile. A missile is constructed with the specific purpose of travelling at great speeds, unimpeded, and destroying or disabling whatever lies in the physical space at its intended destination. The missile exists ostensibly in the domain of air related defense-based activities. Missiles may be used in conjunction with, or against, various other artifacts within the spectrum of land, sea, air, and space domains. However, regardless of its application, it is generally regarded as a tool for mitigating imminent threats and deals with tangible objectives. Cyberspace, by contrast, is not necessarily a domain tied to dynamics of threats, danger and urgency.

Cyber driven activities can be utilized in a tangible military sense, such as the alleged deployment of a malicious computer worm called Stuxnet against Iran's nascent nuclear program in 2010. Cyberspace is also a domain in which operations concerning the economy, banking, military and civic infrastructure, communications, and socio-political discourse may be carried out. Over the past decade, information operations have been utilized by several state and non-state actors. The success of these operations is a key point of inception with respect to our current information crisis and should be regarded as a worthy area of focus under the purview of security studies. Furthermore, ideology, the

normative place of adversarial politics, as well as the sensational nature of a non-stop information cycle, predicates our relationship with information in cyberspace. The phenomenon which I have outlined as a security concern, trends increasingly deeper into the social sphere, raising new concerns about our relationships with technology as a facilitator for information consumption. Security studies, as an adaptable discipline, can frame the information crisis as a security issue. The problem is security studies is not the most flexible tool for reckoning with the crisis in the "present-tense." Thus, this investigation suggests that scholars of security studies consider technoscience and sociology of technology for greater inclusion in the present discussion about security and technology. To that end, the following subsection will explore the role of ANT, and its potential contributions to a greater understanding of the information crisis.

2.2 STS-Security Interface

Science and technology studies, traditional abbreviated as STS, is a dynamic and interdisciplinary field of scholarship dedicated to exploring the influence of society, culture, and political instruments on developments in science and technology. Furthermore, it wishes to demonstrate how science and technology, in turn, facilitate changes in social or political world. Some literature has explored the relationships and interplay of roles between science and technology. "The discipline of STS works through case studies. Some describe the social shaping of technologies. For example, how did the bicycle come to take the form that it now does? The answer is that it was shaped by economic and social interests, the cultural skills available, and, of course, by the laws of momentum" (Law 2008, 2). The case studies which Law refers to are purposed with realizing the web of relationships between actors and artifacts, demonstrating that they are essentially interconnected phenomena. An assemblage.

For my purposes, the subset of STS dedicated to the sociology of technology is of principle importance. Pinch and Bijker note that "the sociology of technology is still underdeveloped, in comparison with the sociology of scientific knowledge. It would be a shame if the advances made in the latter field could not be used to throw light on the study of technology" (Pinch and Bijker 1987, 40). Whereas science is very much regarded as a

process, technology in the main, is often relegated to simply being the logical consequence or application of science. This leads to several principle issues. First, it results in asymmetric analysis, and attention largely being dedicated toward successes, and the benevolent applications of technology, as opposed to its failures or malicious applications. I am most concerned in this thesis, with the malicious application. Secondly, it leads to modes of thinking which flirt with technological determinism. Overly deterministic narratives make for interesting storytelling but very unconvincing scholarship, yet we are tempted to view technology through such a lens. "An implicit adoption of a linear structure of technological development, which suggests that the whole history of technological development had followed an orderly or rational path, as though today's world was the precise goal toward which all decisions, made since the beginning of history, were consciously directed. (Ferguson 1974b, 19 as cited by Pinch and Bijker). This preference for successful innovations seems to lead scholars to assume that the success of an artifact is an explanation of its subsequent development" (Pinch and Bijker 1987, 16).

Using Pinch and Bijker as a starting point, asymmetric analysis and technological determinism each have an implication for the information crisis. Regarding asymmetry, we must consider the unforeseen failures and malicious applications of cyberspace and artificial intelligence (AI)-driven technologies as they have directly impacted our socio-political processes. Regarding determinism, the influence of technology as a facilitator for our current disinformation crisis is has been anything but orderly, rational, or inevitable. While many seem to regard the malicious applications of technology as having been somehow inevitable, human agency necessarily predicates malicious use. Technologies as referential objects cannot be inherently malicious without being so purposed. It is for these reasons that STS, in general, and the sociology of technology provide useful perspective for critically analyzing a truly complex relationship.

To date, collaborative effects between security studies and STS have been scant. This is unfortunate given the overlap of both relevant reference objects and policymaking recommendations that can be informed by experts from both fields. The circumstances surrounding the establishment of, and solutions to the information crisis, demand greater cooperation between the fields. Previous collaborative efforts which *do* exist point to the

utility of such endeavors and have been adequately compiled in the most recent comprehensive overview of STS. "The common strengths of those working in the STS-security interface have been (1) to provide counter-narratives on security compared to traditional understandings and approaches found in other disciplines; (2) to innovate and adapt methods, tools, frameworks, and ideas to emerging security concerns; (3) to contextualize how these concerns can be understood in terms of broader historical and discursive context; and (4) to inform and critique policy responses (Vogel et al. 2017, 974).

Consideration of the information crisis as a security issue demands the leverage of these four strengths. The demand for understanding of humans' normative relationship with information, technology as a facilitator, and the socio-political ramifications therein, defy most traditional approaches. Imagining something as prosaic as a Twitter post as being connected with a wider security concern requires methodological flexibility, while still appreciating how emerging phenomena such as state-sponsored information operations may still informed by the old paradigms of great power politics. Both STS and security studies are disciplines which rightfully embrace change. An STS-security interface provides a convincing answer to the epistemological and real-world questions which will be elaborated upon in subsequent chapters.

2.3 Actor-Network Theory

The conceptual framework of this thesis depends upon operationalizing actor-network theory (henceforth ANT) through understanding the information crisis as a security issue. Dissecting the assemblage of our information crisis necessitates an ANT-security interface. ANT is an evolving critical approach owing its inception to STS scholarship. While ANT was not conceived with security studies in mind it is an effective approach for making holistic accountings of interconnected influences. It is thus well suited for mapping the webs of relationships that predicate the current crisis and informing potential countermeasures and embodies the thesis' primary epistemological recommendation. The practical portion of this investigation will focus specifically on two assemblages that serve to conceptualize the scope of the information crisis; those of alt-right revisionism, and big data. I will use the term "nodes of influence" to characterize key elements within the

assemblages. Nodes can consist of human actors, technologies, cyber-environments, political institutions, or ideologies. Through utilizing ANT to conceptualize the information crisis this paper will establish that it is feasible to leverage it as a critical concept for security studies. ANT provides a better framework for those scholars trying to understand the growing roles that cyber topography and AI-driven technologies play in our relationship to information (and by virtue, misinformation, disinformation, etc.). To achieve these goals, the final section of this chapter will first outline the theoretical underpinnings of ANT, using examples from noteworthy ANT scholars when applicable. It will conclude by advocating that the relationship between cyberspace, people, and information, is demonstrably one that is suited to ANT-like thinking and suggests an ANT-security interface is a worthy approach for this phenomenon.

2.3.1 Theoretical Background

To unpackage the nuances of ANT and make a case for its current utility in our rapidly changing world, we may embark with the question: what is ANT, and how can we use it to better characterize relationships? Scholars specializing in critical sociology of technology such as Bruno Latour and John Law provide us with the principle theoretical background. ANT scholars such as Callon and Urry, provide recommendations on the adaptability of ANT to the political sphere and beyond. These perspectives will be useful to the purposes of this thesis. Latour, Law, and their contemporaries, must be given a great deal of credit for their contributions to STS in offering a theoretical framework which is well suited for the complexities of the 21st century. Indeed, the bulk of the theoretical background which follows is owed in large part to Latour and his work. ANT is positioned to find a third way; between technological determinism on one side, and an over reliance on human agency on the other. This implies that neither people, nor the technologies available to us, can be regarded as the primary agents of change. Society, from an ANT perspective, is a product of interactions between both human and non-human forces. Actors are not the primary focus of analysis but rather the network of relationships created through their interactions. Of course, that is not to say humans are altogether unimportant in ANT. It is the capacity to instill meaning in social artifacts (the discursive, the mechanical, the scientific, and so on) that emphasizes the importance of relationships.

The first principle objective in ANT is to eliminate overreliance on domains. In academia we have grown accustomed to organizing ourselves into neatly cordoned disciplines such as law, science, technology or politics (Latour 2005, 8). By eliminating the emphasis on these spheres of influence ANT strives to, in Latour's words, "regain the sense of heterogeneity, and to bring inter-objectivity back into the center of attention" (Latour 1996, 380 – citing himself, 1994). Through inter-objectivity, or a re-focusing on the substance of relationships between domains, we can better understand the "social aggregates behind all of them" (Latour 2005, 8). ANT does not propose we ignore the existence of different fields altogether, but rather to disengage from using them as a port of call. In some ways, the realities on the ground are helping to vindicate Latour and his colleagues. The utility of re-focusing on the substance of relationships between domains is demonstrable in the way which security studies has expanded its purview over the years to include additional reference objects and relevant relationships. In short, modernity has necessitated an expansion of what we consider to be security-based relationships.

ANT as a critical approach typically uses practical case studies to realize its theoretical tenants. This tact may share similarities with the kinds of case studies used by sociologists of technology like Pinch and Bijker (though they should not be confused as being actor-network theorists). Their treatise on the social construction of facts and artifacts uses the development of the bicycle, and specifically the journey which the antiquated penny-farthing bicycle underwent on its way to becoming what we traditionally recognize as today's bicycle. This transformation illustrates a process in which the interaction of human perspectives and technological artifacts both share equal importance in the process. To establish an actor-network in a practical sense we must consider a few key factors. First, that "all members of a certain social group share the same set of meanings, attached to a specific artifact. In deciding which social groups are relevant, we must first ask whether the artifact has any meaning at all for the members of the social group under investigation" (Pinch and Bijker 1987, 24).

To expand upon the work of sociologists of technology and apply ANT to case studies surrounding counter-factual information, we must account for how certain technological applications such as social media have become a generally acceptable means of obtaining

information. "Another question we need to address is whether a provisionally defined social group is homogeneous with respect to the meanings given to the artifact — or is it more effective to describe the developmental process by dividing a rather heterogeneous group into several different social groups?" (Pinch and Bijker 1987, 27). In the case of the information crisis, delineating between social groups may be variable. For example, their relationship toward information, and specific sources, along lines of political affiliation, as was reflected in the *Harvard Misinformation Review* study. We can, however, regard the spread of inaccurate and deceptive information as a phenomenon belonging to politically homogenous groups within a larger heterogenous group that regards information as being increasingly politicized.

