MA Dissertation
in International Affairs

Cyberthreats to Democracies

Constructed Dangers to Democratic Functions

Thorlaug Borg Agustsdottir

June 2019

HÁSKÓLI ÍSLANDS
STJÓRNMÁLAFRÆÐIDEILD

Cyberthreats to Democracies

Constructed Dangers to Democratic Functions

Thorlaug Borg Agustsdottir

Thesis towards a Master of Arts degree in International Affairs

Research professor: Gunnar Helgi Kristinsson

HÁSKÓLI ÍSLANDS
STJÓRNMÁLAFRÆÐIDEILD

Faculty of Political Science
University of Iceland Department of Social Sciences

June 2019

Excerpt

This dissertation studies recent types of Cyberthreats to Western democracies, most notably Russia‘s interference in the 2016 the UK Brexit referendum and US presidential elections.
It examines Russian Cyber Information Influence Activities (IIA) and calls upon new approaches from Democratic Theory and Constructive Theory to provide frameworks for analysis. Through this analysis Russian Cyberattacks and democratic weak spots are identified and theorized.
A framework of *democratic social functions* outlines vulnerable democratic activities, providing valuable input into Cybersecurity in theory and practice. Secondly the thesis uses an Ideational framework of ideas and levels of change from Constructive theory for an analsyis of Russian IIA, analyzing the methods Russia uses to attack democracy through Cyberspace. The evidence shows that Russia uses an array of Cyber-tactics to systematically attack political action and public discourse amongst its democratic opponents. Russia’s Cyberattacks are markedly different than previous Cyberthreats; they are largely *discursive*, with Russia using techology and system weaknesses to influence democracy.
The purpose of this thesis is to apply political theory to help Cybersecurity experts and public decision makers understand modern Cyber-threats and assist them in protecting democracy.

Preface

This 30ECTS MA thesis in International Affairs from the University of Iceland is written under the guidance and encouragement of my research professor Gunnar Helgi Kristinsson, whom I'd like to thank for his valuable input.

This thesis marks the end of a long and winding road that led me to many unexpected places and discoveries. The journey brought me from Digital crisis-communication in Iceland to Copenhagen where I fought an indescribably demanding battle for my existence. That all-encompassing battle for my life brought with it new personal challenges but also time under forced bed-rest to enjoy academic writings from Constructive Theory and Cognitive studies, which have greatly enriched my life and hopefully also this thesis. The 'time-out' I was given in Cyberspace with IR theory has deepened my understanding of the underlying forces governing global affairs, and also given me an opportunity to bring an original approach to Cyber-studies through theoretical analysis of current Cyber-affairs.

The subject of Cyber-International-Relations is a longtime interest of mine and its relevance for current affairs makes any attempt of addressing it a humbling process. In my opinion we are standing on the brink of a new time period in International Relations, one where battles evolve around people's minds in a space where realities are fluid and created to fit a purpose. For a brief period in time *history was not written by the winners, but those who were best indexed online.* However, with changes in Cyberspace that brief time has passed and now history-creators are fighting a war of minds, using words and Cyber-resources to create 'made-to-order' realities that suit a political purpose.

I would like to thank the University of Copenhagen for its academic upbringing and devotion to IR theory, especially prof. Ben Rosamond who introduced me to Constructive theory which turned out to have great positive influence on my academic life.

I would also like to thank all the people that have made it possible for me to complete this milestone, Bose for the noise cancelling headphones, my son Kilian, MDR, dad and aunt Una.

Index

Excerpt 3
Preface 4
Index 5
1 International Relations in Cyberspace 7
1.1 Introduction 8
1.2 Research Problem: Democracy and Cyberspace 9
2 Studying International Cyber Relations 12
2.1 Scope of Inquiry 13
2.2 Approach 14
2.3 Operating Hypothesis 18
2.4 Methodology 21
3 Concepts in International Cyber Relations 23
3.1 Cyberspace 23
3.2 Cyberpower 25
3.3 Cybersecurity 27
3.4 Cyberthreats 29
4 International Cyber-relations 32
4.1 Internet Governance 34
4.2 The Multistakeholder Model 35
4.3 Social Relations in Cyberspace 37
4.4 Cyber Law 42
4.5 Social Media and Privatized Public Discourse 45
4.6 Cyber-Insecurity 48
4.7 Anarchy and what states make of it – Realism vs. Institutionalism 50
4.8 Cyber-Space: Anarchy, Chaos and Dis-Order 53
5 Democratic theory 57
5.1 Key Components of Democracy 58
6 The Problem: Cyberattacks on Democracy 64
6.1 Democracy's Security Alliance & Emergence of a new Space 65
6.2 Russia: Waking of the Cy-bear 69
6.2.1 Information and the Russian State 73
6.2.2 Criminality in Crimea 76
6.3 Russian Cyberattacks on Democracy 80
6.3.1 Undermining Democratic Institutions 86
6.3.2 Creating social rifts 88

6.3.3 "War is peace. Freedom is slavery. Ignorance is strength." 90
6.4 Social Media & Personalized Cyber-Realities 93
6.5 Applied framework of democratic functions and actions 93
7 IR Theory and Cyberthreats 98
7.1 Theoretical Analysis of a Problem 99
7.2 Constructivism – an Idealistic turn in International Relations....102
7.3 Ideas and Discourse....104
7.4 Ideational power 107
8 Constructive Theory & Cyberattacks 109
8.1 Constructive Theory 109
8.2 Discursive Institutionalism 110
8.3 Ideational Analysis of Russia's Information influence Attacks 113
8.4 Post-Truth: Deconstruction of Discourse 116
8.5 Construction of a Virtual Reality 118
9 Conclusions 122
10 Tables, Figures and Images....126
11 Addendum....127
12 Bibliography....3

1 International Relations in Cyberspace

> Diplomacy is experiencing a crisis, and this has become more evident in the past year. A basic principle, which is honoring one's word and one's signature, is overtly being challenged. A second principle, which is to agree on the facts to find a compromise, is no longer being adhered to because facts are being manipulated, refuted and rebuffed. If there is no shared, common truth, how can there be dialogue? Moreover, actors demolishing multilateralism are ratcheting up their methodical attacks.[1]

The words of the French Foreign Minister describe current state of International Affairs and the French way of looking at an international problem. There are still many who deny that there is a change in international affairs and democratic institutions, but a growing number of scholars and politicians agree that there is a new type of war going one in the world right now, one that is predominantly being waged in Cyberspace rather than with traditional warfare.

This thesis examines evidence and applies IR theory to Cyber-International-Relations in order to deepen an understanding of dangers posed by those attacks, particularly through the use of Constructive Theory from Political Economy which emphasizes the *importance of discourse and ideas in change*.

[1] Le Drian, 2018

1.1 Introduction

Our world is increasingly dependent on connected computers. Nearly all aspects of modern life rely on connected computers running safely and accurately on a reliable electric source, solving high and low problems from predicting the weather to running our power grids. Connected computers handle most of Earths wealth and transactions, they tally taxes, keep business running and we increasingly use Cyberspace to select our leaders.[2] Computer technology is one of the greatest tools ever invented, causing a truly global revolution in how human societies organize and manage themselves. Leaving no area of modern life untouched they keep our societies running and their importance cannot be overstated.[3]

During the early days of Cyberspace its creators, scholars and politicians had high hopes for it benefiting and developing democracy, particularly deliberate democracy, a theoretical branch that focuses on how discussions formulate priorities and consensus.[4] Indeed, Cyberspace has provided plenty of opportunities and benefits to democracies, notably the efficacy of government operations and communication with citizens, considered a key element of democracy by democratic theorists.[5]

However, developments in Cyberspace and international Cyber-relations has sparked growing concerns globally for democratic theorists, politicians and citizens.

Cyber-attacks on states and international institutions have become ever more sophisticated and brazen with evidence linking back to organized crime syndicates, rouge agents and more notably to highly organized foreign state agents that openly and covertly use coordinated multi-level attacks and propaganda campaigns to destabilize and affect targeted aspects of democracy.[6]

[2] Newman, et al., 2018. R. Mueller, 2019.
[3] Schreier, On Cyberwarfare, 2015. Newman, et al., 2018.
[4] Dryzek, 2017.
[5] Dahlgren, 2005. Warren, 2017., Dryzek, 2017. Le Drian, 2018.
[6] DHS & FBI 2016-2018. U.S. Department of State, 2019.

1.2 Research Problem: Democracy and Cyberspace

Technological advancements tend to bring increased power to states, if not through military power, then via increased financial power and status – digital-inventions included. Undeniably communications technology and Cyber-inventions have brought great power, status and wealth to their countries of origin, as well as those who adapt those technologies early. Furthermore, digital technologies and Cyberspace have created a new political arena of power of its own; *Cyberpower*.

Considering human history, it is unsurprising that Cyber operations have become an indispensable part of modern *political warfare*.[7] Advances in technology have historically been at the heart of increased power and significant military successes, from spear-throwers and superior-swords to cannon-designs, stealth-drones and digital-surveillance.

Democratic states have for decades reported that critical infrastructure and vital functions of state operations have been attacked through digital channels. From 2014 those reports have gotten more frequent, more detailed and backed up by more evidence. [8] Cyber-tactics were prominent in the 2014 annexation of Crimea, and have since then been used on Western democratic societies and companies. Executed through a wide array of Cyber-attacks, and most recently – and effectively – through information warfare that's targeted towards democratic institutions, leaders and norms.[9]

An increasing number of scholars and political advisors claim that Cyberspace has brought about changes in modern diplomacy and state operations, opening the door to news types of warfare; one that's never been wrought before. They claim those attacks, conducted in and through Cyberspace, have managed to "manipulate public opinion, disturb elections, isolate vulnerable social groups, and destabilize entire regions and countries."[10]

Up until very recently security experts have maintained that the world had not yet experienced a war that's only taken place in Cyberspace, and that Cyberattacks, however

[7] Jensen, Valeriano and Maness, 2019.
[8] Pomeranzev and Weiss, 2013., Stoltenberg, 2017.
[9] R. Mueller, 2019., Jensen, Valeriano and Maness, 2019., Federal Bureau of Investigation, 2017.
[10] Pamment, Nothhaft, et al., The Role of Communicators in Countering the Malicious use of Social Media, 2018.

sophisticated, had only been used as complementary tools to further a wider online and offline agenda.[11]

We may be currently experiencing the change where wars are waged on minds and systems in Cyberspace – *and even that an asymmetrical Cyber-war is upon us*.[12]

Credible, evidence-based claims by judges, security and intelligence experts, political liaisons, journalists and state officials maintain that Russia has been successful in affecting recent democratic elections, influencing governance and affecting international relations.[13] State representatives, respected media outlets, international scholars and intelligence agencies report that Cyberattacks have changed in tone and form and that they now focus to an alarming degree on democratic institutions, processes and norms.[14]

Reports claim that while a large portion of state-operations is targeted towards infrastructure and systems that currently enable rogue agents and enemy states to shut-down vital services of their opponents whenever they chose to do so at the cost of counter-strike, there is additionally a clear change in tactics and form with the addition of *psychological warfare*. 'Traditional' system Cyber-attacks are now used as supplementary attacks to gain power and information, with the core focus of recent Cyber-attacks directed towards manipulation of information and human cognition. Cyberthreats have been becoming more idealistic and *discursive in nature*.[15]

Cyber-attacks on democratic states, where foreign state agents have successfully intervened in democratic processes using various Cyber-tactics, have reached a level that consists ***an attack on democracy***.[16]

Several official reports, including a report by US Special Prosecutor Robert Mueller "determine[d] that Russia's two principal interference operations in the 2016 U.S. presidential election - the social media campaign and the hacking-and-dumping operations - violated U.S. criminal law" in addition to international treaties.[17]

---

[11] Stevens, Global Cybersecurity: New Directions in Theory and Methods, 2018
[12] Shreier, On Cyberwarfare, 2015., Mueller, 2019.
[13] Way and Casey, 2018.
[14] Pamment, Nothhaft, et al., Countering information influence activities A handbook for communicators, 2019.
[15] Zarate, 2017. Seddon, 2014. Studdart, 2018. Cohen, 2009. Gomez and Villar, 2018. Jensen, Valeriano and Maness, 2019.
[16] Studdart, 2018. Zarate, 2017., Pamment, Nothhaft and Agardh-Twetman, et al., 2019., Seddon, 2014. Pomeranzev and Weiss, 2013., Lucas and Pomeranzev, 2016.
[17] Mueller, 2019.

The Democratic minority of the US Senate Committee on Foreign Relations submitted a report in January 2018 outlining „Putin's Asymmetric Assault on Democracy in Russia and Europe: Implications for U.S. National Security" outlining Russian asymmetric assaults and their possible effect on America:

> Mr. Putin's Kremlin employs an asymmetric arsenal that includes military invasions, *Cyberattacks, disinformation*, support for fringe political groups, and the weaponization of energy resources, organized crime, and corruption. [me mine] [18]

The politicization of Cyberspace has also meant a new type of weaponization of Cyberspace.

[18] Committee on Foreign Relations, US State Senate, 2018.

2 Studying International Cyber Relations

> Land, sea, air, and space power are able to generate strategic effect on each of the other domains. But nothing generates strategic effect in all domains so absolutely and simultaneously as Cyberpower, because Cyberpower is ubiquitous.[19]

The inspiration for of this theory is claims made by several domestic and international intelligence authorities that democracy is under attack *in* and *through* Cyberspace.[20]

Cyberattacks on democracies and democratic processes bring Cybersecurity to the forefront of Political Science, International Relations (IR) and state security; Scholars have to an increasing degree been addressing the *nature of Cyber-attacks* and *if* and *how* these attacks have managed to affect state's democratic institutions, security strategies and military operations.[21]

IR theory can contribute understanding to the relationships between Cybersecurity and Democracy, but more theorization and study of the field is needed. More political Scientists and IR scholars need to focus on politics in the domain of Cyberspace, this holds especially true considering the deep understanding and theorization that's already well established within conventional security and military studies.[22]

The academic and practical aim of this study is to select and apply the appropriate IR theory investigate said reports, and analyze the threat democracy is posed by discursive and misinformation attacks, with two goals in mind; *to further theoretical insights into the subject* and *to increase political and academic understanding of Cyber threats to democracies*. This study researches *dangers posed to democracies by certain types of Cyberthreats* and through theorization hopes to add to democracy's arsenal of viable defense strategies and countermeasures against said threats.

[19] Schreier, On Cyberwarfare, 2015.
[20] Zarate, 2017.
[21] Kramer, 2009.
[22] Kramer, Starr and Wentz, 2009.

2.1 Scope of Inquiry

Here the field of inquiry is defined, but not confined, according to a widely used military and security framework that outlines a 'field of operations' for our research subject: Cyberspace. The framework identifies four operational categories or 'fields of empowerment'; Political/Diplomatic, Information, Military and Economics also known as P/DIME.[23]

The P/DIME model represents a 21st century organizational concept originating in US military academia. It outlines core elements of state power, and how state security relies on the expertise, infrastructure and intelligence of professionals in different areas and levels of society. Decidedly, according to the P/DIME framework this IR thesis fits academically within Political/Diplomatic studies of Cyberspace; it examines Cyberthreats for democracies and how targeting weak spots has affected democracy and International Relations.[24]

Currently there are estimated around 4.2 billion Internet users in the world, with over 3.3 billion users of Social Media spread over hundreds of platforms in every language imaginable, many relying solely on Cyberspace for their source of news and current events.[25]

There is an academic gap in Political Theory regarding Cyberpolitics, particularly on information-based Cyberwars, on the methods used, how these tactics affect humans, their extent and long-term and short-term effects on citizens, norms and institutions.[26]

With the increasing role Cyberspace plays in democratic society and political decision making, this thesis gathers evidence and connects theory in order to provide academic insight into *how information-influence Cyberthreats manifest politically*. The thesis discusses *the role of ideas for democracy* and examines evidence on *how* those ideas are attacked across state borders to influence democratic outcomes and institutions.[27]

The dissertation uses IR theory to explore *what* is attacked *how* in relation to Cyberthreats to democracies, examining Russian cyberattacks against democracies through Cyberspace, the global institutional environment and actors that enabled these attacks.[28]

---

[23] Kramer, Starr and Wentz, 2009.
[24] Starr, 2009.
[25] Hu, 2018. Newman, et al., 2018.
[26] Tenove, et al., 2017., Stevens, Global Cybersecurity: New Directions in Theory and Methods, 2018.
[27] Giles, 2015., Jensen, Valeriano and Maness, 2019., Pomeranzev and Weiss, 2013.
[28] Blaikie, N. 2000. . *Designing Social Research, The Logic of Anticipation.* Cambridge: Blackwell Publishers. Blaikie 2000.

2.2 Approach

The research adheres to positivist *epistemology*, that is, it assumes knowledge can be established through the use of scientific method and the subject findings categorized and postulated into a comprehensive theory.

The underlying *ontological* view is rational and analytical; the goal of the study is not to regress the subject into its parts or governing laws through vigorous simulations or tests.

It is an analytical quantitative study that examines evidence of cyberattacks on democracies and builds upon recent academic research and theorization by Western liberal-democratic scholars with the aim to further understanding of cross-border attacks on democracy through misinformation in Cyberspace.[29]

Assumption of actor's interests and motives is *state-centric*, following both realist and liberal IR theory where "states are the dominant actors in the system, and they define security in "self-interested" term" where states self-interests are taken for granted.[30]

Other actors, such as terrorist organizations and financial criminals can certainly have great influences on global affairs but lie out of the scope of this study. At the same time, it is necessary to acknowledge *a cosmopolitan view of globalization*; the inter-connectedness of a globalized world. To acknowledge the power of economic, circumstantial and environmental factors and an array of important non-state forces, such as international institutions, treaties and diplomatic norms.[31] The international environment - where events play out – has a great influence on the solutions that are available to actors. But following constructive theorization I maintain that ideas also have an influence of their own, especially if they are state-backed and systematically spread. [32]

[29] Kurki and Wight 2007., Pomeranzev and Weiss, 2013.
[30] Wendt 1992.
[31] Internet Society 2001., Internet Society (ISOC)., 2016.
[32] Merton 1948., V. Schmidt, Reconciling Ideas and Institutions through Discursive Institutionalism, 2010., Hay, International relations theory and globalization, 2013.

The Cybersecurity scholar Tim Stevens argues that Cybersecurity studies are coming out of a period of theoretical stagnation where they became too focused on solving policy programs at the expense of theory building and methodological innovation, and that inter-scholarly theoretical inputs were needed.[33]

I agree with this view and point to theorists originating in political economy who have been working diligently over the past couple of decades on creating a new framework within political theory of ideational studies under a Constructivist label.[34]

The goal in this thesis is to contribute towards filling a substantial theoretical gap regarding the relationship between International Relations and Democracy in Cyberspace, by using inputs from Discursive Democracy and particularly Ideational approaches of Constructive theory.

The unique angle of this thesis is the application of IR theory and Political Economics to a Cyber-Space largely governed by anarchy; connecting Democratic and Constructive theory to evidence, with the normative aim to provide insights into Cyberthreats that preserve democracy in a digitized world.

This thesis study brings together old and new strands of IR theory. Identifying weak areas through the use of Democratic Theory[35], with particular insights from *Discursive Democratic Theory* for its emphasis on the importance of discourse and political social action for functional democracies.

The study relies on an analysis by Warren who creates a framework of seven types of political social action that support three key elements that he deems are needed for an organization or state to be truly democratic in function.

Warren's framework of democratic action is critical for revealing *which types of democratic activities are vulnerable* and provides an excellent frame of reference for how democracy is being attacked through Cyberspace.[36]

[33] Stevens, Cyber Security and the Politics of Time, 2010., Stevens, Global Cybersecurity: New Directions in Theory and Methods, 2018.
[34] Dunne, 2013.
[35] Waltz 1998., Warren, 2017.
[36] Warren, 2017.

Secondly the study uses *Discursive institutionalism*[37] as a part of Constructive Theory springing out of studies on Political Economy[38] which examine specifically *the role of ideas* in institutional change, including their spread and impact on International Relations. Its contribution is substantial for understanding virtual worlds and how perceptions influence decision making it provides a framework for analyzing ideas according to their level or generality and to which cognitive or normative ideas are being targeted.[39]

> Discursive institutionalism serves as an umbrella concept for the wide range of approaches in the social sciences, going from the 'ideational turn' in comparative politics and political economy (Beland and Cox 2010; Blyth 1997) and the 'agenda-setting' of policy analysis (Baumgart- ner and Jones 1993) to the constructivist turn in international relations (Wendt 1999; Finnemore 1996) and the discourse analysis of post-mod- ernism (Bourdieu 1990; Foucault 2000; Howarth et al. 2000). In discursive institutionalism, ideas and discourse may appear in different forms, be articulated through different kinds of arguments, come at different levels of generality and change at different rates. Moreover, such ideas and dis- course may be generated, articulated and contested by 'sentient' (think- ing, speaking and acting) agents through interactive processes of policy coordination and political communication in different institutional con- texts (Schmidt 2008, 2011, 2012). [40]

To examine *how* these attacks are conducted I call on evidence for current Cyberattacks from countless studies and revelations of raw data. My approach is to use raw-data, current reports and academic studies to examine *ideational elements* of Cybersecurity, following the methodological discipline of *discursive institutionalism*, a sub-strand of constructive theory, that reveals patterns in discursive Cyberattacks by examining evidence and applying *theoretical frameworks for analysis.*

Ideas are particularly important in relation to discursive democracy, for ideas are „the subjective content of discourse".[41] While Cyber-communication can take on many forms, what's of importance is the substance being conveyed.

Ideas are defined here as "subjective claims about descriptions of the world, causal relationships, or the normative legitimacy of certain actions."[42]

---

[37] Wendt 1992., V. Schmidt, Discursive Institutionalism: The Explanatory Power of Ideas and Discourse, 2008., Hay, International relations theory and globalization 2013)
[38] Blyth, Routledge Handbook of International Political Economy IPE) IPE as a global conversation 2009)
[39] V. Schmidt, 2008)
[40] V. Schmidt, Britain-out and Trump-in: a discursive institutionalist analysis of the British referendum on the EU and the US presidential election, 2017.
[41] Ibid.
[42] Campbell, 1998, pp 3.