Regardless of the case study or practical application, all actor-networks will necessarily require some instance of "coalescing domains." Consider the mobile device as another example. The word device was chosen deliberately because, from the position of the author, "mobile phone" is an ill-suited moniker. It is also out of date. Telecommunication is one function the mobile device serves and represents a commercial domain. That domain has merged almost entirely with the other purposes which the mobile device serves, navigation, computing, photography, banking, news source, and travel agent, to name a few. Over emphasizing any one of these functions misses the forest for the trees, as the saying goes. So too would over emphasizing the role of cyber topography, algorithms, bots and other AI-driven technologies, domestic or international "trolls," special interests, and the procession of "politics as usual." They are all equal players in the network of relationships which has instigated our current crisis. While Latour and his contemporaries did not characterize ANT with mobile devices in mind, this comparison serves to illustrate the increasing futility of an intellectual marriage to one domain or another in social science scholarship. The fields are necessarily becoming more alike and require increasing "cross-pollination" from an intellectual point of view. Therefore, the relationships, for the actor-network theorist, is of principle importance.

It is necessary to also dispel a few common misconceptions about ANT. The first and most crucial to this investigation is that the core tenants of ANT have no correlation with the study of social networks in general. This investigation engages social networking as one

of its relevant reference objects. The relevant actor-network which the case studies in chapters 3 and 4 intend to operationalize is not solely concerned with user activity, or users interfacing with one another on the topic of politics. Latour comments on that topic. "These studies, no matter how interesting, concern themselves with the social relations of individual human actors - their frequency, distribution, homogeneity, proximity" (Latour 1996, 369). While some of the data concerning disinformation will use "distribution, homogeneity, and proximity," to characterize the crisis itself, those trends do not necessarily relate to the relationships between referential objects (people and things).

Latour further notes that these sorts of studies were "devised as a reaction to the often too global concepts like those of institutions, organizations, states and nations, adding to them a more realistic and smaller set of associations. Although ANT shares this distrust for such vague all-encompassing sociological terms, it also aims at describing the very nature of societies" (Latour 1996, 369-70). This example illustrates the dangers of both mistaking ANT as a "networking" theory rather than a theory concerning and emphasizing networks, and a return to domain specific approaches. Finally, Latour encourages us to think outside of our current conceptualization of dimensions. To utilize an example from *Where Are the Missing Masses*, Latour cautions against our tendency to anthropomorphize technology studies. The distinction between the human and machine, or in the case of this investigation – the user (or recipient of disinformation) and the interface (cyberspace), are less interesting (and less important) than the trajectory along which the capabilities and actions of both are distributed (Latour 2005, 165).

Placing too much emphasis on human agency from the social perspective, or too much determinism on the technical end, empowers each domain unnecessarily and ignores the relationship – or merger – of the two. This relationship is paramount to the case study. The rapid social changes we are experiencing vis-à-vis technology, depends wholly on our relationships with it. These elements cannot be characterized in a hierarchy, but rather as Latour concludes "a *sui generis* object: the collective thing, the trajectory of the front line between programs and anti-programs. It is too full of humans to look like the technology of old, but it is too full of nonhumans to look like the social theory of the past. The missing masses are in our traditional social theories, not in the supposedly cold, efficient, and

inhuman technologies" (Latour 2005, 175). The next subsection will provide a brief overview of the relevant framework for how people, information, and cyberspace may be regarded as an actor-network.

2.3.2 Conceptualizing an Actor-network

While the case studies presented in chapters 3 and 4 are not about social networking, Twitter, Facebook, and their ilk are essential to the discussion as their platforms, software, and algorithms, contribute to the outcome of the relationship in question. We might consider this one set of nodes in the multi-dimensional relationship. These are the relevant "characters," figuratively speaking, that comprise the assemblages. The users are also important, as they are conduits for the misinformation and disinformation that embody the current flourishing of counter-factualism. The mechanisms of adversarial politics represent another node, as they provide the context for discursive exchange. The exchange and reception of information is necessarily predicated by the ideologies which color the predispositions behind user activity. This includes but is not limited to the kind of "self-selection" which occurs when users seek out information that already conforms to their world view, and data that corroborates it. And additionally, information brokers of all kinds vying for user engagement provide another potential node in this increasingly complex relationship. As does the hardware and software; the fast technologies enabling the kinds of interactions through which we trace this actor-network. It is enough to conclude in this case, as Latour has, that an actor is nothing but a network, and a network is nothing but actors (Latour 2011, 800). Politics, technology, socioeconomics, and journalistic media are all relevant to the discussion.

As I introduced in the first chapter of the thesis project, misinformation and disinformation have existed for millennia. Both variants have harnessed advancements in telecommunications over the past half-century to extraordinary effect. Technological advancement in general has become something of a catchall and easy scapegoat for a plethora of studies seeking the already self-evident answers as to "why things have changed so much?" The trite and oft repeated adage "media is controlling/ruining everything," is the antithesis of this investigation. This falsehood implies that there is some hierarchy of influence and means for control (or destruction). Characterizing these influences as

constituent parts of an actor-network is a more precise option for social scientists moving forward. In the case of the example, media is simply another conduit whose presence and relevance are elevated specifically due to the existence and politicization of information. For that to be accomplished, we must ask ourselves, what about the connective tissue between people, and processes, that give the relationship relevance? When considering the answer, I have concluded that ANT is a methodologically sound approach by which we may access this modern problem, from a modern perspective.

Reality is created through practice. "By foregrounding 'practices', this notion helps us to go beyond traditional forms of representation, reinforcing the claim that nothing exists autonomously without relations that sustain entities, which is a clear stance against naturalizing ordering or viewing it in a simplistic way" (Alcadipani and Hassard 2010, 424). "Different narratives 'enact' realities rather than simply 'describe' them, and thus are a 'version of the better and the worse, the right and the wrong, the appealing and the unappealing" (Law 2007, 15 as cited by Alcadipani and Hassard 2010, 424). The most precise term for what Law, Alcadipani, and Hassard are alluding to is performativity. "How a reality is performed (e.g. the sorts of techniques or arguments that are brought to bear and put into circulation) can also induce others to share this reality" (Michael 2017, 162). What we regard as a security issue is essentially misinformation and disinformation as a practice. The practice (or process) includes manufacture, distribution, consumption, internalization, and re-transmission of counter-factual information. The various elements implicit in the process can be regarded as the reference objects and relevant relationships which a prospective ANT-security interface must now concern itself with.

Performativity is the concept which underpins the information crisis as a security issue. The process of reality creation through practice lies at the crux of why counter-factual information, facilitated through fast technologies demands attention. Our normative relationship with information has predisposed large subsets of people to tumble down the proverbial rabbit hole of counter-factualism. The infrastructure and mechanisms of cyberspace have allowed for misinformation, and disinformation to share equal footing with established knowledge. Users, institutions, companies, (all of which may embody the role of information broker) necessarily interface with databases, networks, algorithms, and

AI-driven technologies. Together they become something of a "heterogenous entity" made to "relate to one another and work together" (Vogel et al. 2017, 976). The STS-security scholarship duly proposes we safeguard our socio-cyber infrastructure against global threats. In doing so we must also consider the notion that relationships forged between the social and technical may, in practice, be sources of security issues in and of themselves. While we must safeguard our socio-cyber infrastructure against presumptively external threats, I will also advocate that we must take countermeasures against said infrastructure being purposed as a conduit for counter-factual information of domestic origin.

This investigation will concede that positive-negative paradigms are difficult to establish, philosophically speaking. No doubt there are those who will contest that the information I am deriding as counter-factual is, in fact, "the real story." By selecting ANT as a methodology for imagining the information crisis, I will rather adopt the conclusion reinforced by Alcadipani and Hassard. "Good can only be made locally and empirically. In so doing, it can also serve to undermine the bad. The issue, then, is not to 'avoid translation by ANT' (citing Whittle and Spicer, 2008), but to produce ANT accounts that help us develop critical theory in the form of a political ontology of organizing" (Alcadipani and Hassard 2010, 430). Before simplifying information and counter-factual information in a dualistic "good" and "bad" sense, considering the following process. Many revisionist narratives (misinformation) cast the status quo (information) as the product of a malicious establishment. When the status quo then provides additional information, backed by established knowledge, for the sake of reestablishing legitimacy, it is then disregarded as a gambit by the malicious status quo (Greven 2016, 6-7). This is how we have arrived in a place of cognitive dissonance regarding the use of facemasks as a common-sense public health measure to prevent the spread of the SARS-CoV-2 virus. This intellectual feedback loop is product of the technology, users, and information brokers involved, which form their own entirely unique actor-network. This actor-network represents a threat to any society that is predicated on its citizenry being adequately informed.

It is a threat (or in the language of this investigation, security issue) when considering the relationship between counter-factual information and ideology because, as Law notes,

realities are not immutable. "They are shaped, enacted and contested. Ontological politics [relates to] the way in which the real is implicated in the political and vice versa, meaning that things could always be otherwise" (Law, 2008; Mol, 1999 as cited by Alcadipani and Hassard 2010, 424). While we may challenge traditional notions of politics, socio-political security in electoral democracies requires there be at least some basis for an agreed upon reality – insofar as process is concerned, at the very least. Counter-factual information, as an expression of rival ideologies, have created (through practice) willful contestations of reality. Mike Michael, who writes extensively about ANT, discusses this very phenomenon in characterizing ontological multiplicity / politics:

> The enactment of divergent realities (that together produce ontological multiplicity) can relate to each other in a variety of ways. Sometimes these are overtly political insofar as there is conflict between realities; sometimes they simply coexist; sometimes the politics are more tacit as when they are quietly and practically managed or hang together non-coherently. Where multiple realities are quietly managed, this rests on 'collateral realities' that allow for communication across divergent realities. This evokes another politics, namely the exclusion of those who do not share in those collateral realities. (Michael 2017, 162)

I will briefly characterize the web of relationships that we might consider when confronting the misinformation assemblage surrounding the SARS-CoV-2 virus from chapter 1. We may begin by considering the relationship played by social networks. Twitter, Facebook, and other social media platforms have become a popular means for sharing and receiving politicized information. They are unique and distinct from past means of information sharing because they have fostered an environment in which normal everyday users become active participants in politics. This is not because they are themselves public servants, but rather because they are complicit in the transmission of politicized information in a sphere which transmitting information is itself, a relevant act. If all the information were true, and the probability of exposure equal, then the dilemma would not exist. If all the information were true, the normative relationship we have to information in general would not instigate the conflict between divergent realities. A 2015 study from Eytan Bakshy on social media's ideological divide indicates that if "individuals acquired information from random others, approximately 45% of the hard content liberals would be exposed to would be cross cutting, compared to 40% for conservatives (Bakshy et al. 2015, 2). Randomness does not occur though. Users, as typical social actors, naturally self-select their sources of information and tend to gravitate toward narratives which confirm or

reinforce their believe systems. Bakshy's 2015 study corroborates what the *Harvard Misinformation Review* study demonstrated regarding information about the SARS-CoV-2 virus.

Social media platforms such as Facebook and Twitter also run upon algorithms that rank content and determine exposure based on the interactive history of a user. Therefore, the type of political discourse which a user is consuming continues to inform which kinds of information will be presented to them moving forward. The defining characteristic of this relationship is that it inherently manipulates the types of information that users may access to inform their decisions. The "nearest neighbor algorithms," for which cyber security scholars have invested a great deal of time in characterizing detection strategies, present a unique opportunity for those actors who would seek to spread counter-factual information (Varol 2017, 3). This "topography of cyberspace" can be used to gain advantage, and there are those who would exploit it. (Marwick & Lewis 2017, 83). To revisit the prospect of cognitive dissonance, when a particular user has decided that the perspective on the virus being espoused by the Trump administration conforms to his or her beliefs, they are more likely to encounter information that reinforces that position on account of nearest neighbor algorithms. This assemblage is prefaced by users' tendency to regard information as being ideologically polarized, it creates an environment in which realities become mutually exclusive. To reiterate what Mike Michael's point, "inability to communicate across divergent realities evokes another politics, namely the exclusion of those who do not share in those collateral realities" (Michael 2017, 162).

Another key actor (or actant), whose influence triangulates with the user-algorithm dynamic, are those who would willfully spread counter-factual information as an act of willful misinformation or of deception. We will refer to the latter actors as disinformation brokers. Any actors who engage in promoted information campaigns have a vested interest in the content reaching the broadest possible audience. Disinformation brokers may manifest in many forms including, but not limited to, trolls, ideologues, hate groups, the alt-right, as well as opposition politicians (Marwick & Lewis 2017, 33-39). They can also come in the form of foreign activists vying to intercede to the detriment of another

sovereign country. Russia in this case embodies one of the more recognizable recent examples which I will elaborate upon further in the chapters to follow.

I now revisit writer Alastair Reynolds and his rhetorical question. Everything depends on everything else, doesn't it? If we fully unpackage that assemblage surrounding misinformation vis-à-vis the current pandemic in the United States, there are several key nodes of influence we must consider. For instance: the nearest neighbor algorithms which I will also characterize as cyber topography. These foster homogenous online communities. The inherent bias of the users (on a group level) by virtue of their relative wealth, experience, geographic location, etc., and furthermore – the cognitive predispositions toward ideology, or why exposure to opposing political views increases polarization. The framework of adversarial political processes which instigate ideological competition in the first place. The end goals, and intentions of the information brokers must be considered, be they benevolent or malicious. And additionally, the tools for strategic amplification of messages deployed by information brokers. No single one of these nodes of influence "causes" the other. Therefore, there is no hierarchy. They exist as an entity forged by their relationship to one another; an actor-network.

Latour paraphrases this phenomenon in way better suited to the purposes of this paper. "The reason why people said that interactions create phenomena superior to the individual social atoms is because they had first defined the atoms as self-contained entities deprived of all the other entities necessary for their subsistence. (They had failed to see actors as actor-networks.) Then no wonder that, when entering any interaction, those simplified and castrated atoms had produced unintended consequences: Too little was known about them in the first place! (Latour 2011, 806). This methodological application of ANT has used social media platforms as an example. This is because it provides one canvas, upon which the other relevant influences can be painted. Also, because, for better or worse, a thesis must be written in a linear way. One could just as easily approach the dilemma from a classical great power politics angle, however. In which case social media as a useful distribution tool for disinformation might be rendered just another device for maximizing national interest.

This carousel of intellectual starting and end points could carry on spinning for quite a long time. Therefore, there is real value in focusing on relationships rather than actors (or atoms) themselves. According to Law we need to study "how webs assemble themselves to stage effects such as actors and objects, and binaries such as nature and culture, human and nonhuman, or indeed macro and micro (Law 2013, 42). The following remarks by Law lend themselves so necessarily to the spirit of this investigation that they are included in their entirety.

> "In this version contemporary STS asks questions that are simultaneously about realities and politics or normative. Recognizing its of performativity, it understands that it makes a difference. But what kind of difference does it make? The answer is that it typically tries to find ways of living together well. It does this in many ways, but here are two. In a world in crisis economically, socially, and environmentally, we urgently need to find better ways of living together. STS tells us that technoscience in its present form is part of the problem. Separated from the political, it is destructive because it takes reality to be fixed. So, think about this? One draws on democratic political theory and practice. Democracy is about living together well in a common world. Perhaps the old ways of reconciling difference democratically – parliaments and their analogues – have failed because they reproduce the nature-culture divide, fix nature and exclude it from politics. The task, then, is to invent new method for softening realities, reworking social collectives, and melding these productive and democratically together" (Law 2013, 45).

ANT is emerging as a more viable framework through which the constituent artifacts might be evaluated. "Actors are always interfacing among different social collectives as they are both composed and component of networks" (Venturini 2010, 273). There is of course, also a cautionary tale within all this. There must be some viable connective tissues and ANT as a methodological process cannot be somehow retrofitted to all things that appear to be connected. "Whenever an action is conceived as networky [misspelling intentional due to creative license of Latour], it has to pay the full price of its extension. It's composed mainly of voids. It can be interrupted. It is fully dependent on its material condition. It cannot just expand everywhere for free. (Its universality is fully local)" (Latour 2011, 802). After placing this one frame of this larger image under the microscope, it is apparent that the confluence of relationships contributing to the disinformation crisis we now face.

At present time, we coexist with technologies that give us unprecedented access to both information and counter-factual information. Consequently, we live in a digital briar patch of that threatens our ability to form normative perceptions of reality. The following two chapters will create a legible map of this briar patch. In doing so, they will characterize nodes of influence, and relevant reference objects, that form the web of relationships which

are currently embody our actor-network. They will consist, equal parts, of human and non-human actors. After which, the investigation will conclude with a set of scholarly and practical recommendations regarding the disinformation crisis as a more holistic issue.

3. The Mainstreaming of Alt-right Revisionism as an Assemblage

It was forty years ago when Isaac Asimov observed "anti-intellectualism has been a constant thread winding its way through out political and cultural life, nurtured by the false notion that democracy means 'my ignorance is just as good as your knowledge." Unfortunately, Dr. Asimov's sentiment has aged exceptionally well and is perhaps even more relevant today than in 1980. Tom Nichols, who also channels Asimov in *The Death of Expertise*, adds "these are dangerous times. Never have so many people had so much access to so much knowledge and yet have been so resistant to learning anything…. the modern media, with so many options tailored to specific views, is a huge exercise in confirmation bias. This means that Americans are not just poorly informed, they're misinformed" (Nichols 2017, np). The phenomenon which both Nichols and Asimov allude to, is a symptom of what I have characterized in this thesis project as an information crisis.

The first chapter established that we are currently experiencing an information crisis which has a uniquely debilitating effect on liberal democracies. This is because misinformation and disinformation, as such, impede public understanding and the implications of its own choices (Nichols 2017, np). The second chapter placed emphasis on the role of both security studies and STS, as they have both demonstrated flexibility with respect to relevant reference objects and yet have their own inherent disadvantages due to the scope and speed of the information crisis. Therefore, I have advocated for an ANT-security interface, both as a conceptual and methodological framework, to better conceptualize and provide countermeasures to the crisis. The chapter which follows will introduce a case study for the purposes of operationalizing the ANT-security interface. In doing so, it will emphasize the "connective tissue" between the patterns displayed by human actors and the

technological artifacts which have facilitated and accelerated the crisis at hand. This case will present the mainstreaming of alt-right revisionism as an assemblage.

I have deliberately selected conservative populism, and the alt-right more specifically, to demonstrate our information crisis as an assemblage. This is because its demonstrable causes and effects which realize the assemblage pertain to security studies in four main respects. First, their ideology is both adversarial and more likely to reject established knowledge. Those identifying with populism (and in particular conservative populism) are demonstrably more conspiratorial, likely to disbelieve established knowledge, and (whether knowingly or as a proxy) serve as a channel for spreading counter-factual narratives. This is supported by the conclusions of the *Harvard Misinformation Review* study. The study demonstrates that, regarding the current pandemic, conservatives were less worried about exposure to the virus, less likely to consider it a major health threat, more likely to approve of the Trump administration's handling of the pandemic, less knowledgeable about the lethality, and a remarkable correlation between these views and exposure to corroborating viewpoints on social networks (Jamieson 2020, 2).

Second, they have used cyberspace and social networking to spread their ideology and promote conspiratorial thinking. Technological artifacts such as social networks and the underlying topography of cyberspace has fostered conditions which favor the establishment of intellectual echo-chambers where conditions of cognitive dissonance appear to metastasize. Studies from both Bail and Bakshy corroborate this position. Christopher Bail's study notes that platforms like Twitter and Facebook may "exacerbate political polarization because of social network homophily, or the well-documented tendency of people to form social network ties to those who are similar to themselves (Bail et al 2018, 1). Bakshy observes a higher propensity toward homogeneity in the communities associated with conservative and populist content (Bakshy 2015, 1-2).

Thirdly, the alt-right embodies a threat to democratic institutions and domestic security. In a report cataloging incidents between January 1st and May 8th of this year, Transitional Threats Project director Seth Jones notes that 13 of 14 incidents in the United States were classified as being right-wing. Jones report additionally confirms that in 2018 and 2019, right-wing attacks accounted for 90 percent of terrorism related deaths in the United States

(Marx 2020). According to Major General Clive Chapman, a former head of counterterrorism in Britain's Defense Ministry, "there is a growing trend of right-wing extremism in the U.K., but it is not as significant as the rising right-wing extremism in America." He continues, "terrorists need more than just an ideology to act – they often nurse grievances of some kind and typically have encountered a recruitment environment. That could be a social activity in a real-life community of online." (Marx 2020).

The fourth and final justification in selecting the alt-right as a primary focus is that their potential for destabilizing democratic institutions has been noted and is being exploited by foreign information operations. The preponderance of right-wing literature amplified or placed into circulation via foreign information operations indicates a preference on the part of geopolitical rivals such as Russia and China. Russia for instance has chosen to amplify political and ideological discord in the United States because it serves to destabilize the post-Cold War liberal democratic order, thus aiding Russia's own geopolitical goals (Waltzman 2017, 4). All four elements provide ample justification for considering the alt-right a serious issue. The rationale for suggesting an ANT-security interface for addressing the alt-right is due to the research dilemmas of scope and speed which crop up when attempting to engage the assemblage with more traditional hierarchical approaches. The relevant technologies and human behaviors cannot be considered causal on their own, in isolation. Thus, they must be considered as equal parts in an assemblage.