Ideas are furthermore the foundation of this study, as *critical agents for change* on all levels of International Relations: "ideas shape the understandings that underpin political action and the rationale and purposes of organizations and policies."[43]

For the discussion of ideas, we view them through a theoretical Constructivist framework that categorizes ideas according to a 'theory of mind' that assumes political ideas fall into a two-dimensional framework for ideational analysis, distinguishing between *cognitive* and *normative* types of ideas, on the levels of *policy*, *programs* and *paradigms*.[44]

"*Principled beliefs* are essentially the normative bases and justifications of particular decisions, while *causal beliefs* are beliefs about means-ends relationships."[45] Normative ideas attach values to political action and serve to legitimate the policies in a program through reference to their appropriateness", while cognitive ideas focus on *how*.[46]

„Whereas both policy ideas and programmatic ideas can be seen as foreground, since these tend to be discussed and debated on a regular basis, the philosophical ideas generally sit in the background as underlying assumptions that are rarely contested *except in times of crises*." [47]

The Constructive framework of ideas provides a scheme to (better) understand the message that's being sent. Applying it to evidence is my attempt to develop a tool to analyze constructively what type of ideas are being attacked through Russian information and idealistic attacks.

[43] Béland and Orenstein 2013)
[44] Schmidt, 2008)
[45] Blyth, 2007, pp 14. Hall 2003., Goldstein and Keohane, 1993. Bottici, C. and Challand, B. 'Rethinking Political Myth. The Clash of Civilizations as a Self-Fulfilling Prophecy', European Journal of Social Theory 9(3), 2006, pp. 315-336..
[46] V. Schmidt, 2015. Schmidt, 2011.
[47] V. Schmidt, 2015.

2.3 Operating Hypothesis

This study investigates claims made by Juan Zarate former US Deputy National Security Advisor for Combating Terrorism, that Russia has used "information and influence operations and Cyber tools to achieve three important and complementary goals:

- **To undermine faith and confidence of democracy and its institutions from within**
- **To exacerbate social and political divisions advantageous to Russian interests, including in furtherance of Russian foreign policy or simply to undermine Russia's enemies and opponents**
- **To take advantage of 21st century information environment to obfuscate or confuse the truth and amplify narratives that align with Russian interests, even when patently false**

Operating under the hypothesis that:

> Democracies, particularly key Western democracies, face a new type of Cyberthreats that use information and ideas to attack and deteriorate democratic institutions, processes and norms through Cyberspace.

Russian state operations and state connected entities have launched sophisticated and successful mis-, dis- and mal-information attacks on Western democratic norms and institutions via Cyberspace.[48]

While a large portion of Cyberattacks continues to follow previously established Cyber aggression patterns, with constant and continued attacks on infrastructure and technology, there is a marked change in Cyber war-tactics and operations with a torrent of Cyberattacks that are discursive in nature, following a pattern and ideology established by the former Soviet Union (USSR).

It should be clear that while those attacks have not been proven beyond reasonable doubt to be *the single* causal influence in certain cases, but they have undeniably been highly effective, and may in harmony with other factors have pivotal influence at key junctions in time.

[48] Stoltenberg, 2017., Pomeranzev and Weiss, 2013., Pamment, Nothhaft, et al., The Role of Communicators in Countering the Malicious use of Social Media, 2018., United States of America, 2018. Zarate, 2017., Higgins, 2016., Wardle and Derakhshan, 2017.

Because "[t]he open architecture of the internet creates a unique vulnerability" the dangers these discursive Cyberattacks pose are both urgent and serious. [49]

The evidence chosen for the study predominantly relates to Russia's recent attacks on key Western democracies. These attacks have been widely reported, press releases sent, and evidence provided by Social Media to world leaders on various occasions.[50]

Russia is selected as an actor of inquiry for two reasons; first because Western governments have repeatedly and very publicly accused Russian state agents of a variety of Cyber-attacks, charging and convicting individuals and organizations in-absentia of interfering with democratic elections and public discourse through covert action[51]. Secondly because Russia's "supposedly trouble-proof political machine"[52] has as good as admitted that it is behind discursive interference: "playing with the West's minds" using its allowance for public debate and mistrust towards authorities against themselves.[53] In the past few years Russia has showed signs of outward aggression after the fall of Communism, surfacing internationally with populist tact and old power-moves while campaigning an ideology of 'managed democracy'.[54] Reportedly Russia has meddled in the politics of at least 24 countries since 2004 and is showing increased intent to resolve matters through any means available outside of the realm of international norms of cooperation and institutionalization.[55]

According to experts, evidence and own admittance Russia towers over any other government in the scale and scope of attacks on democratic norms and institutions, often executed with help of domestic actors and interest groups that receive Russian financing and know-how, but then execute the attacks locally and in coordinated attacks with Russian paid agents.[56]

I limit the scope of evidence in this study to Russian attacks on NATO states, predominantly USA and the UK but also other democracies where Russia has attacked The

[49] Jensen, Valeriano and Maness, 2019.
[50] Committee on Foreign Relations, US State Senate, 2018., Zarate, 2017., Pamment, Nothhaft and Agardh-Twetman, et al., 2019. Stoltenberg, 2017.
[51] Committee on Foreign Relations, US State Senate, 2018.
[52] Surkov, 2019., Trudolyubov, 2018.
[53] Surkov, 2019.
[54] Isasc and Wakabayashi, 2017. The Daily Beast, 2018. R. Mueller, 2019.
[55] Dorell, 2017.
[56] Zarate, 2017., United States of America, 2018.

scope is limited to Cyberattacks that integrate Cyber-tactics and information influence activities to wage a propaganda war in Cyberspace, one that attacks democratic candidates, norms and institutions.

The view here upon IR players is a liberal-realist stand, it views current (nation) states, institutions, agencies and actors as entities with interest and agendas that often constitute more than the sum of their parts operating under the goal to secure liberty and democracy for its citizens.[57]

[57] Cohen, 2009.

2.4 Methodology

As previously stated, this study in International Cyber Relations examines Cyberattacks and Cyberthreats on democracies through application of Democratic theory and Constructive theory.

It explores *what* and *how* in relation to Cyberthreats to democracies, that is the focus is on *what* is being attacked *how,* before finally discussing the influence and dangers those attacks face to democracy.[58]

The method of enquiry is to examine evidence of recent Cyberattacks on several developed and allied democracies from the perspective of Constructivism; the ideational ways and means used to attack democratic processes, institutions and norms.[59]

The thesis establishes its *foundation of knowledge* through evidence provided by official sources and information from peer-reviewed articles on theory and Cybersecurity by scholars and experts published in academic journals and periodicals. This is in accordance to the view of The English School of International Relations that "combines theory and history, morality and power, agency and structure."[60]

This study has revealed that the focus of security experts and academics has predominantly been military centric protection of infrastructure and financial security with little emphasis on the effect of Cyberattacks on human cognition and reactions.[61]

Most of the literature published on Cybersecurity and democracy covers 'traditional' state-centric view of Cybersecurity, with a small, but growing number dedicated to the effects of Information Influence Activities (IIA) on liberal democracies. Little has been written about these events from the perspective of political theory and even fewer from Constructive theory, with some noteworthy exceptions.[62]

This lack of cross-disciplinary literature on Cybersecurity and limited access to gigantic datasets gathered by Cyber companies is a weakness for theoretical advancement,

[58] Blaikie 2000.
[59] Blyth, Routledge Handbook of International Political Economy (IPE) IPE as a global conversation, 2009. M. Blyth, 2010.
[60] Dunne, 2013.
[61] Franklin D. Kramer, Stuart H. Starr and Larry Wentz, eds., Cyberpower and National Security Washington DC: Center for Technology and National Security Policy, National Defence University, 2009. .
[62] Schreier, On Cyberwarfare, 2015., Schmidt, 2017., Hay, 2019.

but new areas also provide opportunities to test existing theories, as done here, and an opportunity for new theories to be developed, applied and tested.[63]

The scholarly articles and theoretical writings that provide the foundation of this study fall into one of three categories; summaries of peer-reviewed writings on Cybersecurity and IR theory; cited and peer reviewed scholarly articles that further democratic and constructive theory; and third policy reports, interviews, books and op-eds by (former) top-level experts in the field of Cybersecurity and International Affairs.

The study additionally relies on strategic reports, analysis and publications from official sources such as international organizations (UN, NATO, EU etc.), ministries and state agencies, leaked information and finally news reports and op-eds published in renowned news outlets operating under a code of journalistic integrity such as The NY Times, The Washington post, Guardian and London Times to name a few. [64]

The data used for an ideational analysis was provided to authorities by Social Media companies as part of official investigations by democratic nations into Cyber- IIA.[65] The information and data gathered for the study was obtained through books and digital libraries in written, graphic and audiovisual form.

Following an *introduction* of subject, in this chapter the thesis establishes the *methodology* and approach for examination, moving over to *definitions* of main Cyber-concepts. Next it describes the *institutional environment* for International-Cyber-Relations, outlining opportunities and restraints for actors. Next the study examines the actors and what happened, establishing '*a case*' for theoretical examination. Next, I introduce the appropriate IR theory for a broad assessment before, applying a *democratic framework* to identify key social activities that are under threat; introducing Constructive theory and a framework for discursive analysis of ideas and discourse, leading to an outline the main elements at play, summarized findings and conclusions.

[63] Stevens, Global Cybersecurity: New Directions in Theory and Methods, 2018.
[64] Tenove, et al., 2017.
[65] US House of Representatives PSC on Intelligence, 2018.

3 Concepts in International Cyber Relations

Proceeding a discussion of IR in Cyberspace we establish a common understanding of concepts:

3.1 Cyberspace

Cyberspace is a term used to describe a world created by connected computers running on electricity, exchanging information for human consumption.

While there is not much literature within IR theory on Cyber-diplomacy and Cyberpower there is a significant body of work on the subject from other traditions, especially from military theory where scholars have commonly used infrastructure-oriented definitions of Cyberspace such as "the interdependent network of information technology infrastructures"[66]

Cyber- and national security experts have typically focused on the infrastructure and information aspects of Cyberspace, which is reflected in a common definition of Cyberspace as a „*global domain within the information environment whose distinctive and unique character is framed by the use of electronics and the electromagnetic spectrum to create, store, modify, exchange, and exploit information via interdependent and interconnected networks using information-communication technologies*." [67]

While those definitions may work for Intelligence, Economics and Military studies, for a study on Cyber Information Influence Attacks (IIA) this thesis utilizes a broader definition of Cyberspace, one that also includes *Cyber-communication.*

This study relies on a 4 layered model of Cyberspace by Klimburg and Mirtl that has the advantage over most older definitions to account for the social-cognitive aspect of Cyberspace:[68]

- The physical layer, consisting of infrastructure and hardware
- The logical layer, consisting of code and protocols
- The content layer, consisting of information, processes and ideas
- The social layer, consisting of human interaction and understanding

[66] Buckland, Schreier and Winkler 2015:1.
[67] Kuehl, 2009.
[68] Klimburg and Mirtl, 2012.

All four levels must be regarded equally when considering Cyber-security and Cyberthreats, for modern Cyber-interactions flow freely between layers, and issues that arise on one layer affect events and actors on other levels.

This definition that allows for a social and perception/cognition-oriented view of Cyberspace and opens the field for Political/Diplomatic studies of constructed realities and how they affect different actors of Cyberspace, an area of International Relations that's been widely cited, but regretfully under-studied and theorized.[69]

The social-cognitive element of Cyberspace is especially important for this study because modern Cyber-attacks are more than crime on the technical, logical and content layers, they fall under psy-ops and human-computer propaganda. They are socially designed to change perceptions and world-view, often while utilizing weaknesses in human interactions and perception.[70]

With the emergence of Cyberspace as the fourth NATO space and NATO's Secretary General Jens Stoltenberg claiming that Cyberspace "matters as much to NATO as land, air and sea defense" [71] a new dialogue and concepts has arrived on the world arena. This new social-technical dictionary has been somewhat fluid with changes in meanings and labels and endless methods for digital-tele communication and abuses thereof. Cyberspace is a broad term which includes the Internet (www), email, file exchanges, all forms of social media and information sharing.

Cyberspace can both be described as governed by *standards and institutions* on one hand and by *anarchy* on the other. This juxtaposition of Cyberspace will be discussed later in this thesis.

[69] Schreier, On Cyberwarfare, 2015. pp 11. On creation of reality in Suskind 2004.
[70] Pamment, Nothhaft, et al., 2019.
[71] Stoltenberg, Why cyber space matters as much to Nato as land, sea and air defence Jens Stoltenberg on Article 5 and why cyber defence has become core to the alliance, 2018.

3.2 Cyberpower

State *power* in Cyberspace is in most ways similar to the use and structure of power in other arenas whether on land, air and sea or through business, military and intelligence operations, although Cyberpower is undeniably not as tangible and physical in nature.

Power, in Political Science and International Affairs, is commonly defined as the ability for A to exert their will onto B, whether by deterrence, coercion, convincing, charisma or contracts.[72]

Cyberpower follows along very similar lines, with direct physical force being replaced by many forms of Cyber-tactics and Cyber-strategies. Military experts have defined *Cyberpower* as „the use, threatened use, or effect by the knowledge of its potential use, of disruptive Cyberattack capabilities by a state.“[73]

I believe a more fitting definition of Cyberpower are to see it as "the ability to use Cyberspace to create advantages and influence events in other operation environments and across the instruments of power"[74]. This view is broad enough to encompass the non-Cyber effects that this thesis argues, but has the limit of being too military oriented, therefore the definition of Cyberpower used here is to see it as “the sum of strategic effects generated by Cyber operations in and from Cyberspace“ [75]

While other actors than state-actors can certainly possess and utilize Cyberpower, such as large corporation, this definition fits well to the state-centric subject of this study.

Furthermore Cyberpower, according to Shreier, has three major characteristics:

> it is ubiquitous, it is complementary, and it can be stealthy […] nothing generates strategic effect in all domains so absolutely and simultaneously as Cyberpower, because Cyberpower is ubiquitous.[76]

This view towards Cyberpower emphasizes both the social element and the anarchic nature of Cyberspace which shall be discussed later in this thesis. Cyber-strategy is here considered "the development and employment of capabilities to operate in Cyberspace,

[72] „the very reason it is applied to solve the nation’s problems – to coerce, deter, assure, and compel populations in the “human domain.” Sauer, et al., 2017., Carstensen and Schmidt, 2015.
[73] Schreier, On Cyberwarfare, 2015.
[74] Starr, 2009.
[75] Schreier, On Cyberwarfare, 2015., F. D. Kramer, 2009.
[76] Schreier, On Cyberwarfare, 2015.

integrated and coordinated with the other operational realms, to achieve or support the achievements of objectives across the elements of national power." [77]

> Cyberpower is subservient to the needs of policy and strategy is the process of translating those needs into action. Cyber operations take place in Cyberspace and generate Cyberpower, but they do not serve their own ends: they serve the ends of policy. Strategy is the bridge between policy and the exploitation of the Cyber instrument. [78]

Cyberpower is closely related to ideas of *digital diplomacy* and *political warfare*, executing soft power in many forms such as exchanging information, lowering trade barriers through digital means, establishing the rule of law, co-operation and channels of problem solving. Digital diplomacy can be practiced domestically, regionally and internationally. Diplomatic actions can affect progress of projects and terms of trade negotiations, and so can digital diplomatic actions.[79]

Political warfare is defined as "the disruption of another country's public opinion and decision-making" and is a practice that dates back centuries, if not millennia.[80] Seeing Cyberattacks simply as political warfare is, however, a rather simplistic view, for Cyberattacks can mean very severe and life-threatening results for citizens and state security.

Cyber-diplomacy, Cyber-strategy and Internet governance belong squarely to the social layer of Cyberspace while being dependent on and affecting the other three layers. Ultimately, however, all Cyber-activity seeks to influence human action through the social layer in and outside of Cyberspace.

[77] ibid
[78] Starr in Kramer, 2009.
[79] Kuehl, 2009.
[80] Pamment, Nothhaft and Agardh-Twetman, et al., 2019.

3.3 Cybersecurity

Cybersecurity is a complicated concept that has developed alongside Cyberspace itself, with related concepts such as *Cybertorts*[81] and *Cyberthreats*.

Cyberspace is the product of US and European military and science development and as such, Cybersecurity has been at the heart of Cyber operations from the very beginning. Because of these origins Computer scientists and military experts have had a traditionally narrow view towards Cybersecurity, treating it as protection of property, infrastructure and information such as „ the organization and collection of resources, processes, and structures used to protect Cyberspace and Cyberspace-enabled systems from occurrences that misalign de jure from de facto property rights."[82]

I argue that recent developments that include information-based Cyberattacks demand a broader definition that includes *human-computer interaction* and protection from uniquely Cyber enabled attacks on human cognition, as part of Cyber-strategies that intend to influence and undermine democracy. [83]

Klimburg & Mirtle have divided Cybersecurity into five main areas, each of which is typically covered by a distinct government department: [84]

- Military Cyber-activities,
- Counter-Cybercrime,
- Intelligence and Counter-Intelligence,
- Critical Infrastructure Protection and National Crisis Management, and
- Cyber-diplomacy and Internet Governance,

Furthering their argument for the fifth security obligation, Cyber-diplomacy and Internet Governance, they reasoned that in a digitized world traditional forms of diplomacy were insufficient, and that Cyberspace provides opportunities that would be unwise to leave unattended. I find their arguments compelling and argue that further development is needed to secure citizens - and societies - against threats of Cyber-violence. There is a large gray area when it comes to Cybercrime and Cyber-diplomacy with the development of Cyber-law and Cyber-norms still in their early stages.

[81] Crootof defines Cybertorts as „acts that employ, infect, or undermine the internet, a computer system, or a network and thereby cause significant transboundary harm" Crootof March 1, 2016.
[82] Craigen, Diakun-Thibault and Purse 2014, Oct.
[83] Cavelty and Suter, 2009., M. D. Cavelty, 2018.
[84] Klimburg and Mirtl, 2012.

A growing number of definitions for Cyberspace and Cybersecurity acknowledge Cyberspace as more than hardware, software and information and recognize a level that is a unique virtual-space, where interactions take place and where people's ideas are influenced through targeted information-dissemination.

Keeping with the state-centric view of this study and its emphasis on the influence of information on ideas, this study builds upon Canongia & Mandarino's 2013 definition of Cybersecurity by adding the word 'institutions' to it:

> "The art of ensuring the existence and continuity of the information society of a nation, guaranteeing and protecting, in Cyberspace, its information, assets, *institutions* and critical infrastructure."[85]

This definition has the critical benefit of including 'information society' a recognition of a societal aspect which also includes media, public discourse and civil society in Cyberspace.[86]

State centric Cybersecurity has until very recently been primarily focused on the protection of infrastructure, information and financial transactions, that is, on issues protecting property, technology and information, and to a much lesser degree to human-computer interaction and cognition.

Cybersecurity is facing a need to incorporate protection against Cyber-information warfare and creation of false 'Cyber-realities", including distribution of incorrect information and material that's geared to influence humans through the use of psychological means, as will be discussed later in this thesis. This is very much in line with recent actions taken by states, defense alliances and international actors, that are taking steps to include Cyber-information tactics in their responses. [87]

[85] Canongia and Mandarino, 2013.
[86] de Jong, et al., 2018.
[87] Grynkewich, 2018., Jensen, Valeriano and Maness, 2019., de Jong, et al., 2018. NATO, 2018.

3.4 Cyberthreats

The Cyber-threats and Cyber-attackers discussed in this study originate with state actors and serve a *geopolitical* purpose. The origins of Cyberattacks are often difficult to distinguish, which has work to the advantage of those who wish to establish their own Cyberpower.[88] Other crimes are relatively quickly solved. Cyber-criminals are not very different from offline criminals, they all have their agenda, whether working alone or for state actors. Cyber criminals have been categorized into five groups; *vandals, burglars, thugs, spies* and *saboteurs*.[89]

Fred Schreier classifies Cyberattacks into three broad types: *Cyber vandalism*, *Cyber-crime*, and *Cyber espionage* classifying idealistic and cognitive attacks as modern *Information warfare*.[90]

This thesis looks at a specific type of Cyberthreats, ones that take place on the informational and social levels of Cyberspace, committed by state actors

Security scholars have categorized Cyber-attackers into the following groups and motivations: [91]

- **Nation-states** are motivated by economic, ideological, and/or geopolitical interests.
- **Hacktivists** are motivated by ideological issues.
- **Cybercriminals** are motivated by financial profit.
- **Terrorist groups** are motivated by violent extremist ideologies.
- **Political actors** are motivated by winning political power domestically.
- **Thrill-seekers** are individuals seeking reputational or personal satisfaction from successful hacking.

Here, those who operate with the goal in mind to further a state's agenda are called state actors, whether they are a part of larger operations or not and whether they are paid to do so or not.

As part of Cyber-security defenses, security experts predominantly focus on threats to the *confidentiality*, *integrity* and *availability* of data"[92] Copying and leaking data threatens its confidentiality; deleting or manipulating violates its integrity; and encryption or network

[88] Canongia and Mandarino, 2013. Collier, 2018.
[89] Sanger, 2018.
[90] Schreier, On Cyberwarfare, 2015.
[91] Tenove, et al., 2017.
[92] Andress 2011, 4–6 In Tenove, et al., 2017.

disruption can change its availability. In my opinion Cyber-security needs to incorporate a hybrid of Information-Influence defenses with a Cyber-emphasis that addresses Cyber-specific issues.

I argue that there is more to information than just confidentiality integrity and availability, information contains ideas and ideas have an influence off their own. I argue that many Cyber operations fall in-between definitions Cyber-threats and Information-threats and have a deeper influence on world-views because of the opportunities that are unique to the Cyber platform.

The line between Cyber-attacks on information and Information warfare is not always clear. I argue that attacks on the social level of Cyberspace through information-tactics that take place in the fourth dimension and are uniquely Cyber. I argue that they are Information-Cyber tools that belong to a new type of asymmetrical warfare. The subject of this thesis is to examine these threats in a democratic and theoretic context, and therefore we categorize them as fits the subject: application of IR theories on ideas and democracy.

Whether those are classified as information-warfare, Cyber-warfare or multimedia-attacks, for the sake of simplicity those combined information-Cyber-multimedia-influence attacks are here categorized as *Cyberthreats*. Because of their hybrid nature, executed in sync with other Cyber-attacks and utilizing specific Cyber-weaknesses it is impossible to categorize the attacks reviewed here as anything other than Cyber. The Cyber-threats reviewed here require a new approach that accounts for the constructed nature of the medium and the nature of the threats, allowing us to account theoretically to the *constructive nature of Cyberspace*.[93]

It is important to recognize that there is a difference between Cyber-warfare and Information warfare – and that a hybrid of the two falls under the heading of Cyber-attacks. Cyber warfare can include information warfare, and information warfare can be executed in Cyberspace in coordination with Cyber warfare and Information warfare waged through other communications channels. Neither are operations in Cyberspace synonymous with Information Operations.

[93] Schreier, On Cyberwarfare, 2015.

"Information influence activities are here understood as *the targeting of opinion-formation in illegitimate, though not necessarily illegal ways, by foreign actors or their proxies*. This targeting is used to support and amplify diplomatic, economic and military pressure."[94]

Information Operations and Information Campaigns are set of operations by a foreign power that can be performed in Cyberspace and through other communication channels. They are coordinated efforts of an array of Information activities that all work in different ways towards one or more common goals. Operations in Cyberspace can directly support Information Operations, and non-connected Information Operations can affect Cyberspace operations.[95]

These Information Operations could include influencing the decisions of politicians and public officials, public opinion amongst special groups or the public as a whole, attacking political decisions or public opinion in other countries where sovereignty or state interests can be severely affected.[96]

States who seek to advance their power through Cyberspace frequently use hired help or Cyber-mercenaries to execute their agenda as will be discussed later. It can be very difficult to trace the origins and motivations of actors in Cyberspace but several items separate state actors from non-state actors, as defined by Tenove et. al:

> state actors are distinguished from non-state actors by their ability to combine sophisticated Cyber capabilities (either possessed by their own personnel or purchased), extensive intelligence of targets, and long-lasting, multi-dimensional campaigns of coordinated action on multiple fronts […] Moreover, states can coordinate their digital activities with large-scale "non-digital" activities, such as diplomatic campaigns, crack-downs on activists, or military actions.[97]

Because of the difficulties involved in pinpointing the origins of Cyberattacks and because states seek to operate in areas where they can assume plausible deniability, they frequently hire freelancers and finance rouge actors to do their bidding.

[94] Pamment, Nothhaft and Agardh-Twetman, et al., 2019.
[95] Schreier, On Cyberwarfare, 2015.
[96] Pamment, Nothhaft, et al., 2019.
[97] Tenove, et al., 2017.

4 International Cyber-relations

> "The growth of the internet has been characterized by an emphasis on interoperability, efficiency and freedom but our growing reliance has not been matched by efforts to keep it secure".[98]

Before the existence of legally binding documents securing rights and subsequent foundation of institutions to uphold those rights, there was no benchmark or guarantee for human rights in the world. In many areas the same atmosphere applies currently in Cyberspace. Globalization in the 20th and 21st century has also meant global normalization of legal treaties and human rights.

In 1966 the United Nations adopted a treaty that commits the states that sign up to it "to protect and respect the civil and political rights of individuals" - regardless of regime types or whether those individuals are their own citizens or not.[99]

Human Rights treaties have now been ratified by most states on Earth independent from their form of governance; acknowledging that particular human rights are universal and that they apply in monarchies, dictatorships, communist regimes and democracies alike.

The treaties represent norms of peaceful international problem-solving, replacing military force and bilateral negotiations with supranational authorities. These treaties sparked an institutionalization of global rule of law and diplomacy over the past century, further strengthening norms of peaceful cooperation in a form of 'virtuous cycle'.[100]

This trend now involves nearly every single country on earth, bringing with it globalization of democracy and domestic institutionalization of government, including an equivalence of a Ministry for Foreign Affairs that facilitates bilateral, multilateral and international cooperation.

Most countries in the world are parties to the Universal Declaration of Human Rights (UDHR) and nearly all of them allow public Internet access, albeit under known and unknown restrictions. No country offers "all" of the Internet or all of Cyberspace.[101]

[98] Buckland, Schreier and Winkler 2015:1.
[99] United Nations, Equality and Human Rights Commision: United Nations, 2017.
[100] Tenove, et al., 2017. Tavris and Aronson 2007.
[101] McDonald, 2018.

By joining the UN General Assembly and signing the declaration countries agree that "The General Assembly, Proclaims this Universal Declaration of Human Rights as a common standard of achievement for all peoples and all nations" and by accepting it, commit themselves to support the rights. [102]

The declaration represents noble ideals of social justice that have become the global benchmark human rights. Those rights also include Cyber-rights with article 19 of the declaration is considered the key to Internet access and personal freedom online, it states: "Everyone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers."[103]

In addition, the right to become 'a Netizen' or a connected participant in Cyberspace has been campaigned hard by the Internet Governance Forum (IGF) on behalf of the UN and citizens worldwide. Not only do people expect the right to be connected to others in Cyberspace, we also take for granted that certain rights follow us into the space, with other Cyber-rights established as the virtual environment grows and develops.[104]

Human rights are *ideas* who become institutionalized as norms, embedded in physical structures, information and practices. *Global institutionalization* of human rights is a trend that's not fully developed within the realm of Cyberspace. While the ideas shaping Cyber-governance and institutional development are not the subject of this analysis, they represent an environment and serve as a reminder to the power of ideas and how they shape human agency.

[102] United Nations 1948.
[103] United Nations, 2017., United Nations 1948.
[104] Citron, 2014.

4.1 Internet Governance

Cyberspace is innately interspersed and dependent on cooperation. At the heart of its existence lies the successful execution of complex *cooperation*, *procedures* and *protocols*.[105]

The International Community is an increasingly complicated, multilayered network of international, supranational and regional institutions that serve the purpose to solve international problems and facilitate cooperation.

Cyberspace wouldn't function without similar layers of international and domestic institutions of *Internet Governance* that have developed out of needs and strengthening norms for institutionalized problem-solving.[106]

In order to facilitate, maintain and organize the colossal infrastructure that is required for operating Cyberspace, a myriad of domestic and international organizations have been evolved and established in a system of Internet Governance called the *Multistakeholder Model*.[107]

The Multistakeholder Model is important for the discussion of this thesis, for it creates an environment that reveals both strengths and weaknesses of Cyberspace.

The empowerment Cyberspace has meant for operations, knowledge and power-dynamics has created a truly revolutionary change in human societies. On the other hand, those changes have created severe problems relating to Cybersecurity, problems that now are translating into serious threats to democracies themselves.

[105] McCarthy, 2018.
[106] Bradshaw, DeNardis and Hamps, 2015.
[107] Internet Society (ISOC), 2016.

4.2 The Multistakeholder Model

Many of the early pioneers of the Internet operated according to the ideals that scientific discoveries and knowledge are a *public good* that should be used to benefit humankind, similar to the idealistic reasons behind the donation of the Polio vaccine into the public domain. The first generations of 'Netizens', as they commonly dubbed themselves, believe that it is "our responsibility as individuals to preserve an open internet and a free web for the benefit of humankind."[108]

The Internet and Cyberspace are direct products of this ideology of free and open flow of information held by the first generation of internet creators. This environment of free sharing of technical know-how, information and cooperation allowed people to create something greater than the sum or their parts could ever have accomplished. The ideals of information freely belonging to human kind have largely influenced the current institutional setup of Cyberspace, including the establishment of the Internet Governance Forum (IGF) out of the UN umbrella and the Multistakeholder model (see Figure 1 for an institutional overview).[109]

Internet institutions developed responsively along development of the Internet itself, some as internet responsibilities were brought to pre-existing organizations as in the case of telecommunications, while others were founded specifically for the purpose, mostly in the US.[110] Because of their origins and US dominance over Cybercommunications most experts agree that the institutions of the Internet they had a considerable slant towards US interests, while also being predominantly geared to solve problems on the first three levels of Cyberspace, leaving the social level especially vulnerable and under-regulated. As a response countries that wanted to curb US and/or Western influence on Cyberspace pushed heavily for its institutions to belong under the UN umbrella where they assumed their interests would be represented on a more equal footing.[111]

[108] Foster, 2014.
[109] Klimburg and Mirtl, 2012.
[110] Internet Society (ISOC), 2016.
[111] Bradshaw, DeNardis and Hamps, 2015.

Figure 1: The Multistakeholder Model of Internet Governance[112]

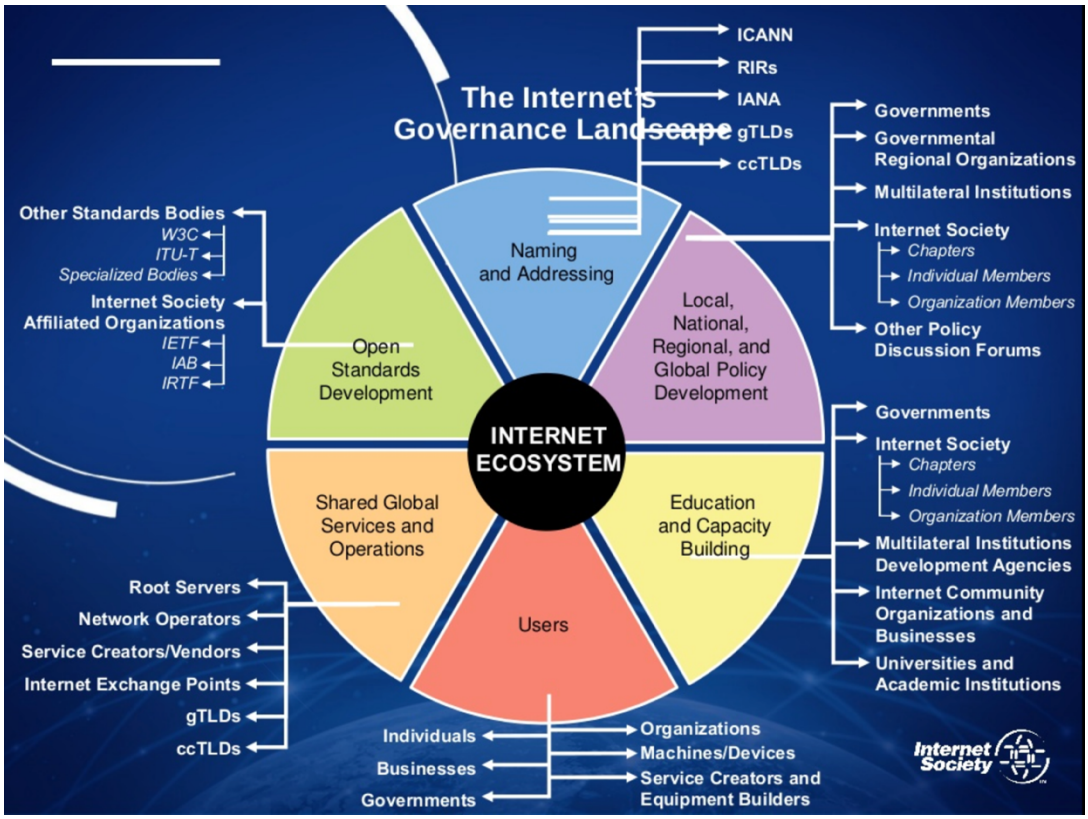


Figure 1 includes an overview of a majority of Internet Institutions with the IGF establishing itself over the last decade as a central forum for Cyber- discourse. The Multistakeholder institutions and the problems they solve show that the organizations operate in a mostly technical and legal area. The 'problem-solving mechanisms' have been evolving according to pathways scholars attribute to Institutional Theory which addresses how practical, legal and normative matters seek institutionalized solutions.[113]

The Multistakeholder model outlines a division of labor where states and private companies all need to address and solve the problems that arise in Cyber-governance, and has for the most part been successful at doing so. The field also includes with a vital epistemic community of experts, political officers, civil servants, corporate interest, journalists and academics. The model is representative but not democratic, with discourse at its core.[114]

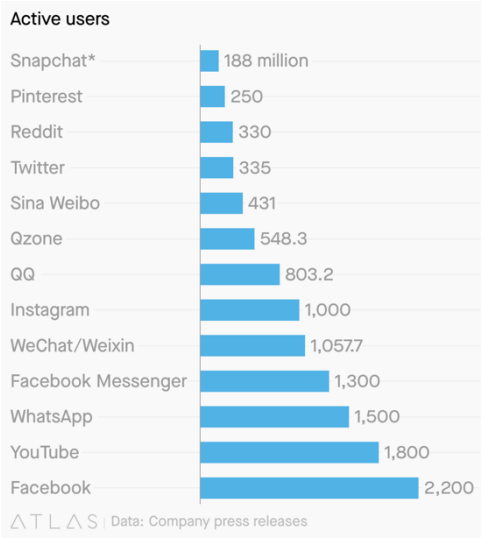
[112] Internet Society (ISOC), 2016.
[113] V. Schmidt, 2008., V. Schmidt, 2011., V. Schmidt, 2015.
[114] Internet Society (ISOC), 2016. Internet Society 2001.

4.3 Social Relations in Cyberspace

Social media has been a part of Cyberspace from its early days of irc and Usenet chat groups, but with the advent of Social Media (SM) outlets like Facebook who owns Instagram, Twitter, Reddit and Youtube public Cyber-discourse is now mainstream with over 3.3 billion users worldwide and, despite being somewhat limited by language barriers, Social Media platforms count as the largest societies on earth.[115]

A staggering amount of crime takes place in Cyberspace and on SM with much need for cooperation with local and international law-enforcement, which again is proving to be a sore subject for the publicly traded SM giants.[116]

Figure 2 - Active Social Media Users 2018



Service providers are bound to follow domestic law and international treaties while defining their service and operations according to their own Terms of Service (ToS), which in theory are subservient to law and treaties, but in practice reveal large failings in SM operations and local law-enforcement.[117]

Cross-border monitoring, reporting and prosecution of crime is a particularly big problem; staff members in one country are supposed to understand and make decisions on user-reported and auto-flagged posts in a different langue, often failing users miserably in the process, particularly women and other groups that are vulnerable to torrents of online hatred.[118]

Users have repeatedly pointed out that not only are service providers breaching their own ToS and not acting in accordance with local law, their lack of cooperation with law-enforcement poses a physical danger to citizens.[119]

[115] Brandwatch, 2019.
[116] The Daily Mail, 2012.
[117] Waters, 2012.
[118] This author was personally targeted by trolls in 2013 and received an formal apology from FB after repeated unsuccessful attempts to get rape threats and violent imagery removed Hudson, 2013. .
[119] Zabrisky, 2017.,

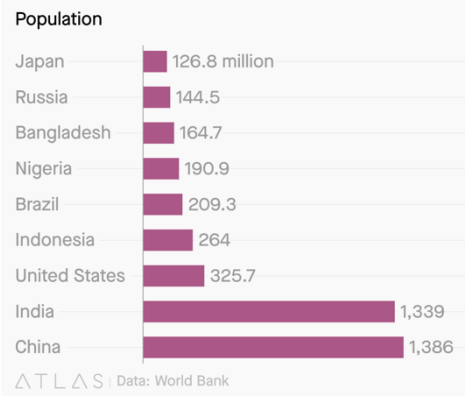


Figure 3 - Cyber Users by Country 2018

Following the developing world entering and enlarging Cyberspace by the billions came increasing demands from states, stakeholders and civil organizations for consideration and inclusion of their Cyber related concerns. [120]

Those concerns included allegations of governments exerting improper influence over 'the free web', particularly including illegal monitoring and espionage.[121] Preparing for those changes, in 2009 US military assessed the dangers of institutional changes in Cyberspace and made a list of entities that would likely benefit from changes from the previous institutional model: individuals, hacktivists, non-governmental organizations, terrorists, transnational criminals, corporations, nation-states, and international governmental organizations such as the European Union and United Nations.[122] Unsurprisingly, all of those groups were actively working towards increased institutionalization and respect for international law, while maximizing their own position.

One of the largest data-leaks ever reported took place in 2013 when several news outlets led by the UK newspaper Guardian published information they obtained through Edward Snowden, a US whistleblower, on extensive, intrusive, illegal and lawless surveillance practices by the US and UK governments targeted towards individuals, industries and world leaders.[123]

The leaks revealed massive systematic state-surveillance[124] in addition to various breaches of user privacy on behalf of private companies[125], particularly by the largest SM platforms which house a predominant portion of world's public and political debate.

[120] Internet Society (ISOC), 2016. NATO Cooperative Cyber Defense Center of Europe CCDCE, 2019.
[121] Bradshaw, DeNardis and Hamps, 2015. Higgins, 2016. Kramer, Starr and Wentz, 2009.
[122] Starr, 2009.
[123] Macaskill and Dance, 2013.
[124] Francheschi-Bicchierai, 2014.
[125] Ashford, 2014.

The leak furthermore revealed serious shortcomings of Cyber-law, large areas appeared lawless while other activities that were arguably illegal according to state law were not covered or enforceable by international laws and treaties.[126]

Demands for amendments to local law, international treaties and respect for sovereign rights arose immediately, including an outcry in public debate for guarantees of an Internet free from state interference.[127] With the overwhelming evidence provided by the leak those demands became too loud to ignore, leading, after much debate, to amendments and the birth of the current Multistakeholder model of Internet governance and amendments to Cyber-law such as the Tallin 2.0.[128]

The Multistakeholder governance framework is informed by three components:

a) opened-ended unleashed innovation (infrastructure),

b) decentralized governance institutions (governance) and,

c) open and inclusive processes (human). […]

The Internet Society has developed four attributes of successful multi-stakeholder decision-making to guide the next phase of its evolution: inclusiveness and transparency; collective responsibility; effective decision-making and implementation; collaboration through distributed and interoperable governance. [129]

These 'multi-stakeholders' are a motley crew of state actors from developing and developed countries, private and publicly traded corporations, and non-governmental actors, including charitable actors and an epistemic community with deep roots in human rights studies.[130]

Citizen influence and participation in those institutions is limited to say the least, predominantly taking place through contributions by epistemic communities and non-democratic forums.[131]

The Multistakeholder Model falls extremely well to models of rational-institutionalism, it officially promotes Internet neutrality and inclusiveness in decision, being

[126] NATO Cooperative Cyber Defense Center of Europe CCDCE, 2019.
[127] Reuters - The Guardian, 2015.
[128] R. Deibert, 2015. Crootof March 1, 2016.
[129] Internetsociety 2001.
[130] Crootof March 1, 2016.
[131] Bradshaw, DeNardis and Hamps, 2015. R. Deibert, 2015.

ruled by both state-designated forums and an epistemic community of experts, who theoretically have benign goals and no special interests governing their decisions.[132]

While the ideals of the model are lofty, in practice governing Cyberspace is a daunting task. This is demonstrated by countless examples that show private actors and state's deliberate actions to abuse their power for various ends, such as to curb opposition and tighten reigns over domestic discourse through an assortment of digital tactics.[133]

The model has surely been able to resolve many issues in theory, however dispersed jurisdiction and division of responsibilities between various governing bodies makes resolving issues a daunting ordeal particularly for small and developing states. Only states with considerable diplomatic and technical resources have the capacity to represent and execute a broad Cyber-strategy, which creates a very uneven plain field on an issue of such importance.[134]

Cyber-diplomacy is an area that's maturing fast with states and stakeholders using every resource available to further their agenda. This includes hypocrisy at the highest level, where some states push for institutionalization and the rule of law where it suits their purpose, while forcefully fighting such avenues when it doesn't. [135] This has resulted in alliance forming, similar to institutional developments in other fields, with developing states and those of weaker Cyberpower staking their bets on institutional resources, while more powerful players resort to founding their own Cyberspace similar to Chinese, Russian and Brazil.[136]

Over the past few years there has been marked increase in acrimonious behavior in Cyber Diplomacy, particularly noticed in tension between state actors.[137] Stakeholders have fought to keep their place at the table and the old principles of freedom still hold strong amongst representatives, however in this social field of Cyberspace there are serious signs that Cyber-torts and 'minor' Cyber-attacks, have escalated into systematic state aggression:

> No other areas of IR have been marked by such a pronounced shift from relatively simpl[e] coordination problems to a challenging hybrid of cooperation problems alongside complex coordination problems characterized by large numbers of players with divergent

[132] V. Schmidt, 2008., V. Schmidt, 2015., M. Schmidt, 2017.
[133] R. Deibert, 2015.
[134] Bradshaw, DeNardis and Hamps, 2015.
[135] Crootof March 1, 2016.
[136] Buckland, Schreier and Winkler 2015:1.
[137] Bradshaw, DeNardis and Hamps, 2015., Internet Society (ISOC), 2016.

> preferences over the available equilibria. The emergence of contention in Internet governance is, therefore, a novel problem with potentially large implications for successful governance of the Internet. These include destabilization of the Internet governance ecosystem and the threat of various forms of Internet fragmentation. Typically, states have dominated in cooperation problems, raising troubling questions about whether the private sector-led multi-stakeholder approach can survive in this context. [138]

The Centre for International Governance Innovation, formerly the Global Commission on Internet Governance, is an independent international think tank dedicated to 'International Governance Innovation' at the highest level. Its experts foresee three possible futures for Cyberspace;

a) a dangerous and broken Cyberspace where malicious activity and criminal rule

b) a fragmented Cyberspace where regions wall themselves in, resulting in uneven and unequal gains

c) broad access to Cyberspace, resulting in unprecedented progress of all through utilization of global potentials.[139]

This thesis heeds the call for political scientists to study current affairs in order to contribute to international stability and state's domestic security, *one that normatively includes continued peaceful democratic governance and allied institutional cooperation for a free Cyberspace*.[140]

[138] Bradshaw, DeNardis and Hamps, 2015.
[139] Global Commission on Internet Governance, 2019.
[140] Starr, 2009.

4.4 Cyber Law

The advent of Cyberspace has caused problems for individuals, companies and states alike, with Cybercrime becoming a major issue around the world. Institutions of the Internet are still working to respond to the need to regulate those issues.

Two main treaties cover crimes and rights in Cyberspace; The Budapest Convention and Tallin 2.0.