For the purposes of the case study, I will once again primarily consider the conditions in the United States. The practical portion of this thesis project will contain five subsections, each addressing a relationship, or node of influence, in the larger assemblage. The first influence I will explore is the ideological roots and rhetoric of the alt-right. Since the information promulgated by the alt-right is the primary focus, their ideological underpinnings are the logical starting point. The second section will discuss the relationship between the alt-right and information in cyberspace. It will pay specific attention to how their rhetorical norms logically lead to conspiratorial thinking. The three sections which follow will characterize technologies as actants in the assemblage. I have asserted that the relationship between ideology and newly available technologies have facilitated the mainstreaming of the alt-right. I will elaborate upon the ways in which these

technologies have facilitated the spread of counter-factual information through the manipulation of available information, amplification of misinformation, and the manufacture of disinformation.

3.1 The Ideology and Rhetoric of the Alt-right

Right-wing populism has flourished over the past two decades. Its growth is concurrent with the upswing in access to information in cyberspace. The populist boom is tangible in the demeanor of political discourse and also at the highest levels of leadership. In Europe, Hungary's Fidesz and Poland's Law and Justice party (PiD) have consolidated their power across multiple election cycles. Populist right-wing movements like those in Italy (MS5), France (RN), Germany (AfD), and the Czech Republic (SPD), have also made significant inroads during their most recent spate of parliamentary elections (Kirchgaessner, 2018). The populist turn has brought about Britain's exodus from the European Union and is reflected in the leadership selected for Boris Johnson's present government. In the United States, the leadership and candor of Donald Trump's administration has increasingly trended towards far-right populism as he favors engagement in America's worsening "culture war" over principles of traditional conservatism. As if caught in a feedback loop, the political situation in these democracies appear to be both symptomatic and faciliatory, of a populist-right turn.

Right-wing populism and its ideological progeny, the alt-right, are disaffected offshoots of mainstream conservativism. In *Ctrl-Alt-Delete: The Origins and Ideology of the Alternative Right*, Michael Lyons traces the origins of the present-day alt-right in the United States to the 1980s. Lyons says the alt-right owes its ideological roots to the anti-interventionist, anti-free trade, anti-immigration stance of the 1980s paleoconservatives and the European New Right (ENR) project from 1960s France whose goal was to blend a kind of neo-fascism with choice elements of liberal and leftist doctrines to neutralize accusations of elitism (Lyons 2017, np). Lyons additionally observes an ideological vein running through today's alt-right movement in the United States, from the opposition of "new deal liberalism" of the 1930s, wartime isolationism of the 1940s, and the obsession with threats of domestic communism which characterized McCarthyism of the 1950s

(Lyons 2017, np). Through the decades the more conservative elements within the party drifted apart from the "coastal elite" Republicans whose positions were more inclined towards institution building and the role of the state. The conservative schism which Lyons characterizes occurred at last during the 1980s when paleoconservatives, advocating American isolationism, opposed the "aggressive spread of democracy" promoted by Ronald Reagan's "neoconservatives" (Lyons 2017, np). The successive neo-con administrations of both father and son George Bush, as ideological heirs to the Reagan-era, continued with expansionist foreign and domestic policies.

While things like small government, non-interventionalism, and individual liberties are all characteristic touchstones of the right-wing political ideology, "populism's central and permanent narrative is the juxtaposition of a (corrupt) political class, elite, or establishment," and a populace whose (often unheard) voices are the true and enduring representation of "the people" (Greven 2016, 1). Populist movements like the alt-right favor both policies and narratives which favor the dismantling of established institutions which are presented as being inherently out of touch with the people. This ultimately manifests, in alt-right circles, as an ever-present us versus them paradigm. Much of what the alt-right circulates in the online sphere reinforces this. The proverbial "them" is essential for giving "us" context. This us versus them mentality produces two tendencies which both characterize alt-right revisionism. The first pertains to identity creation, the second to adaptability of rhetoric.

First, populist movements tend to juxtapose an authentic people, "us," against some "other." In some cases, this "other" may represent a political establishment. In other cases, "other / them" is adaptable and embody any policy, person, or group, who runs afoul of the best interests of "us." Irrespective of who or what embodies the "other," identity formation among the "the people" is a key impulse. Today the people are "real-Americans" (or Germans, Italians, Czechs, Poles, etc.) who's traditional values are under threat from overblown governments whose policies directly challenge the set of values upheld by the authentic "people". If one is to follow this process to its logical conclusion, the formation of "an authentic people" identity also logically necessitates the creation of "others." "The more ethno-centric the conception of the people, the more xenophobic the positioning

against the "other", and the clearer the desire to overthrow democratic governance" (Greven 2016, 2). The implication which underpins Greven's point is that the "others" are somehow favored by institution-builders in the government, thus necessitating a change of leadership or in the most extreme cases changing the form government itself.

The second point concerns rhetorical methodologies underpinning the "us versus them" paradigms championed by the alt-right. Both Greven and Bails's work corroborates my assertion that the alt-right must continually deploy politically negative rhetoric. Without their "other" to stand against, there is no core stability for "us". Thus, they must constantly assume the strategy of the ideological offensive. The means by which they accomplish this vary, "but all refuse the give and take of political compromise and demand radical solutions (concerning their core issues)" (Greven, 2016, 2). The tendency to utilize negative or adversarial discourse, could be because populist movements often operate from outside the establishment and lack the institutional capability, central organization, or means to levy their desired outcomes at the institutional level. Thus, they must utilize whatever means necessary to discredit and undermine the legitimacy of the system. Rhetorical approaches utilized by the alt-right range from simple speech acts which may defy politically accepted norms to vast conspiracy theories which call into question a range of themes such as the legitimacy of the government, to reality in general. It is the marriage of populist rhetorical approaches and alt-right narratives facilitated by fast technologies such as social networks that has facilitated the mainstreaming of alt-right revisionism.

In a 1999 linguistics study, Robin Shoaps illustrates a rhetorical device called transposition. Transposition, insofar as it concerns the alt-right, is a tactic that was popularized by conservative talk radio show hosts like Rush Limbaugh and has grown to become mainstream on television and is particularly ubiquitous across cyberspace. "Transposition can be either conceptual, such as ideas or attitudes, or discursive, such as prior speech events, as long as they point to an 'out there' that is separate and beyond the moment of discourse that creates them. In the case of the Limbaugh show, what transposition usually entails is a succinct glimpse 'behind the scenes' of a political event or into the psyche of a political figure" (Shoaps 1999, 402). Transposition is a key facet of the alt-right's

rhetorical methodology. An actor will interpret a policy, speech, or news event while recasting it in the terms of their own world view. The artifact is thus transposed from its original context to satisfy an alternative narrative. We may consider the recent alt-right response to the advice of medical experts as one such example.

Infectious disease experts like Dr. Anthony Facui have suggested wearing facemasks to slow the transmission of the SARS-CoV-2 virus. Alt-right voices have condemned the advisory as a suppression of civil liberties and an attempt to undermine the narrative of the Trump White House. The alt-right has used transposition to create what is known as a red herring fallacy – introducing an idea of only marginal relevance to distract from the point at hand; in doing so, transposing information into misinformation. Fauci's grim assessment of the United States' response to the pandemic has been characterized as a deliberate undercut of President Trump at best and a left-wing ploy to weaken the administration at worst. Using the basic rhetorical device of transposition, populist and alt-right narratives can be adjusted to accommodate radical changes in circumstances. This also holds true for critique. Most criticisms of the alt-right can be transposed to satisfy their us versus them paradigm. Critical voices are distorted or dismissed with ad hominem counter narratives, suggesting critics are part of the establishment or faction to which they are opposed. Alarmingly, the marriage of populist rhetorical approaches and alt-right narratives facilitated by technologies such as social networks that has facilitated the mainstreaming of alt-right revisionism.

Another product of the rhetorical underpinnings of the alt-right is their penchant for conspiratorial thinking. This can in some respects be a logical biproduct of "us versus them" thinking. From the alt-right perspective, if brokers of (what we consider to be mainstream) established knowledge amplify their own narratives to deliberately obfuscate "the truth," then "the truth," so to speak, must lie elsewhere and the establishment must have some hidden and malicious agenda. One such recent example of conspiratorial thinking in action lies in the conspiracy video *Plandemic.* The video asserts that the current pandemic is in fact "based on a vast deception, with the purpose of profiting from selling vaccinations" (Cook et al. 2020, np). John Cook and his colleagues delineate several

hallmark characteristics of conspiratorial thinking. These characteristics are important because they have been increasingly visible in conjunction with the sharing of information across online platforms, the primary means of mainstreaming alt-right revisionism.

The seven characteristics of conspiratorial thinking, which Cook outlines, are contradictory beliefs, overriding suspicion, nefarious intent, conviction that something is wrong, persecuted victim, immunity to evidence, and reinterpreting randomness, which I will briefly summarize. "The *Plandemic* video advances two false origin stories for the coronavirus. It argues that SARS-CoV 2 came from a lab in Wuhan – but also argues that everybody already has the coronavirus from previous vaccinations and wearing a mask activates it" (Cook 2020, np). Herein lies an example of contradictory beliefs. Conspiratorial thinking implies any scientific evidence which fails to conform to the conspiracy theory must be falsified. Unfortunately, believing that the scientific data is falsified naturally leads to the conclusion that the very organizations behind the research must also be complicit. If this is indeed the case, it means the conspirators (individuals or whole organizations) must have nefarious motives (Cook 2020, np).

When conspiracy-based thinking encounters evidence which disproves their world view, there remains an obdurate conviction that something is still wrong. "When *Plandemic* filmmaker Mikki Willis was asked if he really believed COVID-19 was intentionally started for profit, his response was 'I don't know, to be clear, if it's an intentional or naturally occurring situation, I have no idea.' He has no idea. All he knows for sure is something must be wrong: It's all too fishy" (Cook 2020, np). The reason why it is so difficult for conspiracy theorists to change their mind is because even a lack of evidence to support their world view is often offered as further proof that a conspiracy indeed exists. Because, of course, the conspirators themselves are experts in deception. We are all victims of their ruse. Cook's final point, the reinterpretation of randomness, observes that conspiracy theorists see connections everywhere, and therefore cannot scrutinize their own world views for spuriousness. Seemingly random occurrences can be integrated into the conspiracy theory. "For example, the *Plandemic* video suggestively points to the U.S. National Institutes of Health funding that has gone to the Wuhan Institute of Virology in

China. This even though the lab is just one of many international collaborators on a project that sought to examine the risk of viruses emerging from wildlife" (Cook 2020, np). Ultimately, conspiracy-based thinking is the extreme manifestation of transposition, and a natural consequence of the identity creation and adversarial rhetoric popularized by the alt-right.