First, the 2004 *Budapest Convention* on Cyber and property crime which "serves as a guideline for any country developing comprehensive national legislation against Cybercrime and as a framework for international cooperation between State Parties to this treaty"[141] The Convention outlines a framework for domestic legislators to follow to update their law and enable the legislation of Cyberspace. That process can take time and have obstacles of its own on the way to becoming legally binding obligations.

> Despite domestic and international law covering large areas and forms of Cybercrime, they still provide significant loopholes. Add to that technical and legal difficulties tracing criminal activity back to its source, acquiring evidence and bringing forth legal cases across borders. „In general, international law on Cyber-operations (both hacking and information operations) is disputed, imprecise, and lacking in meaningful enforcement"[142]

The second main legal framework for Cyberspace is the 2013 *Tallinn Manual on Cyber Operations*, followed by *Tallinn Manual 2.0* in 2017 which is the only manual of its kind on International Law Applicable to Cyber Warfare.

Though the Manual is extensive, it has significant undeveloped areas and loopholes. It has furthermore proven hard to suffice burden of proof and track the origin of attacks back to state aggressors, especially for stakeholders of weaker means. There is additionally a marked reluctance amongst stakeholders and governments to address some problem areas, leaving areas of maneuver.[143]

[141] Council of Europe 2004/2019. Buckland, Schreier and Winkler 2015:1.
[142] Crootof March 1, 2016.
[143] Crootof March 1, 2016. R. Deibert, 2015.

> The *Tallinn Manual on Cyber Operations,* arguably the most influential guide on international law in this issue area, proposes that Cyber violations of sovereignty require either a coercive intervention in the *domaine réservé* of a state, or the "interference or usurpation of inherently governmental functions" (Schmitt 2017, 20).
> However, information operations like those pursued by Russian in the US 2016 elections may not meet these criteria (Crootof 2018; Ohlin 2017). It is thus generally recognized that there are major gaps in international norms and laws to address such threats. [144]

This leaver a large area of law-less-ness when it comes to Cyber activities. Cyber-attacks and Cyber-aggression have become a part of Cyber-statecraft over the past decades with initial dominance and aggression laying with by the US and joint NATO operations, but a steadily leveling playing-field emerging as worldwide governments acquired resources and started executing their own Cyber-strategies. [145]

Security and protection against danger has always been a major issue for any human society. Humans have come to accepted general security reality that we live in a world of uncertainty and risk, we cannot prevent all disasters, but we can take precaution and prepare. The same acceptance is applied to Cybersecurity; most security plans accept that breaches will happen, and that very likely systems might go down until control is re-gained again. States have come to accept that Cyber-breaches will not be totally prevented, so the strategy is to minimize damage and down-time if and when the inevitable happens. Some security-experts even claim that Cybersecurity has become ritualistic and 'a self-fulfilling prophecy' in its preparations for some unlikely events and not more likely breaches relating to the human element, a mostly neglected area.[146]

Most governments have been cautious asking citizens to prepare themselves for Cyber-disasters or even to properly incorporate Cyber-security into their lives, with exceptions such as a recent call from the Swedish government to update national preparedness for what to do in case of modern war.[147]

The Cybersecurity strategy of states, private companies and citizens alike mostly evolves around routine protection such as updates, password protection and anti-malware software, and contingency plans in case something happens like safe and frequent backups.

[144] M. Schmidt, 2017.
[145] Bradshaw, DeNardis and Hamps, 2015.
[146] Stevens, Cyber Security and the Politics of Time, 2010. Deibert and Rohozinski, 2010.
[147] Noack, 2018.

States setup legal ramifications outlawing harmful practices, often neglecting the *practical impossibilities* involved in the process such as identification and extradition.[148]

Just like most government aren't actively in armed conflict with their neighbors, most countries are not actively seeking to weaponize themselves in Cyberspace, focusing their strategy to protection from attack, minimizing economic damage, and support to law-enforcement and defense operations.[149]

Withholding major attacks, Cyber-users put their trust in the protection of private service providers, whether it be a bank, the government, online shopping, subscriptions or gaming environments. Lawsuits against Cyber-criminals are rare and unlikely to bring justice to harmed parties, more likely they bring unrecoverable cost.[150]

Most studies of Cybersecurity traditionally view the subject in line with a self-protection-focused standpoint on state security and physical protection attributed to Realist IR theory, however recent changes in Cyberattacks and their effects require an adjustment in that view as will be discussed later in this thesis.

This stand has meant a substantial public-private institutionalization and cooperation on Cybersecurity where private companies, tasked with their own protection, provide governments with much of the know-how, procedures and execution of state security.[151]

The state has not shouldered the role of 'Cyber-policing' in a similar manner to physical protection within its boundaries, but that may change as the field is still being developed, predominantly based on *needs* and experienced *threats*.[152]

The general conclusion of this examination is that democracies have few choices for legal defense in Cyberspace but to participate in international institutionalization such as the Multistakeholder model and legal treaties, and rely on private companies to fulfil security services on technology, code and information, with each user operating 'at their own risk' as will be discussed next.

[148] Crootof March 1, 2016.
[149] Stevens, Cyber Security and the Politics of Time, 2010. Buckland, Schreier and Winkler 2015:1.
[150] McCarthy, 2018.
[151] Crootof March 1, 2016. McCarthy, 2018.
[152] Cavelty and Suter, 2009.

4.5 Social Media and Privatized Public Discourse

Social Media evolves around discourse and it takes many forms, from short video clips to memes, news links and political discussions to game-societies, academic and professional groups and epistemic communities on endless subjects. Unlike news outlets and other content distributors SM's business model is to get paid for publishing ads next to content that users themselves post. Social Media relies users to provide the content themselves, unlike online-ad services that allow companies to place ads next to third party content.

In its simplest form it can be seen as a platform for paid and unpaid material that's either created by users themselves or re-shared from other sources. In its most sinister form Social Media is seen as a self-identifying advertising machine where user content is the bait and the users themselves have become the product.[153]

When people open a website or click a link their history follows them through cookies, little bits of programming that identify users and enable sites to personalize people's internet and target users for specific content. Cookies connect our browsing history and our information to our names and pictures. The cookies are intended to push web-content to people that they might be interested in but how they put people into target-groups is flawed and can create strange versions of the internet based on people's search and history. No two users see the same material and users that see a lot of information on emotionally charged content can easily get trapped in a very emotionally trapped version of the internet. [154]

The SM business model allows advertisers to buy their way into people's 'content-bubbles' where the same material gets pushed towards users over and over again, who then marinate in that message, often unaware that they are not seeing the same part of reality as other people are, and that they, as the product, are now seeing web-content that somebody else wants them to see.[155] When content-bubbles that re-enforce political messages go unchecked they can have significant effects on people's worldview as will be discussed later in relation with theory.

[153] Hodge, 2018.
[154] Tenove, et al., 2017. Wardle and Derakhshan, 2017.
[155] Walsh, 2011. Pomeranzev and Weiss, 2013.

Because SM evolves around human communication it is also forced to deal with a myriad of problems that arise in between humans, a sort of digital policing, a role that has been a struggle for the companies to adjust to.[156] Women and minorities are a frequent target for harassment and hate despite a promise of a harassment-free environment in Social Media's Terms of Service. During the first years of Cyberspace and SM limited progress was made by service providers to protect users from unwanted and harassing content.[157]

Facebook started a reluctant acceptance of its responsibility to process harmful content on behalf of its users and to assist law enforcement following a public campaign addressing Facebook's advertisers criticizing the company for its mistreatment of posts that involved murders and violence.[158] User's complained that death threats and distribution of personal information and harassments were frequently not dealt with, and that too often the company failed to alert law enforcement of possible violent users and in bringing criminals to justice. Up until 2016 many social media companies mostly dealt with hateful content as a first amendment right that applied globally and still today strongly opposes any law or regulations on their "editorial responsibilities".[159]

Historical evidence and academic studies show that people's words are an indication of how people will act in the future and Artificial Intelligence (AI) has become very good at identifying and flagging dangerous dialogue, giving monitors the ability to give law-enforcement agencies a notice of possible violent offenders in their area. The employees that process these reports of inappropriate behavior on social media have been allowed to make unsupervised judgement calls on these instances which has resulted in repeated failures in detection and investigations of criminal cases. For example, FB did not consider Cyber-stalking or death threats as serious indicators of future harm and parts of a larger pattern, something the social media giant has now accepted is a part of a larger pattern after mass-shooters have repeatedly used the platform to distribute their hateful message.[160] Meanwhile Social Media companies have been repeatedly accused of not following their

[156] Sandberg, 2019.
[157] Facebook, 2019. Bisen, 2019.
[158] Hudson, 2013. Citron, 2014.
[159] Citron, 2014. Bisen, 2019. Fowler and Esteban, 2019.
[160] Kayali, 2019. Sandberg, 2019.

own ToS and not shouldering the responsibility that comes with hosting human interaction.[161]

Add to human users the problem of fake accounts and (ro)bots that scan user's account for information and post automatic messages on 'walls' and groups. The problem of chasing origins of Internet content is too much of a task for any organization to handle, social media companies have tried to estimate how much of their content is created by bots and fake accounts and reluctantly released more after the 2016 attacks.

Conversations on social media are frequently affected and manipulated by automatic scripts called bots that react on certain type of discourse, Twitter has estimated that around 8% of its users are bots, while Valor's extensive studying of discourse and misinformation in social media suggest that at least 15% of active Twitter accounts as bots.[162]

Through the help of self-identification and market analysis people have been categorized into market segments based on location, language, education, race, religion, interests, along with technical information on type of gadget, location etc. Cyber-marketing executives rely on this user data and send specific users customized messages to influence user behavior across the world, usually for monetary purposes but to a growing degree also political. This is a problem for transparency regarding election spending and shields foreign governments and law-breakers from the accountability that democratic transparency includes.

Evidence shows that SM companies have been very reluctant to work with governments, on revealing political spending, the origins of purchases and content or monetary transactions unless directed to do so by legal authorities. [163]

As a general tendency SM companies have pushed a model of self-governance and been extremely reluctant to work with governments, rejecting attempts at regulation. With SM operating in a partial state of law-less-ness governments are forced to use parliament hearings to get information and have a discourse with SM giants.[164]

[161] Kayali, 2019. Ivanova, 2018.
[162] Valor, 2017. Bisen, 2019.
[163] Spence and Di Stefano, 2019. Cadwalladr, 2018. Frenkel, et al., 2018. Bisen, 2019.
[164] United Kingdom Parliament Committee, 2018. US House of Representatives PSC on Intelligence, 2018.

4.6 Cyber-Insecurity

This environment paints a picture of *a constant state of insecurity* for Cyber-citizens and states. Users consider themselves taking a calculated risk when logging online, unsure if their personal affairs are private, whether their financial transactions are secure and whether the information they receive is accurate. For example, information whether to evacuate or stay put during a national emergency.[165]

On top of a constant state of uncertainty there are several things that contribute to a perceived 'unrealness' of Cyberspace. Because of the nature of the medium people treat information from the Internet more callously than information received from print media, tv or books.[166]

> Citizens with less digital literacy are less able to assess trustworthiness or origins of digital messaging and are more prone to manipulation. Even digital natives struggle to determine which news sources are fake and which ones are real (Stanford History Education Group 2016; Stecula 2017). Since coordinated or algorithmic production of content means that the same misleading news stories appear on many different sites, readers can falsely believe they have verified information by checking against multiple sources (Rojecki and Meraz 2016; Sollenberger 2017). [167]

Telling untruths and speaking without a filter is a Cyber-security-norm. People feel safe to say and do things in Cyberspace they would not do as easily face to face because of the (perceived) impersonality of the communication and because most Cyber-actions come without repercussions. This callousness is a clear Cyberthreat. People fall prey to online scams and letters from exotic princes in need of assistance but specifically to targeted (spear-) phishing attacks and doxing, when somebody has gathered SM or private information on somebody to extort, hack or use them.[168]

Users have become used to their passwords being leaked, they rarely read Terms of Use and are de-sensitized to Cyber-companies claiming ownership and downloading their (semi-) personal pictures, sharing private messages with the highest bidder. Third parties have access to user's cloud-stored files, their face scanned, and DNA info shared and even

[165] Buckland, Schreier and Winkler 2015:1.
[166] Crootof March 1, 2016.
[167] Tenove, et al., 2017.
[168] Citron, 2014. The Daily Mail, 2012.

their telephone records and location records accessed by the government via backdoors into systems. [169]

When breached, Cyber-users have few options other than market-exit when they receive news that their 3G/4G phone is a source of constant location and possible audio and video surveillance[170], or that their purchased connected electronics are under foreign control and are being used to take part in coordinated attacks on their own governments.[171]

Users are dangerously uninformed about Cyber-vulnerabilities and the information data companies own on them. User information is one of the hottest commodities of Cyberspace and is of monumental importance for people's privacy.[172]

The human element is an extremely underestimated area of Cybersecurity where much more attention and education is needed. Hacks frequently involve extremely simple methods like trying the default password on a service or gadget which in turn can be used in a Cyberattack against a third party.[173]

> Citizens often fail to follow adequate Cyber-security practices, as do individuals in political parties, civil society organizations and government agencies. In addition, as Herring et al (2011, 381) note, trolls often "prey on inexperienced Internet users and populations that are vulnerable for other reasons."
> Additionally, many states lack the technical and regulatory capacity, or lack the willingness, to identify and prosecute actors who violate domestic and international Cybercrime laws. [174]

The evidence suggests that there is much work to be done in the institutionalization of Cyberspace and that the current atmosphere is causing significant problems for users, businesses and governments.

[169] Obar and Oeldorf-Hirsch, 2018., Frenkel, et al., 2018.,
[170] Douglas, 2017.
[171] Casey, 2016.
[172] Ivanova, 2018.
[173] Casey, 2016.
[174] Crootof March 1, 2016.

4.7 Anarchy and what states make of it – Realism vs. Institutionalism

> Once free virtual space, advertised as a prototype of the coming paradise, [has been] captured and demarcated by Cyberpolice and Cybercrime, Cyberweights and Cyberspies, Cyberterrorists and Cybermoralists.[175]

The nostalgic notion of early Cyberspace as some sort of a Cyber-Eden where idealistic computer-geeks roamed free in their benign quest for a better technical future is incorrect and incomplete. A good portion of the people that formed Cyberspace together through cooperation held simplistic views on human activities and naively misjudged the downsides of lawlessness.[176]

There is a strange duality in Cyberspace where on one hand it includes disciplined technical and structural frameworks that follow rigid standards and programming-languages, when conversely the state of human interaction and organization within Cyberspace demonstrates many attributes of anarchy.[177]

As discussed, Cyber-aggression and Cyber-attacks have been hard to translate into lawful text that states, organizations and individuals can rely upon for protection against harmful act and currently "our information landscape is ripe for misuse."[178]

Over the past decade increased contention has marked the power battle between state actors arguing for a state-controlled Internet via UN governed organizations on one hand and on the other champions of the Multistakeholder Model that fight for an independent Internet of non-state actors.[179]

Experts agree that despite the creation of the Multistakeholder Model and an international consensus of a free and open internet, there is an undeniable power-battle within the forum of Internet Institutions with states playing dual strategies and paying lip service to common goals. Every month new threats arise, and novel battles take place, for example with AI, the Internet of Things (IoT), DeepFake videos and Space-War, areas and examples that again need to be addressed and analyzed by IR scholars.

Cybersecurity is currently in an "uneasy equilibrium between war and peace".[180]

---

[175] Surkov, 2019.
[176] Bradshaw, DeNardis and Hamps, 2015.
[177] Crootof March 1, 2016. Wendt 1992.
[178] Pamment, Nothhaft and Agardh-Twetman, et al., 2019.
[179] van Eeten and Mueller, 2012.
[180] Sanger, 2018.

The problem with anarchy is that aggressors tend to abuse the system, which creates an unsafe atmosphere for everybody. Insecurity in turn has an effect on user's behavior and the norms of Cyberspace, creating an atmosphere of distrust and self-protection, as theorized by Gomez and Villar: "The phenomenon of dread in Cyberspace is a confluence of the domain's inherent characteristics and individual cognitive processes."[181]

The Sovereign Principle is a norm above all others in International Relations.[182] Violating the principle by interfering in political activities across state lines can amount to a breach equal to a declaration of war according to international treaties, with domestic law treating acts detrimental to state interest as High Treason, crime only equal to murder, punishing violators with the severest of punishments. Additionally, democratic states have passed regulations that are aimed to protect democratic processes with domestic law covering a wide spectrum of political behavior from transparency regarding campaign finance and political advertisements to secret clearances and codes of conducts for elected officials. [183]

States have frequently been stricken a blow by attacks in or through Cyberspace, but have been stumped in their responses, typically unsure whether to respond in kind or out of the specific arena through other channels.[184] While the Rational -Institutionalist solution has been to enter into treaties and organizations, the hurdles still facing those seeking justice or retributions prove to be overwhelming, making Cyberspace an inherently insecure space.

Cyber-aggression has not had the same consequences as similar acts in other arenas, partially because traditional definitions from the physical space don't translate well to Cyberspace, and secondly because states holding great Cyber-power have been reluctant to agree on conventions and international law, preferring a state of anarchy, plausible deniability and responses out of the Cyber-arena.[185]

[181] Gomez and Villar, 2018. Wendt 1992.
[182] Crootof March 1, 2016. Bradshaw, DeNardis and Hamps, 2015.
[183] NATO Cooperative Cyber Defense Center of Europe CCDCE, 2019.
[184] D. E. Sanger, 2018., Miller, Nakashima and Entous, 2017.
[185] Miller, Nakashima and Entous, 2017.

> States are not being held accountable for the vast majority of their harmful Cyberoperations, largely because classifications created in physical space do not map well onto the Cyber domain. Most injurious and invasive Cyberoperations are not Cybercrimes and do not constitute Cyberwarfare, nor are states extending existing definitions of wrongful acts permitting countermeasures to Cyberoperations (possibly to avoid creating precedent restricting their own activities). Absent an appropriate label, victim states have few effective and non-escalatory responsive options, and the harms associated with these incidents lie where they fall.[186]

Cyberspace is international yet its legal resources are domestic, which creates huge obstacles for countries. Add to that the technical and regulatory inability of weaker states to track, confront, prosecute or seek restitution from Cyber-attackers that trace back to other state actors. Take for example the Russian hackers that are being charged and sentenced *in absentia* in the US for Cyber-crimes.[187]

Multistakeholder model's institutional setup and aims are designed to prevent escalation of Cyber-aggression, but at the same time its distribution of power is proving to be a hindrance for order and peace in Cyberspace.[188]

As means of protection states have been forced to develop an arsenal of appropriate responses to Cyber-aggression, both domestic and in alliances, due to the very real danger of escalation.[189]

In 2016 the G7 states agreed on the Lucca 'Declaration on Norms for Responsible State Behaviour in Cyberspace', an agreement on responsible and ethical state behavior in Cyberspace that is intended to minimize the risk of cyber-war escalating into physical conflict, but does not include any legally binding clauses, rather is a re-iteration of legal obligations and peaceful intent in Cyberspace. [190]

The strategy to respond to Cyber-aggression with a range of diplomatic, financial, legal and tactical responses has been strengthening over the past few years but the topic has been far from simple. The development to respond out of the Cyber-arena is strengthening norms and tools that belong in the category of asymmetrical warfare where state weapons and tact are stressed to the borders of imagination.[191]

---

[186] Crootof March 1, 2016.
[187] Mueller, 2019. United States of America, 2018.
[188] Wardle and Derakhshan, 2017. Bradshaw, DeNardis and Hamps, 2015.
[189] Miller, Nakashima and Entous, 2017., Gomez and Villar, 2018., Jensen, Valeriano and Maness, 2019.
[190] Center for Cyber Security and International Relations Studies 2017
[191] Pamment, Nothhaft, et al., 2018. Carroll, 2019.

4.8 Cyber-Space: Anarchy, Chaos and Dis-Order

Classic realist models of zero-sum international political relations are making a comeback in Cyberspace after a relatively long period of peaceful multi-stakeholder institutionalization of all things Telecom- and Cyber- in line with Institutional Theory. [192]

Realist theory of power politics and peaceful *Institutional* theory of cooperation provide convincing insights into the development of Cyber International Relations. Humans tend to organize themselves and create security alliances in order to deal with aggressors and the creation of Cyber-law, international treaties and institutions is one such development

The work on Discursive institutionalism is particularly influential in explaining this development because it includes many of the discursive and constructive elements that apply to Cyberspace and its institutionalization through the Multistakeholder model.[193]

Superpowers like Russia, USA and China typically adhere to realist power positions and have in many cases tried to minimize the role of globalization and maximize the state centric view, only participating in international institutions where it suits them, leaving other areas unregulated and vulnerable.[194] Conversely institutionalists are striving to create order through law and cooperation, maintaining that isolationism and mistrust creates costs that are too high to bear.[195]

Countries that don't accept the current US-Europe dominated Cyberspace are actively working on creating Cyber-environments and rules of their own similar to the Asian RATS SCO alliance against terrorism, including Cyber-attacks.[196]

While smaller states seek international cooperation many large countries see their interests best served with Cyber-Isolationism; China is running its own internet surrounded by „The Great Cyberwall of China", Brazil has started plans to establish an independent South-American Internet free from Western interruption and most recently Russia took itself offline momentarily in order to protect itself in case of Cyberwar. [197]

[192] Gomez and Villar, 2018.
[193] V. A. Schmidt, 2010., V. Schmidt, 2008., V. Schmidt, 2015 (2).
[194] Bradshaw, DeNardis and Hamps, 2015., Crootof March 1, 2016.
[195] Hay, 2013.
[196] The Regional Anti-Terrorist Structure of Shanghai Cooperation Organization, 2017.
[197] Agence France-Presse Moscow, 2019.

Simultaneously, rational interest-based actions seem to have governed much of state-behavior in and through Cyberspace with democracies, particularly USA, pioneering a strategy that can be described as offense is the best defense.[198]

News on upwards of 200 state-on-state Cyber-attacks have been published in the last decade but the real number of attacks is much higher than that. A decade ago only a handful of nations had effective Cyber forces but due to low startup capital and increased need for protection these players are now around 30, with USA employing 6000 dedicated workers in a 21st version of a Cyber-army. Now there are seven countries considered to be aggressively participating in Cyber-operations of Cyber-conflict: USA, UK, Russia, China, Iran, Israel, North-Korea.[199]

Most NATO countries now acknowledge publicly that they have been subjects of cross-border Cyber-attacks, stating that the most serious attacks are other state actors, particularly naming China as an actor in defense- and military related Cyber-violations with the bulk of attacks traced back to Russian private and state-actors. [200]

This type of aggression is not new, some form of these tactics has been known throughout history, but what is new is the simultaneous extent and depth of attacks in a new 'space', with tactics that sound more like spy novels or conspiracy theories rather than reality. There is a lack of clear international norms or laws regarding Cyber-interference in elections, and therefore challenges in collective action to address the problem.[201]

Hacks and hostile activities have been confirmed by officials, private companies, media outlets and whistleblowers who took part in the operations and have described them in detail.[202] Those activities would for example be hacks done through spear phishing that traced their way into closed systems, acquiring data, changing data, then following came ‚controlled leaks' of information and misinformation, spear-phishing operations, dDos denial-of-service attacks, Troll armies, fake news outlets, fabricated reports, fake news and

[198] Sanger, 2018. Starr, 2009.
[199] Sanger, 2018.
[200] Wardle and Derakhshan, 2017. Zarate, 2017.
[201] Crootof March 1, 2016. Tenove, et al., 2017.
[202] O'Sullivan and Griffin, 2019.

even viral campaigns designed to silence women during the #metoo movement and Kavanaugh hearings.[203]

In the global war for Cyberpower actor's beliefs influence actions. A dog-eat-dog view of a scary world is commonly contributed to realism. It is a world where one state's gain is another state's loss and one state's loss is another state's gain. This view fits tightly alongside typical realist views of the state that see the state as a republic that in itself is more than the sum of its parts.[204]

Realism is often contrasted with the view of cooperation held by institutionalists and many followers of deliberate democracy who argue that peaceful cooperation and communication as part of negotiations is the most sensible strategy. This is a rational-liberal standpoint that tends to view the state as an extension of the will of the people, surely more than the sum of its part but designed to protect the rights and interests of its citizens.[205]

IR theory is here receiving an input from International Political Economic (IPE) Theory (with a capital T) and Ideational studies, rejecting the consensus that had converged out of the realist-institutionalist debate of rational self-interest seeking motivations of states and agents. Ideational studies connecting Cyber-discourse and citizen behavior to real-world data, that's currently gathering in countless, ginormous Big-Data databases all over the world, offer modern scholar's unique opportunities with the human psyche available for analysis and manipulation to anyone with the intelligence and resources to utilize it.[206]

International Relations revolve largely around power politics and while International strategies, programs vary to some extent depending on current state leaders, foreign policy and the relations of nations are remarkably stable and follow a pathway of increased institutionalization and rule of law.

There are, however, actors and situations that provide ample opportunities for great change, for example through elections. The US and French presidential elections provided such opportunities, and similarly the UK referendum on Brexit in June 2016 after several years of debate is another such junction of great change.[207]

---

[203] Petriczko, 2019. Grimes, 2017.
[204] Wendt 1992.
[205] Hay, International relations theory and globalization, 2013.
[206] Cohen, 2009.
[207] Tenove, et al., 2017.

There are sure signs that confirm that elections and important democratic junctions have been specifically targeted recently. Those attacks have been traced to Russian fronts and state operations, albeit formally denied by Russia. Unofficially however the Russians seem rather proud of their success.[208]

After a 'test run' in Ukraine during the annexation of Crimea Russian institutions focused on Western targets, for example with targeted hack and misinformation attacks on the Brexit referendum. Also, in the US by hacking and leaking information on Hillary Clinton and the Democrats during critical points in the US presidential campaign. Hillary Clinton has no doubt that Russia got Trump elected[209].

Tenove et. Al's synthesis of existing research suggests there are five key vulnerabilities to Information Influence Attacks:

- deficits in citizens' digital literacy and data protection,
- polarized political cultures and media systems;
- problematic social media design and policies;
- inadequate electoral and criminal regulations;
- inadequate international norms and laws on Cyber interference.

These vulnerabilities affect different political systems in different ways, and comparative research to assess these differences is needed.[210]

Before examining the evidence, we look at democratic theory to assist us in reviewing Cyberthreats to democracies.

[208] Surkov, 2019. R. Mueller, 2019.
[209] Clinton, 2019.
[210] Tenove, et al., 2017.

5 Democratic theory

> 'Many forms of Government have been tried, and will be tried in this world of sin and woe. No one pretends that democracy is perfect or all-wise. Indeed, it has been said that democracy is the worst form of Government except for all those other forms that have been tried from time to time.…' Winston Churchill, 1947[211]

Governance has been the subject of human inquiry for millennia, and with the current dominance of democracy as the world's ,rule of choice', scholars continue to debate the subject in theory and practice, for example arguing what makes systems democratic and where the legitimacy of such a system lies.

> While *democracy* is a property of political systems, it is enacted and reproduced through social actions, and thus retains (ontologically speaking) its agent-focused, normative foundation in self-government. *Institutions* such as elections and legislatures are rule-based, incentivized, and sociologically stable combinations of social actions that assign roles to individuals (e.g., voter, representative, etc.). [212]

Over the past several decades theorists have debated different models of democracy, with countless democratic models arising on paper such as "electoral democracy, competitive elite democracy, competitive multiparty democracy, pluralist democracy, corporatist democracy, developmental democracy, republican democracy, advocacy democracy, agonistic and adversarial democracy, pragmatic democracy, participatory democracy, progressive democracy".[213]

All those models of democracy have contributed to the development of Democratic Theory, with the liberal-discursive model emerging as the dominant prevailing regime.

While those models are both interesting and worthwhile in themselves, I agree with critics who say that these strands of Democratic Theory have respectively not managed to theorize political behavior in Cyberspace and in isolation fall short of being able to explain to the wide-array of problems and threats currently facing democratic institutions and norms. However, together those sub-strands of Democratic Theory are able to provide input into defining political actions and institutions that help us define key *functions, forums and norms* that are present and need to be protected in a democratic society. [214]

[211] Churchill 1947.
[212] Warren, 2017., pp 43
[213] Ibid.
[214] Ibid.

5.1 Key Components of Democracy

The political theory I apply to analyze Cyberattacks on democracies is Warren's well-theorized outline of principle functions of democracies. His outline is based on a functional view of democratic organizations and an analysis of available academic democratic writings and theories, where he pinpoints key social functions that need to be present – and in working order – for a system to be truly democratic;[215]

> "If a political system *powers inclusion*, *forms collective agendas and wills*, and *organizes collective decision capacity*, it will count as "democratic." […] I shall suggest that political systems that solve democratic problems will make use of seven kinds (or classes) of generic political practices: *recognizing, resisting, deliberating, representing, voting, joining,* and *exiting*. [216]

Warren builds upon the ontology of Weber[217] viewing deliberate democracy not as a theory of power or distribution of wealth, but as *social functions*: The institutionalization of democratic indicates a social-state of constant problem-solving, or a ‚self-governing' society as Warren puts it – notably all communicated, decided and planned through *discourse*:

> "only by understanding discourse as substantive ideas and interactive processes in institutional context can we fully demonstrate its transformational role in policy change."[218]

This view acknowledged that above all *ideas* and *discourse* are primary causes for change, relying heavily on the work of Discursive theorists such as Habermas who claims that: „[Discursive Democratic Theory] is a primarily a collective will formation, focused on mediating conflict through the give and take of reasons."[219] Discursive democratic theory is attributed to the late 20th century theorizing of scholars like Jürgen Habermas and Hannah Arent, evolving from their studies on democratic power in modern democracies, its origin and how *legitimate decisions* are taken within the political sphere. Democratic theory sees discourse at the heart of any political action.[220]

Discursive Democratic Theorists have assumed rationality, as demonstrated in the writings of Beetham who claims Democratic participation includes "the process of deliberating with others about solutions to such problems leads participants to modify their

[215] Warren, 2017.
[216] Ibid.
[217] Ibid.
[218] Schmidt, 2011.
[219] Habermas 1996. in Warren, 2017.
[220] Flynn 2004, 3 (4) .

personal preferences in the light of evidence and the needs of others, and to consider a wider public interest."[221] Constructive theorists with their broad view of ideas however see ideas and discourse in a wider context and not necessarily rational, which leads us to seek a different angle for examining democracy, one that assumes ideas and discourse at the heart of every democratic interaction, as will be theorized later.[222]

Warren's extensive examination of academic work on Democracy and analysis of democratic problem-solving-functions leads to him to emphasize three key elements that he says must be present and well-functioning in order for a system to be considered a functioning democracy: *inclusion*, *forming of collective agendas and wills*, and *organization of collective decision capacity*.[223]

In line with Discursive Democratic Theory, we think of systems as comprised of resources, interdependencies, and constraints that are relevant to problems of democracy. Warren points out that each action faces problems that reveal strengths and weaknesses, which he outlines in Table 1.

Warren furthermore states:

> Political systems are more democratic just to the extent that they use (and institutionalize) these practices in ways that maximize their strengths and minimize their weaknesses, relative to the problems of empowered inclusion, collective agenda setting and will formation, and collective decision making. [224]

This places a normative view onto democracy: it puts a value on which societies or systems are democratic and what makes them so.

First a democratic system must *recognize all citizens as equal* and „include those people entitled to voice and impact into political processes through distributed empowerments "[225] Secondly citizens need to *formulate their agendas* into common policy which all (or nearly all) can live with. This is done through institutionalization of forums that negotiate rules and political agenda and third; democratic entities institutionalize legitimate execution of the public will. This takes place through a myriad of political social action that falls into the seven functions outlined above.

[221] Beetham, 2005. pp 132,
[222] Hay, International relations theory and globalization, 2013.
[223] Warren, 2017.
[224] Ibid.
[225] Warren, 2017.

Recognizing refers to the acknowledgement of all citizens, their needs and ideas. The right to be counted. *Deliberating* applies to the right of free speech and the process to influence others – and to be influenced yourself – in order to formulate consensus for a common will which leads to decision making on behalf of the group. *Representing* refers to each person's right to represent their own ideas leading to the right to be represented and heard through *voting*, in effect delegating your own discursive and democratic power to another agent. *Joining* refers to the right to create, join and leave any peaceful organization of your choosing and is closely related to *exiting* which is the right to produce competition-based accountability, an alternative choice. All these actions are a form of 'positive freedom' for action whereas *resisting* refers to 'negative freedom' from imposition and oppression. Resisting is each person's right to resist other 's power over them, but it also refers to systematic resistance and persistence of institutions and norms.[226]

In Table 1 Warren outlines strengths and weaknesses for democratic functions, from a normatively democratic point of view, assessing strengths and weaknesses for each function. It is an encompassing outline of social functions that problem-solve democratic procedures, providing a framework to assess how these activities serve their three-fold democratic purposes. While I will not venture into a discussion of democratic strengths and weaknesses based on Warren's framework, it outlines a useful framework for analysis of democratic functions and institutions.

[226] Ibid.

Table 1 – Warrens' Framework of Essential Democratic Functions and their strengths and weaknesses [227]

Generic practices that can serve democratic functions		Functions necessary for a political system to work democratically		
		Empowered inclusion	Collective agenda and will formation	Collective decision-making
Recognizing	Strengths	**Moral inclusion; deontic commitments support rights and duties of citizenship**	**Deontic commitments underwrite illocutionary dimensions of discursive conflict resolution**	**Deontic commitments underwrite obligations to collective bargains and compromises**
	Weaknesses	Insufficient for empowerment	Insufficient for conflict resolution	Insufficient for collective decision-making
Resisting	Strengths	**Incentivizes inclusions**	Incentivizes responsiveness to reasons	Induces collective responsiveness
	Weaknesses	Those with more resources have greater capacities to resist	Can undermine deliberative responsiveness	Veto players undermine collective capacities
Deliberating	Strengths	Responsiveness to persons, groups, discourses	**Connects preferences to collective wills and agendas; generates epistemic and ethical goods**	Discursively-generated agreements underwrite commitment to decisions Reduces veto players
	Weaknesses	May privilege articulateness and established discourses	Dangers of group think and "internal" exclusions	Lack of inherent decision rules
Representing	Strengths	**Expands inclusions over time and space; manages complexity**	**Enables perspective-taking; enables small-group deliberation within large polities**	**Representative bodies can function as accountable decision-making bodies**
	Weakness	Often difficult to monitor, motivate, and enforce principal-agent relations	Two/three-level games in representative bodies can undermine deliberation influence	Two/three-level games can undermine incentives for agreement
Voting	Strengths	**Easy to distribute empowerments; clear means for motivating representative responsiveness**	Reveals and expresses multiple preferences	**Enables clear decision rules; retains expressions of dissent**
	Weaknesses	*Demoi* must be pre-formed, generating exclusions; inclusions highly sensitive to electoral system design	Weak collective will formation: preference cycling, low capacities for preference ordering	Highly sensitive to decision rules
Joining	Strengths	**Constituency formation, across boundaries; empowers resistance**	**Supports articulated positions and discourses**	Underwrites "governance"
	Weaknesses	Over-representation of well-resourced and organized groups	Can undermine responsiveness, collective will formation	Can undermine collective decision capacity; gridlock
Exiting	Strengths	**Empowered exit can induce organizational responsiveness**	**Highly responsive "signaling" capacities**	**High capacity for varied and proximate responsiveness**
	Weaknesses	No inherent equality of distribution	No collective will formation	No collective agency

This framework of democratic functions applied to the Social-level of Cyber-security and democratic Cyber-functions has the possibility to show us from a political science standpoint *which activities are vulnerable for attack. It gives us political and practical tools to analyze and prepare what actions of democracy must be protected.*

Applied to democratic social activities that involve Cyber-systems and Cyber-activities each political function and social action includes institutions, infrastructure, staff, processes, objectives and junctions that provide opportunities for Cyber-attacks.

The framework allows us to examine how the seven functions (*recognizing, resisting, deliberating, representing, voting, joining and exiting*) are performing their three main functions; *empowered inclusion, collective agenda and will formation,* and *collective decision making.*

[227] Warren, 2017.

5.2 Applied framework of democratic functions and actions

Below is a *framework for identifying and categorizing Cyber-attacks using Warren's functional Democratic framework, revealing in the process discursive weaknesses of democracy.*[228]

The table shows Warren's framework applied to democratic Cyber-functions; each box represents *Cyber-attacks* on democratic functions and activity. The table is *not* a complete overview of attack types, and activities can belong to more than one box.

Table 3 – Examples of Weaknesses of Democratic Cyber Activities

Function → ↓ Activity ↓	Empowered inclusion	Processes of collective agenda & will formation	Norms & Collective decision making
Recognizing Examples:	In-access to information, exclusion through technical barriers. "no such person"	Fake-news targeting minorities, troll-storms, media block-out.	Silencing of certain opinions, denying groups to vote, trolling women & minorities. Voter registration tampering.
Resisting Examples:	Surveillance, frivolous legal targeting, creation of paranoia through thought bubbles.	Silencing/altering free press, tracking down & silencing critics & viewpoints.	Attacks on certain websites and groups, targeting those who resist. Dissolving organizations.
Deliberating Examples:	Trolling and disrupting discourse. Establishing actors 'above the law'.	Silencing journalists & views. Targeting representatives w. lies	Portals with false mal-information Targeted false information, mis- & dis-information
Representing Examples:	Targeting volunteers & candidates, hacking, leaks, "burning" volunteers	Smear campaigns, 'shooting messengers' Hacks and blackmails, confusing voters	Breaching institutions, media and planting incorrect information. Undermining the system.
Voting Examples:	Invasion of voter privacy to target or sway. 'Hiding' polling stations	Targeted ads, targeting representatives. Targeting POC to abstain from voting	Hacking elections, undermining legitimacy of targeted areas
Joining Examples:	Expelling people from voter registry, make it hard to register	Make joining dangerous "no such voice"	Make politics repulsive and uninteresting
Exiting Examples:	'Canceling' political opponents, making them un-electable, smear campaigns	Removing political choice through hacks, voting frauds	Systematically skew opinions and make them unthinkable as solutions

[228] Warren, 2017.

The application of Warren's framework to Cyber-security of democratic social-activities helps democracies identify Cyberthreats and act proactively in incorporating remedies. It provides a good starting point for a political Threat-analysis of democratic Cyber-activities.[229] Take for example referendums involve deliberating, representing, voting and exiting which involves Cyber-threats such as misleading political ads, trolls that disrupt discourse, hacking of candidates, leaks of private information and removal of choice.[230]

If and when attacks that fall into the above framework take place: they should be interpreted as attacks on democratic functions, institutions and norms.

Next, *we operationalize the study* by examining Zarate's claims that Russia has used "information and influence operations and Cyber tools to achieve three important and complementary goals" that undermine democracy according to Warren's theorization: [231]

- To undermine faith and confidence of democracy and its institutions from within – *attacks on participation and public deliberation*
- To exacerbate social and political divisions advantageous to Russian interests, including in furtherance of Russian foreign policy or simply to undermine Russia's enemies and opponents **–** *attacks on public safety, public deliberation and democratic norms*
- To take advantage of 21st century information environment to obfuscate or confuse the truth and amplify narratives that align with Russian interests, even when patently false – *attacks on democratic participation, public deliberation and democratic institutions.*

[229] Tenove, et al., 2017.
[230] Pamment, Nothhaft, et al., 2018.
[231] Zarate, 2017.

6 The Problem: Cyberattacks on Democracy

> Putin] has used the security services, the media, public and private companies, organized criminal groups, and social and religious organizations to spread malicious disinformation, interfere in elections, fuel corruption, threaten energy security, and […] protect and exploit Cybercriminals in Russia who attack American businesses and steal the financial information of American consumers.[232]

This inquiry focuses on a specific type of information-social Cyber-attacks on voters, candidates and democratic institutions in NATO countries. This chapter examines the methods and approach that was used to attack democratic processes, and norms in order to create a state of „information disorder". [233] This study is normatively unapologetic in its protective stand on democratic values and institutions.

Before examining these attacks in relation to the research questions we take a closer look at the actors and the situation.

[232] Committee on Foreign Relations, US State Senate, 2018.
[233] Wardle and Derakhshan, 2017.

6.1 Democracy's Security Alliance & Emergence of a new Space

The goal of the North Atlantic Treaty Organization is to ensure democratic countries continued freedom and security from outside aggression through political and military means. From its foundation the organization has been an active global 'peace-keeper' and protector of [democratic] freedom and security.[234]

The alliance has expanded in 'waves' and now contains 29 member states, including many former Warsaw-pact nations and has as its back-bone most of the oldest democracies on Earth. NATO includes around 10% of Earth's land-mass and is of immense security and economic importance for its 604 million members and democracy worldwide. For many members the alliance serves as a symbolic and strategic beacon of democracy and freedom in the world.[235] For its adversaries, however, it represents capitalist imperialism and intervention in government affairs and civil-wars around the globe.[236]

The first members of NATO were also the founders of the United Nations and among the first states to ratify the legally binding treaties that make up the UN's Universal Declaration of Human Rights who guarantee their citizens' rights to security.[237] NATO is also coincidentally the place where scientific research and security related projects launched what later would become the Internet, and later the world-wide-web and Cyberspace. NATO countries are leading Cyber-users with reported 80% to 100% of the population online and a majority of them actively using social media.[238]

While NATO nations officially adhere to democratic values and freedom of information, they are also state entities that run joint and individual military agendas and have commitments and obligations to their citizens. In the name of democracy and freedom NATO is actively running operations to harm its opponents and surveillance on billions of

[234] U.S. Department of State, 2019. NATO, 2018.
[235] The North Atlantic Treaty Organization (4) January, 2018. . Member countries.
The 29 members states in alphabetical order are: Albania, Belgium, Bulgaria, Canada, Croatia, Checz Republic, Denmark, Estonia, France, Germany, Greece, Hungary, Iceland, Italy, Latvia, Lithuania, Luxemburg, Montenegro, Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Turkey, United Kingdom, United States. NATO, 2018.
[236] Surkov, 2019.
[237] United Nations 1948.
[238] Internet Live Stats, 2016.

Cyber-users through hardware and software surveillance all over the world "to intercept data flowing through the global Internet." [239]

After decades of Cyber-dominance by US and joint NATO operations over Russia, there are sure signs that the tide is changing. After a few test-runs, Russian agents utilized key weaknesses of Western democracies to affect democratic elections, revealing that NATO and democratic nations were and are still not prepared for assaults through Cyberspace.[240]

An example of a recent damaging Cyber-attack is the 2017 #WANNACRY virus that crippled hundreds of thousands of computers around the world, including the UK's National Health Service (NHS). The virus entered the NHS system when a staffer clicked a link which installed the virus on the user's computer and from there it piggybacked into the NHS network, holding its information for ransom, causing damage and costing an estimated amount of £92 million in damages.[241] The virus was traced back to North Korea but the Pyongyang government denied any involvement, as it did in the 2014 SONY hack when N-Korean agents hacked and released e-mails, information and four unpublished movies in retaliation for Sony making the comedy "The Dictator" about a fictional North Korean trip, which embarrassed the dictatorship.[242]

Cyber-attacks against NATO's infrastructure increased by 60 percent from 2016 to 2017, with the largest increase in attacks traced back to Russia.[243] "China, Russia, Iran, and North Korea increasingly use Cyber operations to threaten both minds and machines in an expanding number of ways—to steal information*, to influence our citizens*, or to disrupt critical infrastructure."[244]

NATO has acknowledged the increased danger and taken several important steps to better defend against these attacks, including needed critical changes in its organizational

[239] Francheschi-Bicchierai, 2014.
[240] Pamment, Nothhaft and Agardh-Twetman, et al., 2019. Tenove, et al., 2017.
[241] Field, 2018.
[242] Balsamo and Eric, 2018.
[243] Stoltenberg, Doorstep statement by NATO Secretary General Jens Stoltenberg prior to the informal meeting of EU Ministers of Defense, Tallinn, Estonia, 2017, Stoltenberg, Why cyber space matters as much to Nato as land, sea and air defence Jens Stoltenberg on Article 5 and why cyber defence has become core to the alliance, 2018.
[244] Coats, 2019. ,

setup, scope of operations, integration of domestic efforts and its approach to information.[245]

In 2016-17 NATO officially acknowledged the military importance of Cyberspace when it defined Cyberspace as the 'fourth space' in addition to land, air, and sea.[246] Recognizing Cyberspace as an operational domain for political power and global security has implications for NATO member state's overall strategy and allocation of resources.