It is not hyperbolic to suggest that the alt-right is dangerous. In the growing array of reference objects which security studies is concerned, the alt-right must be considered a disruptive influence. The alt-right has grown from a fringe ideology to a mainstream security threat in a short amount of time, carrying with it the accoutrements of conspiratorial thinking; threatening to undermine established knowledge. Their ideology hinges upon framing democratic political processes as an extension of a culture war and in doing so, jeopardizing instruments of both state government and international cooperation. The history, composition, and propagation of the alt-right world view embodies one key node of influence in the larger assemblage of the current information crisis. By claiming they are at war with the establishment, their message has been sadly prophetic. The United States itself is beginning to resemble the echo-chambers reflected online by Twitter and Facebook's nearest neighbor algorithms. President Donald Trump himself is both a consumer of and a conduit for alt-right tropes through the medium of his Twitter account. On account of our increasing dependence on the internet and social networking, the message of the alt-right is now widely accessible, and policymaking is suffering accordingly. The politicization of the current pandemic in the United States embodies one of the most recent indicators, yet the ideological "Balkanization" of cyberspace has been well underway for over a decade. We are now reaping the outcome.

3.2 Introducing Fast Technologies and Cyberspace as Facilitators

The celebration of New Years' in United States, among other things, features a 24-hour television broadcast of Rod Serling's *The Twilight Zone.* The 1960s television series frequently speculates about the influence of technology in society and on our human condition. The emergence of fast technologies as a means of influence in the ways we

gather and interpret information might have served as inspiration for Serling and his screenwriters, had they lived to see it. The relationship between our information consumption and cyberspace, is predicated by what this thesis has characterized as fast technologies; those generating algorithmic responses to the enormous quantity of data available. *The Twilight Zone* has, in popular culture, is also often used as catchall phrase for nebulous, complex, or difficult to grasp concepts. While these characterizations may reflect current public sentiment with respect to the fast technologies that drive cyberspace, that only further signifies a need for better understanding of both their potential for malicious application and potential countermeasures.

Technologies are neither good nor bad. The same holds true for technologies which have enabled us to access and share information. Social networking, AI and machine learning (ML)-driven algorithms, and the advent of web 2.0, all have both benevolent and malicious applications. The difference between benevolent and malicious application of technology depends largely on intent, and human agency. Nuclear technology when used to provide electricity to our cities is ostensibly good, while the same technology used in a bomb to level them is categorically bad. This is dual-use technology. The technologies empowering cyberspace, however, are omni-use. They can be used for purposes that are good or bad, but also exist beneath and within many platforms and applications. Miles Brundage and his colleagues have made significant contributions to the study of how technologies, and specifically AI/ML-driven technologies have been utilized. While a benevolent application could be the use of AI/ML-driven technology to create an automated language translation service, the same technology could be used to drive the production of fake content across social networking platforms (Brundage, Radford, et al. 2019).

Malicious use generally pertains to all "practices that are intended to compromise the security of individuals, groups, or a society" (Brundage, Avin, et al. 2018, 9). The spread of counter-factual information is doing just that. The foundations of AI-driven technologies pertain to language processing, knowledge representation (storing information), automated reasoning (using stored information to make decisions), and machine learning (the ability to adapt based upon information inputs) (Kirk 2019, 188).

"The goal in machine learning is to write an algorithm that can be trained using test data to look for specific patterns" (Haq, et al. 2020, np). The marketing industry has been transformed by the advent of AI/ML-driven, fast technologies. The ability to use data collected by user activity on the internet and subsequently leverage that toward targeted advertising, and projecting new consumer subsets, has been groundbreaking. It has become a more quantifiable and data-driven discipline than in the past (Brightedge Research 2018, 3). If we were to consider politically or ideologically motivated information in the same sense as marketing, the outcomes have been equally significant. According to Meffert, the processing of information can occur three ways, "a preference for negative information (negativity bias), a preference for attitudinally congruent information (congruency bias), and a preference for information about one's preferred candidate (candidate bias). These factors are tested simultaneously and at different stages of information processing: message selection, information processing, candidate evaluation, and message recall" (Meffert et al. 28-9).

In addition to cognitive dissonance, the three factors and four stages which Meffert describes may also have bearing upon why people often struggle with distinguishing between information and counter-factual information. "Information overload leads people to take shortcuts in determining the trustworthiness of messages. Familiar themes or messages can be appealing even if they are false. Statements are more likely to be accepted if backed by evidence, even if that evidence is false. Peripheral cues—such as an appearance of objectivity—can increase the credibility of propaganda. (Paul & Matthews 2016, cited in Waltzman 2017, 6). Individuals, groups, and celebrities, all have the capability to share information and vie for influence over the same platforms as governments, leaders, institutions which generate and disseminate scientific research. While such an egalitarian arrangement is appealing on the surface, it is also problematic. There is a plethora of information now available across the same media as established knowledge advocating positions which are both detrimental to public safety (in the case of the current pandemic), and detrimental to the institutional stability of electoral democracies. "Democratization of influence is not necessarily favorable to democracy" (Waltzman 2017, 6).

3.3 Manipulation of Information Availability

While the ability to manipulate the availability of information is now a new phenomenon, its effectiveness and influence is on the rise. Content on across social networking platforms, search engines, and news aggregators are increasingly contingent upon AI-driven software. Additionally, those of us who engage in social networking, or obtain their news via web browsers and apps, are all participants in the emerging industry of big data. Our habits, preferences, and behaviors are potentially available for third party analysis. This is one crucial means through which information can reach audiences they otherwise would not, by which ideologies may gain followers and momentum, and may limit exposure to contrary or conflicting information. To elaborate upon this process, I will review several means by which technology may be used to manipulate the availability of certain types of information. These methods will be examined from the rudimentary to the more complex

The more rudimentary means of manipulating information availability have been around for over a decade now, with the end goal of changing our perception with respect to what is or is not newsworthy information. This is conducted by strategies such as Google and Twitter bombs. Bombs are noteworthy for a few reasons. First, as I have already established, we tend to confide in sources of information from sources we already trust or agree with. These could be individuals, institutions, publications, or websites. The Google or Twitter bomb is an attempt to exploit our normative relationship with these platforms. In the case of the Google Bomb "web spammers create associations between anchor words or phrases and linked Web pages. These associations force a search engine to give high relevancy to results that would otherwise be unrelated, sending them to the "top 10" search results" (Metaxas & Mustafaraj 2012, 472). Twitter bombs send replies to select users causing them to gravitate toward a specific topic. This generates increased visibility for the topic in question due to its "trending" status. While this had previously been accomplished with the use of bot-driven accounts, which I will discuss further in the subsection focused on amplification, Twitter has recently taken steps to improve its detection and countermeasures against bots (Metaxas & Mustafaraj 2012, 472).

A technique known as astroturfing is another traditional means of manipulating the availability of information. Astroturfing typically pertains to politicized or partisan information and occurs when ideologically like-minded users' band together to influence public opinion on a topic. A 2012 *Guardian* article characterized astroturfing as such: "Astroturfing is the attempt to create an impression of widespread grassroots support for a policy, individual, or product, where little such support exists. Multiple online identities and fake pressure groups are used to mislead the public into believing that the position of the astroturfer is the commonly held view" (Bienkov 2012, np). Astroturfing can also be used to target journalists specifically, giving them distorted view of their work, its reception, and potentially compelling them to modify their view or analysis (Metaxas & Mustafaraj 2012, 473). The common thread running through both bomb and astroturfing approaches is that of human agency. These two techniques exploit our inherent trust in the information we gather online and aim to make certain information appear relevant; legitimate, then it otherwise might be. Metaxas and Mustafaraj's studies refer to the effectiveness of both astroturfing and bombing during both 2010 and 2012 United States Election cycles, when astroturfing was used to observable effect in garnering attention for tea party candidates[1].

The means of augmenting information availability which are most effective today, are the ones that are automated. In 2006 Facebook launched its newsfeed. Users were able to view updates and content shared by their contacts in a linear way. The motivation behind the newsfeed format was a more personalized, tailor-made user experience. It was marketed by Facebook as a place to view the information that mattered most to us. Beneath the veneer of the newsfeed, is the K-nearest neighbor algorithm that generated the content that mattered most. A K-nearest neighbor algorithm, or KNN, is designed "to use a database in which the data points are separated into several classes to predict the classification of a new sample point" (Bronshtein 2017, np). Social networking sites like

[1] The Tea Party movement was a populist / conservative movement during the early part of the 2010 decade. During the 2010 congressional elections, many tea party candidates came to power. It was considered by some political analysists as the right-wing's response to the election of Barack Obama two years earlier. Google-bombs, twitter-bombs, and astroturfing was used to effect by information campaigns on both sides of the political spectrum but is noteworthy as we consider the conservative victories in 2010 as a step in the process of mainstreaming far right populism, and alt-right ideologies.

Twitter, Facebook, Instagram, and YouTube, all personalize their content based upon what users are projected to like. These projections are based on data taken from users' online behavior. These are specifically ML-driven algorithms control the content available to users in at least two substantial ways. Firstly, the quantity of social media users is enormous and growing. Information brokers rely upon "analytics and metrics, sensationalism, novelty over newsworthiness, and clickbait" (Marwick & Lewis 2017, as cited in Brundage, Avin, et al. 2018, 45). From a competitive standpoint this is logical. Yet it also makes them vulnerable to manipulation. All these users are constituent parts in a massive data collection process. Content increasingly depends on the analytics of user activity. Like so many of the relationships examined by this thesis project, the relationship between content and the user becomes a cyclical one. Content is tailored to satisfy what the user is most predictably going to want to see, based on the data of past clicks or interactions, yet the user will privilege the content which is most readily available.

The second effect of ML-driven algorithms is even more significant to the study of counter-factual information and its effects. Algorithms like K-nearest neighbor instigate what can generally be regarded as the "echo chamber" effect. Algorithms such as this, which identify and satisfy content preferences may also trap users in what could be considered an intellectual greenhouse effect. When a subset of the population finds a genre of narrative appealing, irrespective of its veracity, they tend to preference their interactions toward that narrative. The algorithms, when functioning as intended, continue to present ideologically similar content – reinforcing negativity or congruency bias. Equally, alternative viewpoints are filtered out. While this is the natural behavior of the software, it is worthy to also note that content can be promoted within this environment with the explicit end goal of amplifying misinformation and disinformation. Thus, both organic and augmented distribution of information may occur. Through the seemingly innocuous goal of connecting people with like-minded communities, the use of these algorithms has established a domain in which the availability of information can be manipulated.