It also marks a junction for Cyber-theory whether it be Security studies or International Relations, because i*t marks a beginning of a new chapter in International Relations with the acknowledgement of Cyberspace as a virtual government space*.

The Inclusion of Cyberspace as a specific space has been well argued by military and security theory, but it has not, at least not officially, been studied from a constructive political perspective that focuses on ideas and Cyber-propaganda. This study addresses that theoretical gap and utilizes democratic and Ideational frameworks that have potential for theoretical, but more importantly, *practical* contributions. Treating Cyber-as a space in itself, instead of placing it within ground-military, psychological and information operations, acknowledges the psychological effects of Cyberspace, an area of manipulation that Russia has mastered.[247]

Cyber-security and weaponization of Cyber-space is in many ways comparable with Mutually Assured Destruction (MAD) scenarios that involve Weapons of Mass Destruction (WMD). In MAD situations there is a significant danger of escalation frequently due to circumstances that run out of control. Cyberspace is particularly vulnerable to escalation because of the common practice use of AI and automation for all types of monitoring and problem solving, but they are faulty and can increase real danger of unintended escalation of situations, mis-readings and retaliations.[248]

Democracies have had an ongoing domestic debate about who decides when to retaliate to Cyber-attacks in kind and whether they are of a magnitude that requires high-level authorization or if counter-attacks are a part of military privileges, allowable and within

[245] Grynkewich, 2018. NATO, 2019.
[246] NATO, 2018.
[247] Pomeranzev and Weiss, 2013.
[248] Committee on Foreign Relations, US State Senate, 2018.

bounds knee-jerk reactions.[249] Global leaders are generally weary of circumstances where retaliation and escalation can happen and things become real in their consequences.[250]

This is for example one of the reasons countries focus on Cyber-protection and security and don't want to venture into the field of Cyber aggression - there is simply too much at stake.

Another large step towards tackling modern Cyber-threats coincided with the inclusion of Cybersecurity as a space of operations was inclusion of *information* as the seventh joint-function of military operations, when at war which in my view reflects a change in view towards the new information war in Cyberspace. NATO's inclusion of Cyberspace as a space and of information as the seventh joint function includes an undertheorized acknowledgement of a *constructed reality* where Cyber-attacks create an ever-increasing threat to its members, both in importance, cost and scale.[251]

A third major step by NATO and Western democracies were supporting announcements by NATO leaders re-iterating that Cyberattacks can trigger the alliance's Chapter V Collective defense clause.[252]

That announcement sent a clear message that NATO is not to be tested. NATO and its member states pose at least a threefold threat to Putin's Russian regime: [253]

- Through sanctions, put inplace after Crimea
- Free and successful democracies where citizens are free to speak their mind and organize as they please while in peace.
- Democracies with transparent governments, the rule of law, a free media, and engaged citizens are naturally more resilient to the spread of corruption beyond Russia's borders, thereby limiting the opportunities for the further enrichment of Putin and his chosen elite.

Over the past few years an increasing army of international journalists, security experts and elected officials have reported that during the past two decades Russia has managed to interfere in internal politics of at least 27 democratic European and N-American

[249] Sanger, 2018.
[250] Stevens, Cyber Security and the Politics of Time, 2010. Merton 1948.
[251] NATO, 2018. Grynkewich, 2018.
[252] Hardy, 2016. Sauer, et al., 2017.
[253] Committee on Foreign Relations, US State Senate, 2018.

countries, through “sweeping and systemic” attacks on key processes, norms and institutions.[254] Next we examine those attacks.

6.2 Russia: Waking of the Cy-bear

Russia is the largest country on earth and with 144 million inhabitants, and several globally allied countries, is a global force to be reckoned with. It is an historical and present adversary to the USA and NATO. As the back-bone of the Soviet Union (USSR) it has been on the receiving end of severe Cyber-attacks over the past five decades, most of whom were executed by NATO-allied agents and have never been reported.[255]

Russia has had a long and impressive history in Cyberspace, or ‘Cybernetics’ as the West. Following WWII and the dawn of the computer age Eastern-block scientists embraced Cyber-technology. The years following WWII were the dawn of the computer age and Soviet scientists embraced the technology which showed much promise. While the West embraced computer technology its history in the USSR is much more complicated and that historical legacy still influences current events.[256]

Russian computer science provided much-needed solutions for Soviet logistical problems but were only partially allowed to develop due to Stalin‘s mistrust of Computer sciences, antipathic to a future where humans were replaced by machines. As a response during the 50’s the Soviet Communist Party ran effective state-wide propaganda campaigns against Cybernetics, a continued message to its citizens for the next decade.[257] Soviet scientists however soon learned to embrace the concept for solutions of Soviet operations.

The temperament changed during the 60‘a with Cybernetics serving as the vehicle for USSR‘s dominance over Americans during the ‚Space-Race‘ when both governments used race to space to promote their image of intellectual and military dominance.

The space race gave rise to a computerized way of problem solving, sparking a technical and intellectual movement in the USSR. This new movement of computerized

[254] Dorell, 2017. R. Mueller, 2019.
[255] Peters, 2012. Sanger, 2018.
[256] Russian Media VGTRK 2015 .
[257] Ibiid.

problem solving included a new ideological science-based approach where a computational formulation of projects and ideological principles spread with the technology itself. [258]

The success of USSR Cybernetics were impressive and grandiose plans were developed to put Cybertechnologies to use for state objectives at the highest level, not least because with the great need for the system to run mass scale economic planning and military systems for the largest country on earth containing 15 unified republics operating across over 22 million km^2 and 11 time zones inhabiting nearly 300 million citizens. Cybernetics for state use is a Russian legacy:

> Soviet Cybernetics was not simply an intellectual trend; it was a social movement for radical reform in science and in society in general. Cyberneticians came to believe in the possibility of a universal method of problem solving if only problems could be formulated in the right language [...] of objectivity and truth. Soviet Cybernetics challenged the existing order of things not only in the conceptual foundations of science but also in economics and politics.[259]

This movement and language however would be adapted, curbed and utilized by the all-powerful state, in order to further state objectives and central planning. Cybernetics was limited to specific state use after Soviet leaders realized that computers would deliver truthful information to its users instead of allowing for the 'adjustment in message' that was needed from state propaganda masters in order to keep control over people.[260] Therefore the development of computer and Cyber-technologies was suppressed, leaving Russia technologically behind, running Cyber-"patchworks" with their computers connected in clusters, not networks as done by governments, universities and companies in the West[261]

Russia has become increasingly skeptical of using western technology and popularizing the global Internet. For decades it has been on the receiving end of Cyber-aggression and after the 2013 Snowden revelations Russian intelligence authorities changed many of their methods, switching to isolated networks and low-tech solutions like going back to using typewriters for top secret material. "Many documents are still not created in electronic format," [a] source said. "This practice continues inside the defense ministry, the emergency situations ministry and the security services."[262]

---

[258] Gerovitch 2002.
[259] Gershkovich, 2019.
[260] Russian Media VGTRK 2015 .
[261] Baraniuk, 2016.
[262] Elder, 2013.

Currently, around 75-80% of the Russian population has access to the Internet compared to 90 up to 100% saturation in the West.[263] For decades Russian authorities have worked under a state mandate towards setting up a specific Russian Internet, similar to how China has placed itself behind 'The Great Firewall of China' and as part of these plans Russian authorities in 2019 "took itself offline" while state technicians installed routers and infrastructure to re-route all digital traffic through state-controlled servers. According to Russian officials this is done in order to protect Russian infrastructure and communications in case of a Cyberwar.[264]

Russians are now the largest group of European Internet users, they mostly participate in the Russian Internet, RUnet which runs parallel to the Western World Wide Web Internet and are devoted users of social media with 80% of people under 35 using the social media sites Odnoklassniki and VK (formerly Vkontakte) that's is not nearly as 'strict' in removing offensive content as Western SM, a reflection of Russian culture where human rights are defined differently than in the West.[265] Russians can access the ‚regular Internet' through VPN services but due to a language barrier and a specifically Russian view of Cybernetics, only a part of them has become „Netizens" as many of their European counterparts define themselves, rather, most Russians are Cyber-users.[266]

The Russian government exerts power over its citizens and Internet-users on a different level than democracies and NATO. While both parties claim to be protecting themselves and Western accusations evolve mostly about invasion of privacy and data storage, Cyber-users in Russia have real reason to fear for their safety if they're not careful. In Russia people go to prison or disappear for criticizing the government and reporting the wrong news.[267]

As a proactive measure Russia has outlawed ‚fake news', which at first sounds like a positive protection for the sake of democratic debate, except in Russia truth does not depend on facts or compromise but on the government's perspective and critics fear the law will be abused in countless ways. Furthermore, Russian authorities are actively working to

[263] Internet Live Stats, 2016.
[264] Gilbert and Vice News, 2019.
[265] Rescheto, 2019. Kotlyar, 2017. Zabrisky, 2017.
[266] Rescheto, 2019.
[267] Jensen, Valeriano and Maness, 2019.

remove Cyber anonymity, something the West has treated as part of people's right to privacy.[268]

Russia systematically targets, jailed and kills journalists[269]; there is little freedom for bloggers or citizens to express their thoughts on politics or local matters, if you do so you can be legally thrown in jail and silenced. Furthermore, the Deputy head of the Russian secret police FSB has called for complete state control over Cyberspace, demonstrating several actions that show Russia is doing just that, with many fearing Russian isolationism and Cyber-control similar to China and North-Korea.[270]

This fundamental difference between free democracies and "managed-democracy" cannot be understated. It is the difference between freedom and serfdom.

According to Putin's supporters the new Russia is gaining strength after passing several 'stress tests'[271] there are signs that Russia is internally weaker than it shows and "Polling suggests, moreover, that Russians are starting to see the official obsession with restoring national greatness in the face of supposed threats from the west for what it is — a diversion from domestic malaise"[272]

Russia sees the openness of Western societies as a weakness, or as one of Putin's former trusted strategists put it: "The illusion of choice is the most important of illusions, the main trick of the Western way of life in general and of Western democracy in particular." [273]

[268] Al Jazeera News, 2019. Rescheto, 2019.
[269] Committee to Protect Journalists, 2019.
[270] Gershkovich, 2019.
[271] Surkov, 2019.
[272] Committee on Foreign Relations, US State Senate, 2018. Valeriano and Maness, 2019.
[273] Surkov, 2019.

Information and the Russian State

Control over information is an integral part of Russian statesmanship and has deep origins in Marxist-Leninist ideology. It was first taught as a *spetspropaganda* Military theory in 1942 as a response to the well documented success of Nazi propaganda and developed over the next decades into a vital part of USSR's power and military operations, where it remains today.[274]

These tactics fall under Information influence activities are the illegitimate efforts of foreign powers or their proxies to influence the perceptions, behavior, and decisions of target groups for their own benefit."[275] They are a part of *Irregular warfare* which is defined in military theory as "a violent struggle among state and nonstate actors for legitimacy and influence over the relevant populations."[276]

Russian statesmen have long held a respect for scientific approaches to communication and propaganda for the maximum psychological effect. During Soviet times state officials tested and perfected a uniquely Russian approach to mis- and dis-information; creating an arsenal of information-tactics designed to confuse their opponents and compel them into harming themselves by provoking miscalculated reactions to misinformation.[277]

Soviet defectors revealed "a carefully constructed, false message that is secretly introduced into the opponent's communication system to deceive either his decision-making elite or public opinion." [278] Operating under psychological theories such as "according to the laws of psychology, what we have forgotten affects us much more than what we remember"[279]

When the USSR splintered following the fall of Communism some 30 years ago, its old information branches and approaches were seamlessly transferred into a new state machine where they've adapted to new situations and advanced with developments in technology. In addition to excepting total control over information and discourse within its own borders Russian leaders have been unable to accept democratic change in the former Soviet republics. [280]

[274] Lucas and Pomeranzev, 2016. Grimes, 2017.
[275] Pamment, Nothhaft, et al., 2018.
[276] US Department of Defense 2007, Committee on Foreign Relations, US State Senate, 2018.
[277] Pomeranzev and Weiss, 2013. Digital Forensics Research Lab, 2018.
[278] Lucas and Pomeranzev, 2016.
[279] Surkov, 2019.
[280] Committee on Foreign Relations, US State Senate, 2018.

> Russia believes it is entitled to a "gray zone" along its borders, an area in which the sovereignty of other nations is constrained and in which its politicians and its companies enjoy privileged economic and political status. It regards the post-1989 settlement of Europe as both deplorable and temporary. It sees democracies and open societies as a threat, because they may "infect" Russia with their ideas.[281]

Combined with a foreign policy of active interference in its neighbors' domestic affairs, often supported by large Russian-speaking minorities in those countries, Russian leaders have spearheaded information-operations that are designed to influence the policies of targeted governments, undermine confidence in opponents' leaders and institutions, disrupt opponents' relations with other nations and discredit and weaken any opposing governmental and nongovernmental functions.[282]

For example, Russia launched such propaganda Cyber-attacks during the Eastward expansion of NATO and targets journalists that dare expose their tactics to severe personal Cyberattacks that include leaked nude pictures and death-threats.[283]

> Russia's approach to information takes advantage of the idea of freedom of expression in order to subvert it, replacing information with *dezinformasiya,* abusing the idea that "truth is always relative" to the point where Kremlin media show "complete disregard for facts." [284]

Russian information-agencies have manipulated discourse at all levels of their opponents' societies, from planting false information at the highest level of decision making to spreading salacious gossip on the streets, everything and anything published with the goal in mind to *destabilize its opponents*.

Russian agents have perfected Soviet forms of psychological warfare through fake and forgeries in order to let their opponents operate in a "fog of falsehood". "This is a form of warfare in which an attack does not destroy the enemy from the outside but rather leads him to self-destruct, though "self-disorganization" and "self- disorientation."[285]

> There are two aspects of this Russian approach to 'information warfare': first, the outward-facing campaigns of disinformation and propaganda, designed to blunt or divert criticism of Russian actions already carried out and prepare the ground for further steps

[281] Lucas and Pomeranzev, 2016.
[282] Committee on Foreign Relations, US State Senate, 2018.
[283] Higgins, 2016. Aro, 2015.
[284] Pomeranzev and Weiss, 2013.
[285] ibid.

> in the future; and second, the internal efforts to isolate the Russian population from a true picture of events both in the outside world and in their own country. "[286]

This agenda is executed at home against Russian state critics with the help of its institutions and law. Russian officials call for total dominance over Cyberspace and have passed controversial law through the Russian parliament that grants the state great power. The new law cuts citizen freedoms in Cyberspace, makes only certain areas legal while outlawing other types of Cyber-participation. It imposes prison on those who criticize the government and blocks out pages that cover corruption on top of punishing people for such criticism.[287] As a response a very unique protest took place early March 2019 with at least ten thousand people protesting against new legislation, risking their safety and future by participating.[288] There are signs domestic discontent is growing but also that the Russian government has no intention of relaxing its grip on domestic matters:

> Officials can — and have — let disaffected voters express their anger through political venting mechanisms ("friendly" opposition parties, etc.) without destabilizing the existing order." This works in Russia's single party systems, but it can be very influential in countries that have coalition governments or large unsatisfied crowds that can destabilize a country similar to what may have been happening in Europe.[289]

It is extremely dangerous to report inconvenient facts or criticizing Russian authorities. Over the past two decades over 30 journalists critical to the state have been assassinated within Russian borders and several more suspected killings taking place in other countries, making Russia face international accusations of state-sponsored-assassinations and violating the fundamental principles of sovereignty.[290]

Several reports trace the beginning of Russia's current information based Cyber-war and hybrid-war back to Russia's 2014 annexation of Crimea from Ukraine in an attack that combined Cyber-operations and classical military operations, giving us an indication of the type of wars fought in the future.[291]

---

[286] Giles, 2015.
[287] Crosby, 2019.
[288] BBC News, 2019.
[289] Schmidt, 2017. Harford, 2019.
[290] Jensen, Valeriano and Maness, 2019. Pomeranzev and Weiss, 2013.
[291] Lucas and Pomeranzev, 2016. NATO Committee on the Civil Dimension of Security, 2018.

Criminality in Crimea

The Crimean Peninsula in the Black Sea is a fruitful area that's become equally known for its wars and beauty. Russian tsar-time royalty traditionally vacationed at their Crimean palaces with beautiful views over the Black Sea before the revolution. After Russian-Ukrainian Bolsheviks conquered Ukrainians a century ago, with Ukraine becoming a part of the USSR, Soviet leaders maintained the tradition of treating the area as its playground, furthering a Russian elite community around the city Sevastopol.

During the Soviet era Ukrainians became a minority in Crimea when millions of Russians flooded in to work in factories and on government mandated projects, fast outnumbering and moving away original citizens of the region, while at it stripping the previous populations of economic and political power. Similar mass-migration projects were executed over most Eastern Europe from the Baltic states to Crimea where Russian born immigrants became a dominant majority of the population. [292]

These great migration projects were not only done for the purpose of securing labor but a part of a power-strategy that was designed to make Russians a majority in most Soviet republics, or at least a minority of such magnitude that fights for independence would become unattainable. [293]

After the fall of the USSR in the early 90's these republics gained independence but with their loss of power Russian born 'minorities' became increasingly dissatisfied with their status, over-night going from being a ruling social-class to suddenly being considered outsiders in their new home-countries.

The governments of those newly formed democracies were faced with staggering challenges of democratization and real possibilities of armed conflicts or even civil-war when areas within their borders were inhabited by a majority of Russian speaking inhabitants who actively pursue the objective of re-joining Russia.[294] Within Russia there is also a sense of regret that these areas were lost and a great sense of support to assist Russian minorities to re-join 'mother Russia, considering these countries or areas within them rightfully Russian.

[292] Lucas and Pomeranzev, 2016. Jensen, Valeriano and Maness, 2019.
[293] Pomeranzev and Weiss, 2013.
[294] Committee on Foreign Relations, US State Senate, 2018. Sanger, 2018.

This applied to the situation that developed in Ukraine where politicians and business leaders attempted to strengthen ties with its European neighbors to the West to much dissatisfaction and protests from Russia who was still dealing with its own problems, recovering after the '90's power vacuum with Putin now positioning himself and those favorable to him at the center of government. [295]

The modern Russian form of governance, a style dubbed 'managed democracy' by Putin's officials approaches power and freedom in similar ways as the USSR formerly did. The ways of the 'Evil Empire' that Reagan had spoken of in the '80's still governed:

> Within Russia, Putin's regime has harassed and killed whistleblowers and human rights activists; crafted laws to hamstring democratic institutions; honed and amplified anti-Western propaganda; curbed media that deviate from a pro-government line; beefed up internal security agencies to surveil and harass human rights activists and journalists; directed judicial prosecutions and verdicts; cultivated the loyalties of oligarchs through corrupt handouts; and ordered violent crackdowns against protesters and purported enemies. [296]

With Putin and his allies enriching themselves and strengthening their hold on domestic affairs for the first two decades of this century, in 2014 Russia felt confident enough to exert its power and claim back some of its 'lost territory' through military and influence operations in countries which it defined as within its sphere of influence. [297]

Since the fall of USSR most of Eastern Europe and former Soviet republics have either taken gradual or great strides towards the Western model of open democratic societies, by either joining international treaties and organizations including the EU and its common market and/or joining NATO – which Russia interprets as a direct threat to its security.[298]

In March 2014 Crimea lost its power at the same time it was attacked and taken over by unmarked 'little green men' who denied identifying themselves but were by reporters and witnesses identified as Russian special forces working with local ethnic Russians. The little green put in place a functional government and directed Ukrainian institutions to hold a Crimean referendum on whether Crimea should join Russia, which the voters apparently confirmed, under much criticism by the international community.

[295] Sanger, 2018.
[296] Committee on Foreign Relations, US State Senate, 2018.
[297] Lucas and Pomeranzev, 2016. Sanger, 2018.
[298] Lucas and Pomeranzev, 2016.

The Russian green men backed up Russians on the ground took over the region using military power against the much weaker Ukrainian government in an operation where at least 12.000 people thousand people, mostly Ukrainians, lost their lives. [299] Within Russia the military backed annexation was so popular that domestically it was dubbed "the Crimean Consensus", wildly increasing Putin's popularity similar to the surge in approval ratings experienced by Bush Jr. during the Afghanistan and Iraq invasions.[300] Russia utilized all available mediums to execute the operation and justify its cause, using psychological manipulations and 'historical actions' similar to those used by high ranking US 'actors of history'.[301]

Denying the evidence, Russia denied any overstepping any boundaries, argued that the Crimean operations were domestic politics and even an Ukrainian civil war. Locally discontent voices were harshly silenced on- and off-line, and the government put in play democratic theatrics including highly criticized and controlled elections where Crimea's population voted to join Russia.[302]

Russia had good reason to fear Western reactions to the annexation, so as means to justify its actions acted out a remarkable array of tactics, designed to create in tandem a historical sequence of events that re-wrote the annexation as a justified rescue of a pummeled and pressed minority.[303]

> Russia's approach to information takes advantage of the idea of freedom of expression in order to subvert it, replacing information with *dezinformatsiya,* abusing the idea that "truth is always relative" to the point where Kremlin media show "complete disregard for facts." [304]

Through the use of discrete military force, Cyberattacks and propaganda Russia wrote a winner's account of history and created an *illusion of democracy* in Crimea in order to thwart EU and NATO retaliation and build a justifiable case before the International Criminal Court (ICC).

The ICC has confirmed that the events in Crimea constitute international crime, not civil war, and started legal proceedings of the case, which in turn made Russia pull itself from

[299] Zhakarova, 2019.
[300] Lipman and Wilson Institute, 2019.
[301] Suskind 2004.
[302] Pomeranzev and Weiss, 2013.
[303] Ibid.
[304] Ibid.

the court in 2016. [305] For Ukrainian citizens, politicians, journalists and allies it was extremely hard to distinguish between reality and fiction, between real events and propaganda, between what was true and what wasn't. [306]

What is of special interest for this study is that the Cyber tactics utilized by Russia in Ukraine played out like an exercise for a 'model war' with Cyber-operations that took place in tandem and synchronous with military operations.

Once Russia felt secure that it wasn't going to face military retaliation for the annexation of Crimea it turned its focus on defending itself discursively in Cyberspace through very similar tactics it has been developing in Crimea.

Russia's success in Cyberspace has been so great several Russian's have admitted that the state has changed its Cyberattacks and now utilizes successfully methods that attack Western values and democratic values.[307]

[305] Reuters, 2016.
[306] Pomeranzev and Weiss, 2013., Lucas and Pomeranzev, 2016.
[307] Carroll, 2019. Surkov, 2019.

6.3 Russian Cyberattacks on Democracy

> In political terms, Russia's interference was the crime of the century, an unprecedented and largely successful destabilizing attack on American democracy. It was a case that took almost no time to solve, traced to the Kremlin through Cyber-forensics and intelligence on Putin's involvement. And yet, because of the divergent ways Obama and Trump have handled the matter, Moscow appears unlikely to face proportionate consequences.[308]

Following the annexation of Crimea Russia continued its misinformation attack on Ukraine, but once it was secure that NATO wasn't going to retaliate with force, it turned its Information Operations towards the West. Over the next couple of years, the EU and USA led an international consensus to take several punitive actions against Russia in response for the annexation and its continued attacks on allied nations. The reactions included sanctions on several Russian businessmen and companies close to Putin, in effect freezing assets and hurting business interests. According to the Mueller report Russia's plan to help get Trump elected was to make a deal to keep Ukraine.[309]

Standing its ground, Russia next set its eye on targeting democratic weak spots and building upon its Cyber-expertise and established associates, such as the Internet Research Agency, it targeted upcoming elections in USA, UK, France, Germany, Italy and countries on Russia's periphery.[310]

A meticulous analysis by law enforcement, journalists and Cybersecurity experts of online activity during the past few years has revealed a patter on extensive information-operations where Russia and domestic-liaisons collaborated to further certain political agenda – each with their own goals in mind.

> Russian Cyber strategy, in addition to reflecting tenets of Soviet era active measures, focuses on soft targets, including civilian networks. […] As opposed to the US, Russia tends to amplify propaganda with bots and troll farms rather than more traditional diplomatic coercion.[311]

[308] Miller, Nakashima and Entous, 2017.
[309] R. Mueller, 2019. Lipman and Wilson Institute, 2019. Chen, The Agency - New York Times Magazine, 2015.
[310] Committee on Foreign Relations, US State Senate, 2018. R. Mueller, 2019.
[311] Jensen, Valeriano and Maness, 2019.

Moscow tends to use Cyberattacks in three waves: prior to the conflict to *delegitimize and distract* their rival, during the conflict to *support combat operations*, and after the initial fighting to *create chaos* that, consistent with active measures, undermines the legitimacy of the target state.[312]

Table 3 shows an overview of tactics analysts of the Ukrainian attacks call "The Kremlin Toolkit", a strategy that focuses on *first shattering communications* to *demoralize* their enemy and then moving in take out the enemy's *command structure*.

These tactics are executed through various sub-groups employing *vandals, burglars, thugs, spies* and *saboteurs,* under directive from the Russian intelligence services GRU and FSB.[314]

Table 2 - The Kremlin Tool Kit[313]

Kremlin Aim	Kremlin Action
Shatter Communications	Buy up Western media DDoS attacks Paralyze journalism with threat of libel
Demoralize Enemy	Confuse the West with mixed messaging Seduce experts through high-level fora Disinformation campaigns
Take out Command Structure	Divide West though divide-and-conquer ruses Buy up political influence

The evidence indicates that this is just what has happened, now that three major international actors and NATO powers; the US, UK, and France have been preoccupied over the past 2-3 years dealing with internal discourse and disorder, following Russian attacks on their democratic elections.

Two main opportunities presented themselves in 2016 with the UK Brexit referendum and the US presidential elections. and Russia assigned resources to applying its tactics to asserting its influence through Cyberspace. Numerous reliable reports backed by evidence on the 2016 US presidential campaigns conclude that targeted Cyberattacks by Russian hackers and trolls were decisive for the outcome of the US presidential election, an election where Trump proudly won the presidency by some 77 thousand votes in 3 states, 3 million less total votes than his opponent.[315]

In a "sweeping and systematic manner" Russia attacked the US 2016 presidential election with a "two-pronged attack": "One was the hacking and leaking of e-mails from the Democratic National Committee and Hillary Clinton's campaign chairman, John Podesta. The

[312] Pomeranzev and Weiss, 2013.
[313] ibid
[314] Sanger, 2018.
[315] Mayer, 2018. Mueller, 2019.

second was a campaign of misinformation and propaganda carried out largely over social media."[316]

A report from the US Intelligence Community states: "Moscow's influence campaign followed a Russian messaging strategy that blends covert intelligence operations—such as Cyber activity—with overt efforts by Russian Government agencies, state-funded media, third-party intermediaries, and paid social media users or "trolls."[317] Russian Cyber activities are a continuation of the Soviet approach to political warfare optimized using social media and stolen information to manipulate target populations and disrupt rivals from within.[318]

Russian fronts have violated limits on campaign spending in the US, UK, France, Estonia and Ukraine with reports of meddling in several other countries. The British President of the European Council Donald Tusk said recently that Russia's operations pose *a major threat to European unity and its institutions*.[319]

The Mueller Special Council Report confirms previous evidence of interference through Cambridge Analytica, The Internet Research Agency, Guccifer2.0 hacker persona and collaboration between Trump's campaign officials and Russian agents, with at least 10 instances where Trump appears to have obstructed justice privately and publicly in order to hide cooperation between his own campaign and Russian officials, including illegal sharing of campaign data and voter profiles.[320] These attacks have largely been proven and made public because of whistle-blowers and undercover journalists who have spoken about their work on 'troll farms'.[321]

British authorities and political experts similarly claim illegal Russian linked interference in the Brexit referendum, but coverage on the activities has largely been drowned out by domestic discourse and confusion over the technicalities of Brexit.[322] France has seen growing domestic fractioning and its most violent and persistent protest in decades, with Macron's government responding in "Le Grande Debate" a national debate on

[316] Mueller, 2019. Committee on Foreign Relations, US State Senate, 2018. Chen, What Mueller's Indictment Reveals About Russia's Internet Research Agency - The New Yorker, 2018.
[317] The Intelligence Community (FBI, CIA & NSA), 2017.
[318] Ioffie, 2017. Pomeranzev and Weiss, 2013. Lucas and Pomeranzev, 2016.
[319] Broniatowski, 2018.
[320] Mueller, 2019.
[321] Jones, 2018. Pasha-Robinson, 2018. The Daily Beast, 2018. Aro, 2015.
[322] Applebaum, 2019.

the future of France, what it means to be French and how the nation is going forward as a multicultural society. Populist discourse is growing all over Europe.[323]

Similar verified reports confirm that Russia managed to reach and influence tens of millions of British citizens, still with an unproven connection between the ads and voter behavior. It is now clear that campaign laws were broken, misinformation and targeted ads went unchecked and that more people are calling for an investigation similar to the US Mueller probe. Low voter turnout, close margins and polarizing language has catapulted Britain into a dubious political process that's overtaken European political discourse.[324] This indicates success in causing confusion within at least some off Russia's targets. Additionally, populist voices seem to have received welcomed or unwelcomed Russian help in several European democracies.[325]

In the USA Congress seems to be moving forward with calling witnesses from the Mueller report to testify before congress in order to make a decision on whether to impeach the US president for obstruction of justice into the investigation of his campaign's cooperation with Russia during the 2016 campaign. [326]

In France the 2017 presidential elections were hit with hacks, (tainted)leaks, misinformation and scandal. Macron's party En Marché was hacked and the information altered before it was leaked, false stories were posted about the candidates and polarizing advertisements targeted towards disenfranchised groups and false narratives went viral repeatedly. Additionally, Russia hacked France's election infrastructure repeatedly.[327] The France response however was different than in the USA and UK which will be discussed further in relation to theory.

An extensive part of Russia's tactics is disruption of information and creation of confusion, using mis-, dis- and mal-information. Russia's "message is customized for particular markets, varies from country to country, and includes both local and foreign policy themes."[328]

---

[323] Schofield, 2019. Heyer, 2019.
[324] B. Mueller, 2019.
[325] Politi, 2016.
[326] R. Mueller, 2019.
[327] Greenberg, The NSA Confirms it: Russia hacked French Election 'Infrastructure' - The Wired, 2017.
[328] Lucas and Pomeranzev, 2016.

In a 2017 EU report Wardle and Derakshan utilize a framework for analysis in what they call 'dimensions of harm and falseness' where they describe the differences between these three types of information: Mis-information is when false information is shared, but no harm is meant, Dis-information is when false information is knowingly shared to cause harm and the third type Mal-information is when genuine information is shared to cause harm, often by moving information designed to stay private into the public sphere.[329]

They conclude in an extensive analysis of Russian information tactics that all forms of mis-, dis- and mal-information is being used, but that not all amplifiers of Russia's message are aware of their role in spreading false information and eroding democratic trust. They also conclude that "The 2017 French Presidential election provides examples that illustrate all three types of information disorder."[330] Independent experts estimate that at least 6% of all French-election tweets included fake news that reached millions through amplification by bots and actual social media users. Social media companies have estimated that around 8-15% of active accounts are fake accounts.[331] Another report estimates news outlets and social media categorically fail its readers by amplifying false messages and failing to fact-check statements.[332]

Again, Russia specifically targeted frustrated minorities and controversial matters for example with news of system mistreatment and police abuse, flaming sentiments of system failure. The only missing link in this study, evidence that has yet been established with hard data, is connecting the ads to actual voter behavior. Based on the anonymous total outcome the evidence suggests that where those ads were published, an increased number of voters cast their ballot according to the message.[333]

Another example of Russia's information disorder was to use viral campaigns to silence women during the #metoo movement and during the Kavanaugh Supreme Court hearings. The viral messages appealed to women's solidarity, asking them to participate in a social media blackout for 48 hours in protest of social media(?) while donning a black profile picture. The message has been ruled a hoax and is nearly identical to evidence published by

[329] Wardle and Derakhshan, 2017.
[330] Wardle and Derakhshan, 2017. Desigaud et al., 2017.
[331] Valeriano and Maness, 2019.
[332] Gertz and Savillo, 2019.
[333] Schmidt, 2017. Hay, 2019.

Facebook to the US Senate containing Russian ads and messages. It is in my opinion an obvious attempt at silencing women at a moment they were using social media to organize and protest sexual harassment, a sore topic for Trump.[334]

The intelligence agencies of USSR and later Russia have for decades used similar tactics to get protestors to participate in false protests and to wear specific markers or clothing with the purpose in mind to make it easier to target, arrest and 'disappear' those people later, digitally or physically as the examples have shown.[335]

Because of its expertise, how relatively inexpensive online-ads are and the nature of the Cyber-medium Russian operatives "succeeded beyond their wildest dreams and at minimal cost".[336] Additionally, mounting evidence confirms that Russia has targeted electoral systems from voter registration to voting machines in several democratic countries, the US, UK and France included.[337]

Now let's look at the evidence supporting Zarate's claim that Russia had attacked democracy using "information and influence operations and Cyber tools to achieve three important and complementary goals:

- To undermine faith and confidence of democracy and its institutions from within;
- To exacerbate social and political divisions advantageous to Russian interests, including in furtherance of Russian foreign policy or simply to undermine Russia's enemies and opponents; and
- To take advantage of 21st century information environment to obfuscate or confuse the truth and amplify narratives that align with Russian interests, even when patently false."[338]

[334] Kozlowska, 2018.
[335] Lucas and Pomeranzev, 2016.
[336] Ioffie, 2017.
[337] Greenberg, The NSA Confirms it: Russia hacked French Election 'Infrastructure' - The Wired, 2017.
[338] Zarate, 2017.

Undermining Democratic Institutions

The methods Russia uses to "undermine faith and confidence of democracy and its institutions from within"[339] is done by attacking democratic decisions, processes and institutions, for example through smear campaigns as was done when NATO started a phase of Eastward expansion. One of the first examples of Russia's Cyber-aggression was a 2007 Cyber-onslaught on Estonia that crippled government institutions following a symbolic change in Estonia's military allegiance and a vicious smear campaign against NATO in Finland that has been moving closer to joining the alliance.[340]

One Russian troll said in an interview on Russian TV: "Our goal wasn't to turn the Americans toward Russia […] Our task was to set Americans against their own government: to provoke unrest and discontent, and to lower Obama's support ratings."[341]

Russia has attacked political candidates in other countries through hacks and leaks, most famously in the case of Hillary Clinton and her 2016 presidential campaign which was achieved with thousands of spear-phishing and social engineering attacks where party and campaign staff were tricked into opening files that logged their password which then provided access to campaign emails and drives.[342] The data that was acquired was then used in turn for further attacks based on campaign information on weak areas, demographics and topics. In a similar fashion 90 UK parliament email accounts were hacked in 2017, Macron's campaign was hacked and in France and Bundestag members in Germany.[343] Every major agency, party, candidate and media seems to have been hacked in addition to voting machines in France and USA. Russia has done everything in its power to silence 'defectors' and whistleblowers. [344]

Another example is Donald Trump's false claim that millions of 'illegal aliens' voted in and influenced the US elections[345], a misrepresentation of the facts that was reported by Russian and US managed 'fake news outlets' that ran the story as true. Next the news was

[339] Zarate, 2017. Aro, 2015. Pomeranzev and Weiss, 2013.
[340] Aro, 2015. McGuinness, 2017.
[341] Kotlyar, 2017.
[342] Mueller, 2019.
[343] Jensen, Valeriano and Maness, 2019.
[344] It is suspected of several assassinations including the Russian FSB defector Litvinenko and an attempt on Skripol and his daughter, a Russian journalist that fled to the UK. Warrick and Troianovski, 2018.
[345] Jacobson, 2018., Nichols, 2018.

tweeted and re-tweeted by fake accounts, loyal supporters and Russian bots, aimed at specific people who in turn now accept the falsehood as fact.[346]

Macron's party En Marche was the target of deliberately executed attack that consisted of a hack and a timed leak with real and altered information.[347]

> Trolling operations can also be directed at public officials involved in voting processes, and troll networks have been encouraged to develop hashtags and memes to target public officials. Civil society watchdogs and journalists have all been targeted by troll networks during elections, thereby undermining their ability to hold public institutions to account. [348]

The tactics include creation of false news and a virtual reality through an onslaught of news that undermine user's faith in society and justice. This is for example done by perfectly copying popular news sites and setting up news portals that then copy news from other outlets, creating a clone news outlet that publishes real news and false news mixed together in a 60% - 40% ratio, learning by doing that an outlet with too many falsehoods loses credibility.[349]

Assaults and targeting of journalists as enemies of the people has been increasing worldwide, especially from Trump in the US where the situation is 'problematic' with the country slipping down 4 seats on the World Free Press Index.[350] With the US role as a global democratic leader for freedom of speech this development represents a concerning blow. Attacks on journalists are growing, especially when reporting protests. Statistics show that hate-speech and hate-crimes on the rise in both Europe and North-America.[351]

[346] Lucas and Pomeranzev, 2016. Jensen, Valeriano and Maness, 2019. Zabrisky, 2017.
[347] Greenberg, 2017. Matlack and Williams, 2018.
[348] Tenove, et al., 2017.
[349] Pomeranzev and Weiss, 2013.
[350] Wardle and Derakhshan, 2017.
[351] Thomas, 2018.

Creating social rifts

Russia's second mission was to use the Internet Research Agency to execute social media campaigns "designed to provoke and amplify political and social discord in the United States" and "exacerbate social and political divisions advantageous to Russian interests" through numerous Cyber-means.[352]

The Internet Research Agency purchased ads focus on a range of contended issues such as race, police brutality, patriotism, civil rights, Sexual orientation, immigration and economy, frequently sponsoring ads and content on extreme sides of an issue such as with Incels (Involuntary Celibate chauvinists) and feminist groups, or white nationalists and radical civil rights groups.[353]

The messages are usually visual and aimed at invoking feelings of fear and anger. A lot of the messages are simple memes, images of popular icons with messages that reflect current atmosphere and have been defined as "a unit of cultural transmission, or a unit of imitation".[354] They are often simple, humorous and re-enforcing, for example using the same picture over and over again with different captions.

Cyber-users and Social Media companies have an extremely hard time identifying human-managed fake accounts and 'sock-puppets' who hide their origin of internet traffic to create multiple accounts that look real and post 'real' content mixed with propaganda. Those agents are often hired for their knowledge in the local language and they customize the message according to a script to local circumstances and target vulnerable sub-groups in order to maximize its effect on the citizens and politicians.[355]

Some of the IIA tactics are remarkably simple, such as pro-Trump meme with superimposed faces of the candidates on an image of Jesus and the devil arm-wrestling.

Similar discourse attacks have been executed in other countries with varying results and some attributing acts like the New Zealand Christchurch 2019 terrorist act that cost 50 lives as a result of this dialogue and that the attacker designed the assault to go viral. [356]

[352] Zarate, 2017. R. Mueller, 2019.
[353] Emerson, 2017. US House of Representatives PSC on Intelligence, 2018. Grimes, 2017.
[354] Valor, 2017.
[355] Lucas and Pomeranzev, 2016. Confessore, et al., 2018.
[356] Warzel, 2019. Warrick and Troianovski, 2018.

British political commentators point to the effects of Brexit and say that leaving out the economic effects the rift the debate has caused with in the nation will have an even longer effect. Brexit has caused great domestic discontent and a strong pushback from Brits that say they were misled by their own politicians and by incorrect online information that was pushed at them.[357]

The evidence shows that they are correct, with the UK Leave groups spending at least 8 million pounds on social media ads since the campaign started, more than double that of 'stay' groups, with evidence showing financial connections to Russian backers and evidence of campaign finance violations.[358]

> The effects of these techniques used by foreign actors – such as exacerbating social cleavages and distrust, or undermining fair participation and institutional effectiveness – can make democratic countries even more vulnerable to future interference. If such vicious circles continue, and the quality and legitimacy of democracy degrades, then it will become increasingly difficult for democratic states to advance their citizens' interests and resolve social conflicts. [359]

Political Scientists warn that this type of distrust and social friction creates *vicious cycles* that undermine democracy in a spiral of increasing hostility and violence. New research on European news shows that "media narratives about migration are deeply shaped by national press culture" because "[f]rom our perspective, it's more newsworthy if people are abusing the system or exploiting loopholes or abusing the hospitality being extended to them by British society…because that triggers a reaction in readers."[360] When that discourse receives help and amplification from outside forces the odds of violent clashes increase.[361]

However, states are not all equally susceptible to those tactics with Norway and Sweden launching programs to tackling hateful discourse head on with education and counter-discourse.[362]

[357] Hay, 2019. Schmidt, 2017.
[358] Applebaum, 2019.
[359] Tenove, et al., 2017.
[360] McNeil, 2019.
[361] Wardle and Derakhshan, 2017.
[362] Pamment, Nothhaft and Agardh-Twetman, et al., 2019.

"War is peace. Freedom is slavery. Ignorance is strength."[363]

Russia's third achievement has been to "take advantage of 21st century information environment to obfuscate or confuse the truth and amplify narratives that align with Russian interests, even when patently false."[364]

As previously established "Information influence activities are here understood as *the targeting of opinion-formation in illegitimate, though not necessarily illegal ways, by foreign actors or their proxies*. This targeting is used to support and amplify diplomatic, economic and military pressure."[365]

For its own message in December 2013 Vladimir Putin signed an executive order founding „the Rossiya Segodnya multilingual news agency that was to become the main outlet of Russian propaganda for external audiences." Under its branch Russia founded the Sputnik news agency that operates in over 30 languages and consists of news websites and radio broadcasts and the Russian news website LifeNews that includes a news website and 24-hour television channel. Reportedly Russia has been actively seeking bilinguals to work in their 'troll farms' on IIA around the world.[366]

In addition, Russia has founded countless copies of respected news-outlets and no-name news portals that mix fact and fiction into a seamless pro-Russian version of reality. These sites publish un-verifiable 'alternative facts' and information that contradicts official records.[367] Russia's tactics are "[m]ore about ambiguous signaling and amplifying propaganda than it does direct compellence."[368]

Similar methods have been picked up by alleged collaborators within democratic countries, providing sound bites and actual news clips that then get amplified through social media ads, trolls and those who support the message.

This phenomenon of information disruption is probably the most difficult one for social media and public-Cyber debate because it is extremely hard to identify and tackle. When people deny reality and the evidence put in front of them it is extremely hard to

[363] George Orwell in 1984, 1949.
[364] Zarate, 2017.
[365] Pamment, Nothhaft and Agardh-Twetman, et al., 2019.
[366] Sukhankin, 2017.
[367] Mueller, 2019. Kellyanne Conway 2016
[368] Valeriano and Maness, 2019.

establish common ground to start building a public dialogue, which is a critical element of democracy.[369]

"Utilizing a combination of economic, Cyber and information warfare, its purpose is to stoke psychological subversion and increase uncertainty or attrition in a target country or region. "[370]

The ways to obfuscate and confuse the truth take many forms, for example by setting up hoax emergencies like the one in the Columbian Chemicals plant in Louisiana.[371] Another example are news of hate-crimes or mass-shootings that never happened or conspiracy theories that make people distrust their government and news-outlets.