In December of 2018 I presented a research project with four colleagues at Charles University. The project was undertaken toward the successful completion of a course in security and technology. With my colleagues, Connor Austman, Björn Mielke, Maria

Lucia Miotto, Tomáš Veselý, we set out to examine the impact of these digital echo-chambers when applied to the alt-right ideology and visualize the efficacy of the K-nearest neighbor algorithms in manipulating the availability of information. For these purposes we utilized data gathered on Twitter over a period from December 1st to 7th, 2018. The dataset we collected pertained to the nearest neighbors associated with the hashtag #QARMY. The #QARMY hashtag is associated with followers of the alt-right group Q-Anon. Q-Anon are a collective of conspiracy theorists that traces its roots back to the 2016 election cycle. They are typically pro-Trump, associated with right-wing politics, paleo-conservatism, the "patriot movement" in the United States, and most significantly that there is a deep state cabal bent of undermining the presidency of Donald Trump (Downs et al. 2018, np).

The results of the study reflects, for the time period of data collection, the hashtag #QARMY had a high degree of similarity (or correlation) with users who also associated with the hashtags #WWG1WGA, #QANON, #GREATAWAKENING, and #MAGA, and accounts associated with Donald Trump, patriotic groups, militia groups, and curiously enough, content referencing the proverbial "red pill" from the 1999 film *The Matrix.* The high degree of similarity with these hashtags and associated accounts indicates that the clicks, shares, re-tweets, comments, and other reactions within this community are highly insular. The geographic distribution of the hashtag #QARMY, was most prevalent in the United States and Canada, with 89,000 interactions, versus 3,000 in Europe. The age demographics favored the 25-34 subset accounting for 45.6% of all user activity. The 18-24 age group accounted for the second most interfaces with the #QARMY hashtag at 28.2%, followed by 35-44 at 14.8% (Downs et al. 2018, np). These findings are consistent with other investigations such as Patrick Leman's *Born Conspiracy.* Leman found that adherents to conspiracy theories such as those surrounding the events of 9/11, are most likely to belong to the age 20-35 demographic (Leman 2007, 2-3).

This is all consistent with what we already know about the alt-right ideology, the rhetoric of transposition, and its natural inroad with conspiratorial thinking. The relationship between ideology and manipulation of available information through fast technologies is important in the larger counter-factual information assemblage. Influences such as K-

nearest neighbor algorithms, deployed over Facebook, Twitter, and other networks, are ideal for solidifying communal bonds over shared preferences. Information in this sphere essentially shares a level playing field with counter-factual information. Once a user begins to obtain their information within one of these intellectual echo chambers, the likelihood of exposure to contrary ideas deceases. Thus, they become ideologically homogenized communities. If the information they consume is factual, then the effects are banal. This is not the case, however. Users can manipulate the availability of information through proactive techniques such as bombs or astroturfing. In sharing and consuming information online, the inherent topography of cyberspace also fosters ideologically homogenized communities called echo chambers. This embodies one key node of influence and delineates an important relationship within this assemblage. The mainstreaming of the alt-right is also due, in part, to the deliberate amplification of misinformation using fast technologies within spaces which favor manipulation of available information.

3.4 Amplification of Misinformation

At this point it is worthwhile to revisit the distinction between misinformation and disinformation, as the distinction between amplification of misinformation, and the manufacture of disinformation hinges upon understanding the difference. Karlova and Fisher characterized misinformation as inaccurate while disinformation is intentionally deceptive information (Karlova & Fisher 2013, np). Taking this into account, the actor / actant (source of the information), and intent, are both important in making such a distinction. The distinction is also important in characterizing the information crisis as an assemblage because the various motivations behind the amplification of misinformation or manufacture of disinformation require different countermeasures. I will categorize the amplification of misinformation in three different ways. They are strategic amplification, participatory amplification, and automated amplification.

One of the most visible means of amplifying misinformation comes from those who subscribe to the ideology being promoted by a misinformation artifact (a tweet, a news article, a video, an interview, etc.). Marwick and Lewis do an excellent job in

characterizing such discursive influences in *Media Manipulation and Disinformation Online.* In the case of mainstreaming the alt-right, we find narratives to be "propagated by a far-right hyper-partisan press rooted in conspiracy theories and disinformation" (Marwick & Lewis 2017, 2). Actants in this sphere include but are not limited to online trolls, ideologues, influencers, hate groups, the alt-right, men's rights groups, antisemitic groups, and followers of the "one world government" conspiracy. Notably though, they may also include politicians who perceive their interests may be best served by espousing populist or alt-right tropes which appear to be pervasive with their electorate. A spate of Trump-era elected officials such as Governors Brian Kemp of Georgia, Ron DeSantis of Florida, as well as Congressman Matt Gaetz, also of Florida, have touted debunked narratives, alt-right talking points, and conspiracy theories.

In one such case, "Gaetz killed critical research funding for a New York-based nonprofit called EcoHealth Alliance, which for decades has traced the origins of infectious diseases in an effort to prevent pandemics" (Cardona 2020, np). Gaetz' maneuver was rooted in his belief in the narrative forwarded by the *Plandemic* film; the current pandemic was deliberately engineered in Wuhan laboratory. In an interview with Fox News' Tucker Carlson, Gaetz explained "The [National Institutes of Health] gives this $3.7 million grant to the Wuhan Institute of Virology, they then advertise that they need coronavirus researchers, following that, coronavirus erupts in Wuhan" (Cordona 2020, np). According to the *Miami New Times*, the conspiracy theory plugged by Gaetz made its way to the White House when a reporter from the conservative Newsmax TV channel asked President Trump about the grant. The Trump administration subsequently pulled the $3.7 million dollar grant to EcoHealth Alliance (Cordona 2020, np). The Gaetz example demonstrates the potential for misinformation to be amplified by politicians and elected officials. As they represent the instruments of government, when elected officials present information our normative tendency is to accept it as legitimate or factual.

What Gaetz accomplished, knowingly or otherwise, was what Marwick and Lewis characterize as strategic amplification. The use of our normative relationships to politicians and information consumption through various media, to sow revisionist narratives into the mainstream. Cyberspace, and social networks, have become the

dominant medium by which strategic amplification occurs, but also of participatory amplification. “Politicians utilize strategic amplification, bots, memes, and other discursive artifacts within the framework of cyberspace and social media’s participatory culture (Marwick & Lewis, 2017, 33-39). The phenomenon of participatory culture is another key amplification point. Adherents to adversarial ideologies such as the alt-right have what might be considered an assimilationist impulse that leads to propagating their narratives over assessable media. Participation, or agency, is empowering.

Alex Jones is a noteworthy conspiracy theorist and founder of the online community *Info Wars*. Communities like Jones’ *Info Wars*, a name chosen with unintended irony, have led users to embrace alternative sets of facts. As with the Q-Anon community, the narratives which Jones peddles give the user a sense of authority. These conspiracy theories purport that believers are privy to information which “normal” people are not (Leman 2007, 35-36). Jones’ tagline “there’s a war on for your mind” emphasizes the rift between lies; the corrupted establishment media, and truth; the savvy alternative media who are brazen enough us facts which the establishment has denied us. Participants in these kinds of communities ultimately embrace alternative realities. Socially constructed realities, as created by the narratives they consume which are mutually exclusive with those in the mainstream. As Mike Michael notes, practices produce particular realities (Michael 2017, 162). The term which ANT scholars use to describe this phenomenon is performativity.

Categorizing the third method for amplifying misinformation is somewhat tenuous. This is because while it is used to amplify misinformation, the potential for deception means it also shares qualities with the definition of disinformation; blurring the lines between the two. This notwithstanding, the third and final amplification method also contributes to the mainstreaming of alt-right revisionism. Automated amplification refers to methods of information sharing that depend on AL/ML-driven programs called bots. Amplification via bot-driven activities can occur both parallel to, and sperate from the tenants of manipulating information availability discussed in the previous section. Additionally, bots are used to both enable access to information or to deny. Through denial of genuine information, they can thus amplify the impact of counter-factual information.

Bots have a wide variety of applications. For the purposes of this thesis project bot-driven activities will be considered as "socially oriented, automated, imposter accounts" (Howard et al. 2018, 83). They are "automated scripts designed to influence public opinion" and "can be designed to follow and support politicians in attempts to make the elected officials seem more popular. They can spread propaganda in support of, or against, issues or people. In other circumstances, they can be used to send thousands of tweets to online activists in attempts to [motivate] citizens in an AstroTurf campaign or make reasonable exchanges cacophonous." (Howard et al. 2018, 85-6). In this respect, they have been altering the culture of online communication.

I will propose the term "denial via noise" as appropriate for what is happening in cyberspace. As discourse between ideologically diffuse groups becomes increasingly more adversarial, we cannot discount that bot behavior may be a contributing factor. Bots are used to amplify specific types of information at capacities that would be unachievable for human actants. Consequently, social networking platforms and online spaces can quickly become saturated with counter-factual information and combative discourse that otherwise impedes the gathering of real information. What makes bots difficult to categorize in the misinformation / disinformation paradigm is the difficulty in discerning the origin of a bot program. If we cannot ascertain the source of information, we lose the ability to make an objective appraisal as to its authenticity. Some bot programs are designed to be masquerade as an individual or organization. Bots are also often interacting with human users under the pretense that they are genuine accounts. This recalls the element of deception, a hallmark trait of disinformation. Automated amplification of misinformation as facilitated through actants like bot-driven programs thus provides a suitable segue into the third and final means of mainstreaming alt-right revisionism.

3.5 Manufacture of Disinformation

Deception covers an array of associations. Regarding information, deception can occur as both a product of its veracity, but also its source. Manufacture and promotion of disinformation thus concerns both foreign and domestic actants. Shortly before the submission of this thesis project, the security firm FireEye published a report based on

recently discovered disinformation campaigns focused specifically on "undermining NATO and US troops and Poland and the Baltics." Since March 2017 at the latest, disinformation brokers have created, and inseminated disinformation across social media, pro-Russian news hubs like *Sputnik* and *RT*, and in some cases "hacking the content management systems of news websites to post their own stories. They then disseminate their literal fake news with spoofed emails, social media, and even op-eds the propagandists write on other sites that accept user generated content" (Greenberg 2020, np). Topics of the counter-factual information range from "US military aggression, NATO soldiers spreading coronavirus, NATO planning a full-on invasion of Belarus, and more" (Greenberg 2020, np). What the Greenberg article describes is simply the very latest threat assessment to reflect in the influence of something called information operations.

A Second World War-era manual published by the British government characterized political warfare as a "systematic process' that employs both publicity and propaganda in order to 'influence the will and so direct the actions of peoples in enemy and enemy-occupied territories, according to the needs of higher strategy" (Nestoras 2019, 3). The same ethos has filtered down to present-day great power politics. Today, strategic rivals such as Russia and China, also promote revisionist narratives such as those popular with the alt-right with the end goal of making countries like the United States institutionally weaker. "Boundaries of sovereignty in cyberspace are not clearly drawn and this engenders a near permanent state of political warfare" (Nestoras 2019, 14). The RAND Corporation's Rand Waltzman corroborates this position with a 2017 testimony he gave before the US Senate Subcommittee on Cyber Security. Waltzman says that "Russia has a very different view of [Informational Operations] than the United States (or the West in general). For the Russians informational operations (IO) are a continuous activity, regardless of the state of relations with any government, while the Westerners see IO as limited, tactical activity only appropriate during hostilities. In other words, Russia considers itself in a perpetual state of information warfare, while the West does not" (Waltzman 2017, 4).

Russia's IO strategy in particular "called for sub-dividing the target population based on specific interests or needs, determining who in the community is vulnerable to influence, determining the "social dynamics of communication," establishing dominant narratives

(status quo), designing more favorable narratives (revisionism) with which to supplant it (Paul & Matthews 2016, cited in Waltzman 2017, 6). This can be accomplished utilizing a diversity of means ranging from bot accounts, paid trolls, biased news platforms, modified images or video, or artificially generated text. One of the most popular methodologies is the production of biased or even "fake news." Foreign actors will support the creation of news for the consumption of audiences abroad, such as *Russia Today (RT).* We can discern a great deal from foreign-origin disinformation campaigning. International rivals have identified a certain kind of narrative which is believed to have an institutionally detrimental effect on the electoral democracies in which they are sowing disinformation. These narratives have been overwhelmingly consistent with those amplified within alt-right online communities.

Take an inter-European example for instance. In January 2020, it was established that the French political website *France Libre 24* was a creation of far-right political circles in Poland. The circle had ties to Poland's Konfederacja party and the former member of European Parliament, Janusz Korwin-Mikke. "Its content is frequently copy-pasted from traditional sources such as *Agence France-Presse* or *Ouest France*, but modified to fit anti-establishment, anti-migrant, anti-Islam and climate-skeptic themes, further research has shown. Words are changed or entire sentences deleted to fit the narrative" (Kayali & Wanat, 2020). Pages such as *France Libre 24* distort the news, use the anonymity of cyberspace to falsify the authenticity and source of their stories. Among other things, the case of Polish far-right meddling in the French media demonstrates a willingness to use subterfuge and clandestine means to create an information climate in which it appears that a larger audience subscribes these sorts of viewpoints than exists. It also serves to mainstream alt-right revisionism by galvanizing support within the pre-existing alt-right communities in whichever country is the target of disinformation campaigning.

Information operations have been leveraged with tangible effect. I return now to the report from non-profit cyber monitoring group PropOrNot. The report which identified 200 separate websites as "routine peddlers of Russian propaganda" during the 2016 United States presidential election. Content produced and disseminated by Russian IO, according to PropOrNot, reached a combined audience of at least 15 million Americans and garnered

over 213 million views on the Facebook platform alone (Timberg 2016, np). While there is no tangible evidence to suggest Russian IO were successful in influencing the outcome to the 2016 election in the United States, the data does reflect significant influence. Further mainstreaming and normalizing the positions reflected in the information disseminated. The cases raised in this section are examples of disinformation because its source is disingenuous. The user, or consumer of information, has no bearing on where the information is originating, or what kind of agenda lies behind its creation and circulation. Yet there is no actionable countermeasure in place to combat information operations. As users' interface with information in the main, they will share it across social networking platforms, gaining validity as its digital signature circulates in cyberspace and contributes to nearest neighbor algorithms. They will circulate the narrative with no clear knowledge that it is possibly concocted by actants whose interest is not to inform, but rather to create a false impression of legitimacy. The manufacture of disinformation is yet another layer in the web of relationships that contribute to the central concern of this case study, that of mainstreaming alt-right revisionism.

4. Conclusions and Recommendations

ANT scholar Mike Michael says of material semiotics, it is "the study of how in the making of heterogeneous associations all manner of actors (human and nonhuman) and arrangements (organizations, inequalities) are produced. ANT is a sub-set of material semiotics" (Michael 2017, 160). Having considered the case study of the mainstreaming of the alt-right, I have drawn several conclusions. Populist and alt-right narratives have entered mainstream socio-political discourse and could not have do so without the existence of certain technologies as facilitators. In plain terms, the process has been facilitated by actors; both human and nonhuman, and arrangements; organizational, institutional, and otherwise, because there is a normative relationship between people, information, and the technologies they use to consume information.

The mainstreaming of alt-right driven narratives over the past two decades would be an incomplete process without the actors and arrangements presented in chapter 3. Approaching alt-right revisionism from a social theory, or cyber security standpoint, would

only serve to privilege a hierarchy of influences from one or the other. The process by which alt-right revisionism has become increasingly mainstreamed is the product of an assemblage; an overlapping web of human and technological influences are mutually responsible for the present circumstances. I have compartmentalized the three technological arrangements: manipulation of information available, amplification of misinformation, and manufacture of disinformation, for the sake of organization and simplicity. Yet they exist conjointly. While much of the sharing and communication that occurs in cyberspace is benign, these technological arrangements to disseminate and amplify information that is counter-factual or harmful. Technologies are inherently neither good nor bad, ideology, partisanship, both human characteristics, are significant influences in the kind of outcomes they facilitate.

The case study I have selected for the practical portion of this thesis project in just one example of an assemblage that reflects a particular product (or outcome) of the information crisis. I have characterized it as a crisis for two reasons. The first, because counter-factual is fundamentally detrimental to the stability of society. The existence of strategies such as foreign information operations as a tool of great-power politics confirms this. The second reason I have called it a crisis is because it is, at present, confounding to both researchers and policymakers alike. Cyberspace, over which a majority of information exchange now takes places, is something of a legal, and intellectual grey area. It is for this reason that I have proposed a new approach; an ANT-security interface to address the information crisis as both a scholarly and practical dilemma. Protean problems which require protean solutions.

Insofar as practical solutions are concerned, rethinking how we characterize the information crisis is a logical first step. It may be either encouraging or disheartening to recall that it is still early in terms the close relationship we have forged with fast technologies. The 24-hour news cycle is scarcely two decades old, and the ubiquity of data driven mobile networks even younger. How this relationship will play out in the long term is speculative, since the first generation to come of age with these technologies is still in adolescence. There are, however, several practical solutions which I will propose, based the diagnoses of the dilemma laid out in this thesis project. The first set of

recommendations will need to engage with the platforms and private enterprise through which information is circulated and consumed. The second will embrace wider, systemic policymaking initiatives that would need to be implemented at the society level.

4.1 Technological and platform-based initiatives

Given that nearest neighbor algorithms which drive social networking platforms contribute to the creation of echo chambers, these gateways provide a viable point at which to begin initiating countermeasures. The responsibility then falls to tech-giants such as Twitter, Facebook, and YouTube. The dilemma here is persuading or incentivizing these corporations that it is in their interest to monitor and identify malicious uses of their platforms. As Niemitz has observed, "the internet plays into the hands of populists, as they are best able to communicate their ideology in short messages adapted to the new agora of political discourse, the mobile phone screen." The logical place to enact disruptive countermeasure are at the source. The tech giants have generally evaded regulatory frameworks provided by democratic rule of law though, rendering the internet a relatively lawless place (Niemitz 2018, 6-7). That notwithstanding, there are signs of encouraging developments. As of the first of the year, Facebook has made public statements delineating their intent to curtail the dissemination of doctored imagery (Bickert 2020, np). This is a good first step. Policymakers must continue to further incentivize tech giants to monitor activity based on their terms of use. Last year, under the terms of use purview, Twitter, Facebook, and YouTube all discontinued accounts associated with Alex Jones' Info Wars. Platforms such as Twitter have long been able to monitor and curtail bot activity (Varol et al. 2017, np). Yet another challenge lies in establishing better framework for what satisfies the criteria of counter-factual information.

In some ways the public health crisis surrounding the pandemic has help accelerate technological and platform-based responses to the information crisis. In March, "Mark Zuckerberg announced that Facebook was removing false claims and conspiracy theories flagged by global health organizations. Moreover, Twitter, YouTube, and Facebook now direct those searching for "coronavirus" to sources such as the Centers for Disease Control and Prevention (CDC)" (Jamieson 2020, 3). Countermeasure by denial is not the only

potential approach. We can also undercut counter-factual information by making established knowledge more accessible. Another recommendation from the *Harvard Misinformation Review study* suggests that in cases of acute crisis like the pandemic, online newsprint should disable paywalls that lead to critical information. Their findings reflect that reading mainstream print media is associated with higher levels of knowledge (Jamieson 2020, 4). While extrapolating this to account for all mainstream print media creates a profitability issue for those private enterprises, it is worthy to pursue the possibility of helping brokers of information become more accessible.

4.2 Systemic policymaking initiatives

Recommendations thus far require interventions on the part of private enterprise, who serve as gatekeepers to domains which facilitate the spread of counter-factual information. The problem with interventions is they provide countermeasures only after harm has been done. The alt-right, as embodied by groups that were once on the fringe such as Q-Anon, have already made headway in the mainstream. Greater institutional and societal responses will likely be necessary as living side-by-side with fast technologies becomes the norm. Additionally, state level responses are all but required when considering the ramifications of foreign disinformation campaigns. Niemitz speaks to this point.

> The principle of rule of law, democracy and human rights by design in AI is necessary because on the one hand the capabilities of AI, based on big data and combined with the pervasiveness of devices and sensors of the Internet of things, will eventually govern core functions of society, reaching from education via health, science and business right into the sphere of law, security and defense, political discourse and democratic decision making. On the other hand, it is also high time to bind new technology to the basic constitutional principles, as the absence of such framing for the Internet economy has already led to a widespread culture of disregard of the law and put democracy in danger, the Facebook Cambridge Analytics scandal being only the latest wake-up call in that respect (Niemitz 2018, 2)

To elaborate upon Niemitz, it is also important that measures be taken to eliminate our legislative "blind-spots." Governments in liberal democracies should take measures to foster relationships between experts, academics and policymakers. Those with specializations in AI/ML-driven technologies tend to be disparate and removed from policymaking circles. The world of fast technologies, ostensibly run from Silicon Valley,

has very little interface with Washington. If efforts to stem the tide of counter-factual information are to be successful, policymakers in democratic countries must consider what kinds of legal framework will best accommodate the future of a society living in a state of semi-permanent interface with technology. With a longer-term view toward the future, liberal democracies must invest in teaching "critical-thinking skills alongside practical skills such as detecting misinformation and disinformation in various online platforms, identifying fake accounts and trolls, dealing with trolling, tracing doctored images, the 20 ethics of communicating information on social media" (Nestoras 2019, np). With the conclusion of this thesis project it is my hope that interdisciplinary approaches to the issues which arise from our relationship with information and technologies will provide more holistic accountings of how dilemmas arise, and the imagination to deploy flexible responses.

Works Cited & Further Reading

Aronson, Elliot & Tavris, Carol. (2020). The Role of Cognitive Dissonance in the Pandemic. *The Atlantic*. 12 July 2020.

Bail, Christopher A., et al. (2018). Exposure to Opposing Views Can Increase Political Polarization: Evidence from a Large-Scale Field Experiment on Social Media. PNAS, 2018, doi:10.31235/osf.io/4ygux.

Bakshy, Eytan, et al. (2015). Exposure to ideologically diverse news and opinion on Facebook. Science Express. 8 May 2015.

Bickert, Monika. (2020). Enforcing Against Manipulated Media. *About.fb.com.* 6 January, 2020.

Bienkov, Adam. (2012). Astroturfing: what is it and why does it matter? *The Guardian.*

Brightedge Research. (2018). "Future of Marketing and AI Survey." http://videos.brightedge.com/research-report/brightedge-2018-future-of-marketing-and-ai-survey.pdf

Bronshtein, Adi. (2017) A Quick Introduction to K-Nearest Neighbors Algorithm. *Noteworthy–The Journal Blog*, 2017. https://blog.usejournal.com/a-quick-introduction-to-k-nearest-neighbors-algorithm-62214cea29c7

Brundage, Miles & Avin, Shahar, et al. (2018). The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation Available at: www.maliciousaireport.com

Brundage, Miles & Radford, Alec, et al. (2019). Better Language Models and Their Implications. *Open AI.* 14 February 2019. https://openai.com/blog/better-language-models/

Buzan, Barry and Hansen, Lene. (2009). The Evolution of International Security Studies. Cambridge University Press.

Cardona, Alexi. (2020). *60 Minutes*: Matt Gaetz Conspiracy Theory Helped Ax Crucial Coronavirus Funding. *The Miami New Times*. 11 May 2020.

Clark, Joshua & Bryant, Charles. (2020). *What Was the KGB?* [Podcast] Stuff You Should Know. 7 July 2020.

Cook, John, van der Linden, Sander, et al. (2020). Coronavirus, 'Plandemic' and the seven traits of conspiratorial thinking. *The Conversation.* 15 May 2020.

Downs, Alex, et al. (2018). The Story of Q Army, or, building a better conspiracy. *Security and Technology*. Charles University, Prague. 18 December 2018.

Greenberg, Andy. (2020). Hackers broke into real news sites to plant fake stories. *Arstechnica.* 30 July 2020.

Greven, Thomas. The Rise of Right-Wing Populism in Europe and the United States. *Perspective*, May 2016, doi:10.5040/9781472544940.ch-013.

Haq, Izahr, Abatemarco, Michael, & Hoops Jeffery. (2020). The Development of Machine Learning and its Implications for Public Accounting. *CPA Journal.* June 2020.

Howard, Philip N. et al. (2018) Algorithms, bots, and political communication in the US 2016 election: The challenge of automated political communication for election law and administration. *Journal of Information Technology & Politics.* 15(2) pp. 81-93, DOI: 10.1080/19331681.2018.1448735

Jamieson, Kathleen Hall & Albarracin, Dolores. (2020). The Relation between Media Consumption and Misinformation at the Outset of the SARS-CoV-2 Pandemic in the US. *The Harvard Kennedy School Misinformation Review.* 1 April 2020, Volume 1, Special Issue on COVID-19 and Misinformation. DOI: https://doi.org/10.37016/mr-2020-012

Karlova, N.A. & Fisher, K.E. (2013). A social diffusion model of misinformation and disinformation for understanding human information behavior. *Information Research*, 18(1) paper 573. March 2013. [Available at http://InformationR.net/ir/18-1/paper573.html]

Karlova, N. A. & Lee, J. H. (2011). *Notes from the underground city of disinformation: A conceptual investigation*. Paper presented at the ASIST 2011.

Kayali, Laura & Wanat Zosia. (2020). "French far-right site powered from Poland." *Politico.* 14 January 2020. Updated 16 January 2020.

https://www.politico.eu/article/france-libre-24-far-right-poland-disinformation-collaboration/

Kirchgaessner, Stephanie. (2018) Italy: Populist Government Sworn in as Political Deadlock Ends. *The Guardian*, Guardian News and Media, 1 June 2018, www.theguardian.com/world/2018/may/31/italys-populist-leaders-strike-deal-resurrect-coalition.

Kirk, A. D. (2019). "Artificial Intelligence and the Fifth Domain." *Air Force Law Review*, 80, 183-236.

Koerth-baker, Maggie. Why Rational People Buy Into Conspiracy Theories. The New York Times, The New York Times, 21 May 2013, www.nytimes.com/2013/05/26/magazine/why-rational-people-buy-into-conspiracy-theories.html?_r=0.

Latour, Bruno. (2005). Reassembling the Social: An Introduction to Actor-Network-Theory. Oxford: Oxford University Press, ('Introduction: How to Resume the Task of Tracing Associations', pp. 1-17).

Latour, Bruno. (2009). 'Where Are the Missing Masses? The Sociology of a Few Mundane Artifacts.' *In Technology and Society: Building Our Sociotechnical Future*, edited by DG Johnson & JM Wetmore, Cambridge, MA: MIT Press, pp. 151-180 (first published in 1992).

Latour, Bruno. (2011). Networks, Societies, Spheres: Reflections of an Actor-Network Theorist. *International Journal of Communication* 5 (2011), 796–810 1932–8036/20110796.

Law, John. (2016). STS as a Method. *The Handbook of Science and Technology Studies*. 4th ed. edited by U Felt et al. Boston, MA: MIT Press, pp. 31-58.

Leman, Patrick (2007). The Born Conspiracy *New Scientist*, vol. 195, no. 2612, 2007, pp. 35–37., doi:10.1016/s0262-4079(07)61774-6.

Levy, Frank. (2018). "Computers and populism: artificial intelligence, jobs, and politics in the near term." Oxford Review of Economic Policy 34(3). Autumn 2018, pp 393-417, https://doi.org/10.1093/oxrep/gry004

Losee, R. M. (1997). "A discipline independent definition of information." *Journal of the American Society for Information Science*, 48(3) 254-269

Lyons, Michael N. Ctrl-Alt-Delete: The Origins and Ideology of the Alternative Right. *Political Research Associates*, 20 Jan. 2017, www.politicalresearch.org/2017/01/20/ctrl-alt-delete-report-on-the-alternative-right/?print=print#sthash.YrevTTAs.dpbs.

Marwick, Alice, & Lewis, Rebecca. (2017). Media Manipulation and Disinformation Online. *Data & Society Research Institute.*

Marx, Willem. (2020). Jihadist plots used to be U.S. and Europe's biggest terrorist threat. Now it's the far right. *NBC News London.* 27 July 2020.

Massaro, T. M.; Norton, H. (2016). "Siri-ously? free speech rights and artificial intelligence." *Northwestern University Law Review*, 110(5), 1169-1194.

Meffert, Michael F., et al. (2006). "The Effects of Negativity and Motivated Information Processing During a Political Campaign." *Journal of Communication*, 56. pp. 27–51.

Metaxas PT, Mustafaraj E (2012). "Social media and the elections." *Science* 338(6106). 472-473. DOI: 10.1126/science.1230456

Morris, Jonathan S. (2005). "The Fox News Factor." *Harvard International Journal of Press/Politics*, vol. 10, no. 3, 2005, pp. 56–79., doi:10.1177/1081180x05279264.

Nestoros, Antonios. (2019). Political Warfare: Competition in the Cyber Era. *April 2019 Policy Brief.* Wilfred Marten's Centre for European Studies. https://www.martenscentre.eu/sites/default/files/publication-files/cyber-warfare-politics-era.pdf

Nichols, Tom. (2017) How America Lost Faith in Expertise and Why it's a Giant Problem. *Foreign Affairs.* March/April 2017.

Nichols, Tom. (2017). *The Death of Expertise: The Campaign Against Established Knowledge and Why it Matters*. Oxford University Press USA. IBSN: 978-0-19-046941-2

Nemitz P. (2018) Constitutional democracy and technology in the age of artificial intelligence. *Philosphical Transactions A.* Royal Society Publishing. 14 August 2018.

Paul, Christopher, & Matthews, Miriam. (2016). The Russian 'Firehose of Falsehood' Propaganda Model. *RAND Corporation.* PE-198-OSD, 2016.

Scherer, Matthew U. (2016). Regulating Artificial Intelligence Systems: Risks, Challenges, Competencies, and Strategies. *Harvard Journal of Law & Technology,* 29(4). pp. 354-398. Spring 2016.

Sullivan, Margaret. (2020). The data is in: Fox News may have kept millions from taking the coronavirus threat seriously. *The Washington Post.* 28 June 2020.

Shearer, Elisa. (2018). Social media outpaces print newspapers in the U.S. as a news source. *Pew Research Center.* 10 December 2018.

Shoaps, Robin. The Many Voices of Rush Limbaugh: The Use of Transposition in Constructing a Rhetoric of Common Sense. Text - Interdisciplinary Journal for the Study of Discourse, vol. 19, no. 3, 1999, doi:10.1515/text.1.1999.19.3.399.

Timberg, Craig. (2016). Russian propaganda effort helped spread 'fake news' during election, experts say. *The Washington Post.* November 24, 2016.

Varol et al. (2017). Early detection of promoted campaigns on social media. *EPJ Data Science* 6(13). DOI 10.1140/epjds/s13688-017-0111-y

Vostal, Filip. (2016) *Accelerating Academia: The Changing Structure of Academic Time.* Palgrave McMillan. E-PUB ISBN: 978–1–137–47361–5

Waltzman, Rand. (2017). The Weaponization of Information: The Need for Cognitive Security. *Testimony of Rand Waltzman.* The RAND Corporation. Before the Committee on Armed Services Subcommittee on Cybersecurity, United States Senate. April 27, 2017.

Zhou, L. & Zhang, D. (2007). An ontology-supported misinformation model: toward a digital misinformation library. *IEEE Transactions on Systems, Man, and Cybernetics--Part A: Systems and Humans*, 37(5), 804-813.