The goal of Russian modern attack methods is not to convince but to create distrust and confusion. "Instead of agitating audiences into action, it seeks to keep them hooked and distracted, passive and paranoid" a tactic used to disorganize and demoralize an opponent.[372] Democracies are increasingly aware of Russian operational activity built around groups like the APT28 which goal is to inflict damage to the reputation and cohesiveness of organizations and alliances such as NATO.[373]

The attacks included campaign hacks where campaign staff members were first identified and targeted with spear-phising and doxing attacks that tricked staff members to click links that installed backdoors that opened hackers way into the system where hacked strategy and campaign data was pulled, analyzed and utilized to then target specific voter groups on specific topics, often by leaking information to selected journalists and outlets, relentlessly hammering weak spots. If a candidate was vulnerable on a specific topic the attack teams would write and distribute misinformation news, posted on identical fake copies of popular and trusted news sites, spreading the links through advertisements and fake accounts on social media.[374] Russian web-programmers and new-media teams set up news outlets; exact copies of Western news outlets on misspellings of the same domains where they mixed selected real news pooled from the original site with fake news written by propaganda editors. Russian IIA used knowledge and theory of human psychology and user

[369] Dryzek, 2017.
[370] Lucas and Pomeranzev, 2016.
[371] Chen, The Agency - New York Times Magazine, 2015.
[372] Lucas and Pomeranzev, 2016.
[373] Shea, 2017.
[374] Lucas and Pomeranzev, 2016. Jensen, Valeriano and Maness, 2019.

behavior to put together targeted news pieces of re-written semi-real news and blatant lies that included information they assumed would feed into the user's confirmation bias.[375]

Russia's information influence operations are in many ways similar to sophisticated multimedia campaigns that major corporations run for their products and services. But Russia's campaigns go further, marrying stolen campaign and voter data with targeted messages, designed to influence people that meet a certain criteria.[376] Through fake SM accounts that target voters and amplify falsehoods they carefully insert the message into networks of colleagues and likeminded Western users, often controversial media personalities like Alex Jones, and opinion makers that spread their news far and wide to social media networks like Facebook, Snapchat and WhatsApp.[377]

Add to that hacks, leaks, extortion, trolls and saboteurs, Russia's coordinated Cyber-IIA utilized several weaknesses in Cyber-law and etiquette revealing *lack of laws and norms*, *flaws in Social Media services* and *vulnerability of democratic discourse*.[378]

For many the largest obstacle here is lack of transparency and responsibility on behalf of Social Media giants, now publicly traded with legal teams that fight government oversight and legislation at every turn. The companies argue from the position of lawlessness for a self-regulating industry that doesn't comply to government rules for mass-media on campaign spending and transparency. SM companies use semantics to argue their position as a platform that merely distributes content and isn't responsible for administration, leaving future SM communication in a legal void.[379]

With the gigantic legal uncertainty and lack of defense facing democratic discourse and political campaigns SM companies need to respond faster and with more cooperation with domestic governments than they have previously done.

[375] Pratkanis and Aronson 2001. Tavris and Aronson 2007. Zabrisky, 2017. Jensen, Valeriano and Maness, 2019.
[376] Rapoza, 2017.
[377] Valeriano and Maness, 2019. Poushter, 2017.
[378] R. Mueller, 2019.
[379] Frenkel, et al., 2018.

6.4 Social Media & Personalized Cyber-Realities

The foreign manipulation of discourse that has taken place online would not have been possible if it were not for the setup of social media and the current legal framework of self-governance.

Because in-depth understanding of social-media advertising has not been common social media companies like Google, Facebook and Twitter have offered major 'advertising accounts' free assistance setting up their social campaigns, providing 'free' dedicated specialists to service top ad-buyers, as part of deepening relationships.[380]

Compared to other advertising spaces social media is relatively inexpensive and is better at reaching target audiences. Given the knowledge, advertisers can cross-examine user-data and campaign information allowing them to target voters with content that will appeal specifically to them. With little oversight on content or who's buying the ads foreign agents can remotely target users from across the world and thus affect the outcome of elections or excite other groups to incite social upheaval.[381]

Social Media companies actively pursued political campaigns as important customers, offering the campaigns assistance in the form of on-site staff that participated in campaigns with deep pockets. These services were however not provided on an equal basis, those who 'discovered' the medium were supported to an extraordinary degree, with Facebook agents forming close ties with candidates. [382]

Over the past decade Facebook, the largest SM corporation and owner of Instagram and WhatsApp, supported political advertisers by providing FB staff to work on-site in political campaign offices, giving input into advertising strategies and helping campaigns set-up messages to targeted users, contributing greatly to the campaign with their expertise on online targeting, message and anything a paid employee of the campaign would usually do.[383]

When that service is not offered on an equal basis, converse to how TV and newspapers try to allocate equal platform to candidates, it creates a very unequal plain field.

[380] Reuters, 2018.
[381] Lucas and Pomeranzev, 2016. Pomeranzev and Weiss, 2013.
[382] BBC, 2018.
[383] Bump, 2018.

The difference between receiving FB specialist help and not receiving it has been supposed a determining factor in some areas between being elected or being invisible to a large portion of the voters.[384]

In many markets this service is deemed to have unjustly influenced the outcome of elections, under accusations of apathy and incompetence Facebook finally responded to the criticism with news that it would no longer provide on-site political ad services, and instead refers everybody to the same online service for support, as many state is what the company should have been doing all along.[385]

Social media has only recently started to reveal limited information in two countries on political spending such as information on who's paying for the ad they're seeing or to look up the ads they've been subjected to. To many it looks like Facebook has been making more efforts to appear like the company is increasing transparency as the project is very limited and provides little actual transparency.[386]

Social Media does not adhere globally to domestic laws that enable governments to enforce law on campaign spending nor does it obey laws that forbid foreign entities to spend money and advertise across borders. Furthermore, local fronts for foreign agents have been hard to trace for local governments, making it extremely hard to enforce campaign laws that ensure that the rules of democracy are followed.[387]

Since Russia's practices became a legal matter for Social Media companies Facebook, Twitter, Google, Instagram and other SM platforms have confirmed that foreign agents were able to spend millions of dollars on online ads with no oversight.

When called upon to answer questions about possible illegal actions through Social Media by Russia and other foreign agents during Congress and Parliament hearings in several democratic countries SM's were extremely reluctant to provide information even refuse to provide answers. But what has been published confirms that campaign spending laws, user privacy laws and laws regarding foreign advertising were broken when some hundreds of millions of users were exposed to Russian Cyber-propaganda.[388]

---

[384] Ioffie, 2017. Miller, Nakashima and Entous, 2017.
[385] Isasc and Wakabayashi, 2017. Reuters, 2018. Politi, 2016.
[386] Constine, 2018. Spence and Di Stefano, 2019.
[387] Tenove, et al., 2017. Spence and Di Stefano, 2019.
[388] Cadwalladr, 2018. Mueller, 2019. The Intelligence Community (FBI, CIA & NSA), 2017.

This lack of information and evidence is a hindrance for democracy to investigate and prevent the tactics that foreign agents use to affect people across borders. After the 2016 US election only Twitter provided information on discarded political accounts, which they claimed to have been negligible with contradicting reports claiming that thousands of troll-spawned tweets were sent to targeted voters. Recently that news has been confirmed with Twitter admitting that it's been purging up to 10 million possible fake new accounts every month, at the expense of its growth numbers. Self-regulation that contradicts monetary interests is one of the largest issues lawmakers and users have with the model of self-regulation SM companies are.[389]

In 2016 FB announced that it would start using third party outlets to vet the content that was shared on the site, but those very same partners have been accused of publishing incorrect information and threatening the lives and safety of journalists themselves while other journalists have severed ties with the SM giant, disillusioned with the corporations' actions.[390] In the world of Deep-Fakes and disinformation experts predict that the need of business of fact-checking and verifying information will grow, for example the Associated Press recently announced its vetting services that include analysis of videos and images .[391]

Social media outlets have been under pressure from law-makers and users to improve their services and work with governments and journalists on correcting and eliminating the stream of incorrect data and to analyze and learn from these mal-information tactics. But official documents from more than one country show Facebook's limited will to cooperate, answer questions or hand over data. Leaks show much resistance within the company to adopt EU regulations, arguing instead that it doesn't need a regulatory push to improve its practices. Officially it claims that it functions well as a self-regulatory body, despite ample claims to the contrary. [392]

Many weaker governments, especially those subjected to Russian attacks have been unable to get more than lip-service cooperation from Facebook. After the 2016 -2017 attacks on European elections and FB being forced to hand over related evidence, the company still fought regulations vehemently. One European Parliamentarian said about

[389] Craig Timberg, 2018. Matthew Field, 2018.
[390] Levin, 2018.
[391] Shanley, 2017.
[392] United Kingdom Parliament Committee, 2018. Cadwalladr, 2018. Solon, 2016.

Russia: “From their impact on election outcomes, to spreading of conspiracies and hate speech, the consistent message has been that regulation would stifle innovation. This is a losing strategy in Brussels.” [393]

Critics have pointed out that Facebook’s efforts seem to have been mostly focused on changing public *perception* of its participation in an image campaign to fight against Information Influence Attacks, instead of changing its *practices* regarding harmful content. “They’ve essentially used us for crisis PR,” one former partner says. [394]

Political ads have brought the company high earnings and are a growing portion of Facebook’s enormous intake, actively going after political campaigns and catering to their needs with on-site staff. FB’s assistance to candidates has opened channels for the company to future policymakers which has proven beneficial. The company paid no taxes in the USA in 2018 and overall SM companies have had a lot of freedom to operate the platforms without much supervision or interference from lawmakers, outside of the EU that is, where the company has been subjected to the most oversight compared to other markets.[395]

In 2018 FB claimed that the company was hiring 20.000 new staff to monitor dialogue and counter fake news and in April 2019 FB announced that it was strengthening its initiative against IIA with a plan called Remove, reduce, inform. “This involves removing content that violates our policies, reducing the spread of problematic content that does not violate our policies and informing people with additional information so they can choose what to click, read or share.”[396] The efficacy of the program is untested but in an official statement in April 2019 Facebook was unusually direct about the menace of fake discourse.

> Over the last two years, we’ve greatly expanded our efforts to fight false news: we’re getting better at enforcing against fake accounts and coordinated inauthentic behavior; we’re using both technology and people to fight the rise ´in photo and video-based misinformation; we’ve deployed new measures to help people spot false news and get more context about the stories they see in News Feed; and we’ve grown our third-party fact-checking program to include 45 certified fact-checking partners who review content in 24 languages. And overall, we’re making progress: multiple research studies suggest that these efforts are working and that misinformation on Facebook has been reduced since the US presidential elections in 2016.[397]

[393] Kayali, 2019.
[394] Levin, 2018., Kayali, 2019.
[395] Solon, 2016.
[396] Facebook, 2019.
[397] Silverman, 2019.

This announcement was made two weeks after a white supremacist attacked a mosque in New Zealand killing 50 people while live-streaming it on Facebook. The SM giant announces a ban on all "praise, support and representation of white nationalism and separatism" on Facebook and Instagram. This does not indicate that Facebook has confidence it has eradicated or covered the problem, but it indicates an effort.[398]

At the same time, it seems extremely unlikely that law-makers manage to update campaign laws to fill up loopholes before the next election with more news coming in of election hacks all over the world by Russian authorities.

Additionally, there are plenty of ad marketplaces outside of social media that have no oversight where Russia can easily amplify its message and advertise political material and fake news portals. These marketplaces operate across countries, regions and languages and have little or no oversight. Ads are often not approved by humans and only checked if users report. Currently it is virtually impossible for world governments to get those marketplaces to comply with local advertising law or have oversight on campaign finances.[399]

Private-Public partnerships for Cybersecurity have worked for some areas of Cyberdefense but they leave huge gaps as the case has clearly demonstrated. The evidence shows that SM has neither been able to ensure that it respects the domestic laws that apply to their operations, nor that it has any interest in doing so with corporate executives skirting all questions on the subject.[400]

More worrying is how little information is available from service providers about whether and how they've been targeted. A large portion of the evidence is provided by whistleblowers because the public and very few governments have the ability to spot propaganda and request accountability. A lot of IIA tactics are however not necessarily illegal and require a judgement call from appropriate authorities whose jurisdiction is still being debated.[401] Until a solution is found governments and global institutions are at loss protecting public discourse, social cohesion and democracy itself. [402]

[398] Facebook, 2018., Sandberg, 2019.
[399] Spence and Di Stefano, 2019., Gertz and Savillo, 2019.
[400] Gertz and Savillo, 2019.
[401] Valeriano and Maness, 2019.
[402] Popken, 2018.

7 IR Theory and Cyberthreats

> There is a war happening. We are immersed in an evolving, ongoing conflict: an Information World War in which state actors, terrorists, and ideological extremists leverage the social infrastructure underpinning everyday life to sow discord and erode shared reality. The conflict is still being processed as a series of individual skirmishes – a collection of disparate, localized, truth-in-narrative problems – but these battles are connected.. [...]This is a kind of warm war; not the active, declared, open conflict of a hot war, but beyond the shadowboxing of a cold one.[403]

Up until very recently academic understanding of Cybersecurity and Cyberpower has been provided largely by financial and information security research and military theory, as previously discussed in relations to the P/DIME model. The field is now receiving new input through largely unofficial contributions by information-cognition studies enabled by Big-Data and fMRI studies, regrettably with less focus on access for political/diplomatic studies and theorization of Cyberspace.[404]

Cybersecurity is customarily seen as the study of systems and attacks on said systems with a view has followed realist principles, that the intent of attackers is to make financial gain or hold information for ransom. This focus has largely neglected the social element of Cybersecurity and how people and ideas are affected by and through Cyberspace. [405]

Current international affairs demonstrate there are many opportunities for political scientists to test theory and join hands across new academic traditions to gain insights and in cooperation develop, test and further theory of mass-social change.

That does not mean classical theoretical views aren't relevant to Cybersecurity studies, but this thesis agrees with academics that claim it is time for new theories to emerge along with new phenomena and let old ones to be put to the test.[406]

With recent changes in Cyberattacks and claims of looming Cyber-warfare contributions are needed from academia and civil society to assist peaceful solutions and insights that help democratic governments decide what repercussions and actions should be taken against Cyber-threats.

[403] DiResta, 2018.
[404] Stevens, Global Cybersecurity: New Directions in Theory and Methods, 2018.
[405] Starr, 2009. Stevens, Global Cybersecurity: New Directions in Theory and Methods, 2018.
[406] Stevens, Global Cybersecurity: New Directions in Theory and Methods, 2018

7.1 Theoretical Analysis of a Problem

Realist theory of power politics and peaceful Institutional theory of cooperation provide convincing insights into the development of Cyber International Relations.

Acknowledging Cyberspace as a space on pair with air, land and sea as NATO recently did confirms that IR theories have validity for their theoretical insights that explain and predict developments in different areas of Cyberspace, but more importantly for IR theory it also acknowledges the fourth level – the social level – of Cyberspace as a battle field. [407]

Classic IR theory has repeatedly proven its explanatory value on global developments. Realism and the quest to maximize national interest fits well in accounting for current global Cyber-contention and information wars in Cyberspace, an environment defined by anarchy as previously discussed. Institutionalism has similarly had great theoretical value explaining peaceful institutionalization of Cyberspace and the implementation of the Multi-stakeholder model of Internet Governance. [408]

However both Realist theory and Institutionalism lack explanations for agency and the role of change which has led to an idealistic-constructive turn within the school of IR theory led by Alexander Wendt's theorization on the study of anarchy and Vivien Schmid's theorization on Discursive institutionalism which has developed into a framework for idealistic analysis of institutional change and political rhetoric.

> In discursive institutionalism, ideas and discourse may appear in different forms, be articulated through different kinds of arguments, come at different levels of generality and change at different rates. Moreover, such ideas and discourse may be generated, articulated and contested by 'sentient' (thinking, speaking and acting) agents through interactive processes of policy coordination and political communication in different institutional contexts (Schmidt 2008, 2011, 2012). [409]

The work on discursive institutionalism is particularly influential for it includes many of the constructive elements that apply to Cyberspace and its institutionalization through the undeniably discursive Multistakeholder model.[410]

However: "the three neo-institutionalisms of rational choice, historical, and sociological institutionalism – leave us completely unprepared to explain these 'interesting

[407] Klimburg and Mirtl, 2012.
[408] Kirshner, 2009. Abdelal, 2009. Hay, International relations theory and globalization, 2013.
[409] V. Schmidt, 2008. V. Schmidt, 2015.
[410] V. Schmidt, 2010. V. Schmidt, 2008. V. Schmidt, 2015.

times', since they have mainly been focused on continuities based on rationalist interests, path dependent history, and cultural framing."[411] To rational theories "ideas have held a beleaguered status, often derided as imprecise or placed lower in status than material interests as motives for political and social action."[412]

This study postulates with Schmidt's theorizing on constructive institutionalism "it seeks to identify a discursive sphere within which practitioners of these varied approaches can discuss, deliberate, and contest one another's ideas from epistemological, ontological, methodological, and empirical vantage-points."[413]

Discursive institutionalism is a branch of 'constructive institutionalism' that fits the main argument of this thesis *that the 'fourth space' is predominantly governed by constructivism* and that constructive theorizing will provide new insights into the analysis of Russian attacks on Democracy through Cyberspace.

This thesis hypothesis that actors in Cyberspace operate within a constructed reality where ideas based on cognition and *perceptions* matter just as much as 'reality'. It postulates that Cyber-actions and Cyber-perceptions follow the principles of Constructivism where human's act on the information that's available to them and by doing so even false realities *become real in their consequences*.[414]

"The problem with the older neo-institutionalisms is not simply that they give no space to ideas and discourse but that in so doing they are unable to explain the dynamics of institutional change (and continuity) „ [415]

It must also be noted that Realism is highly relevant for explaining motives and agency, assuming interest-based rationality guiding Russian state actors to systematically champion certain beliefs across borders and at key junctions in politics, but it has an extremely dualistic view to human decision-making, assuming rational decision making guiding some people while taking advantage of irrationality in others.[416]

---

[411] V. Schmidt, 2011.
[412] Béland and Cox, 2010.
[413] V. Schmidt, 2011.
[414] Béland and Cox, 2010. . Blyth, Routledge Handbook of International Political Economy (IPE). IPE as a global conversation, 2009. Wendt 1992.
[415] V. Schmidt, Speaking of change: why discourse is key to the dynamics of policy transformation, 2011.
[416] Wendt 1992. Blyth, Great Transformations: Economic Ideas and Institutional Change in the Twentieth Century 2002.

> for all the emphasis placed on them in contemporary models of political economy, vested interests play a considerably less-determining role than appears at first sight. Indeed, because of their neglect of ideas, political economy models often do a poor job of accounting for policy change.[417]

'Classic' Cyberattacks on state infrastructure and information systems have routinely been the main focus of security studies, however they are currently not the main Cybersecurity problems facing democracies. Security experts agree that the human element poses a significant role in Cybersecurity, but its role may have been underestimated.[418]

But the human element is even more important as Schreier outlines in three dimensions of information operations: The physical platforms, systems and infrastructures that provide *global connectivity* to interconnect information systems, networks, and human users; the massive amounts of *informational content* that can be digitally and electronically sent anywhere anytime to virtually anyone; and the *human cognition* that results from greatly increased access to content, which can have a dramatic impact on human behavior and decision making.[419]

Information Influence Cyber-attacks and public discourse is to an ever-increasing degree influenced and affected by manipulation of human cognition and events taking place in Cyber-realities. These Cyber-events and perceptions paint a picture of the world that counters reality while shaping real-world choices, including public debates and voter choices.[420]

The increased focus on human cognition is a reactive Constructive turn in Cybersecurity that attests a change in Cyberthreats to democratic processes. This change reflects the constructive nature of Cyberspace and marks a shift in the *official acceptance of Cyberspace as a conceptual space*.

[417] Rodrik, 2014.
[418] Hadlington, 2017. Kramer, Starr and Wentz, 2009.
[419] Schreier, On Cyberwarfare, 2015.
[420] Schreier, On Cyberwarfare, 2015., Béland and Cox, 2010.

7.2 Constructivism – an Idealistic turn in International Relations

The case in question relies heavily on the power of ideas and discourse, particularly seeking the explanatory value of deliberate-democratic theory and frameworks developed by discursive institutionalism.[421]

Ideas and discourse are hard to separate, Plato elaborated the illocutionary power of ideas arguing that somehow thoughts and ideas gained power and became ‚real-er' from thought to utterance. Political thought largely revolves around communal action and therefore needs dialogue in order to bear fruit.[422]

The contribution of Discursive Democratic Theory is opening Political Science to the focus on the *power of discourse* in the areas of building consensus and establishing legitimate decision-making institutions.[423]

For ideas to gain power they require the utterance of an idea. "Then, these ideas need to be linked to a specific outcome, which also can be measured. The idea must capture the attention of actors who advocate for it, and successfully use it to influence the observed outcome. A similar logic can be employed to examine ideas that fail."[424]

> The basic problem that social actors face is that we do not actually see the generators of reality, but we see only their outcomes. Those outcomes are always mediated by human agents, which invites variation and uncertainty into the mix. Recognizing this does not mean that we have to draw a hard and fast distinction between the physical and social worlds, however.[425]

I align with Constructive theorists and claim that in democracies ideas rather than interests are considered at the core of decision making and in doing so *treating interests as one set of ideas.* Social and psychological research has shown that some people don't operate out of rational self-interest as economic and political models would predict, people are vastly more complicated, and examples repeatedly show that actors can be convinced to vote against their own self-interest.[426]

---

[421] Warren 2017, Blyth 2002, Blyth 2007, Hay 2013, Schmidt 2008, Schmidt 2011
[422] Ketchum, 1980.
[423] Warren 2017 pp 40.
[424] Béland and Cox, 2010.
[425] Blyth, 201, pp 89.
[426] Cohen, 2009. Blyth, Routledge Handbook of International Political Economy IPE. IPE as a global conversation, 2009.

Constructive theory holds that motives and events affect actors and institutions unevenly with varying outcomes that are additionally influenced by actors, chaos and circumstances.[427] Here lies the ability to explain why certain types of rhetoric or logic influences and excites some, while others become more skeptical.

An acknowledgement of the importance and vulnerability of discourse is needed. A discussion of the power of ideas that is intended to supplement for the disadvantages of "The three neo-institutional-isms of rational choice, historical, and sociological institutionalism [which] have mainly been focused on continuities based on rationalist interests, path dependent history, and cultural framing" [428]

To acknowledge the importance of ideas in change is to accept the unique theorizing of *ideational scholars* that people's choices are shaped by the ideas people hold and debate with others. These ideas, in turn, are based on *interpretations* people have of the world, their own interests and their surroundings.

Like Deliberate Democratic Theorists I see interests as influential on discourse, I argue along Constructive lines that interests are *a set of ideas* that influence actor's behavior within the global system. Contrary to Rationalist theorizing, Constructivism doesn't see interests as fixed, but argue that often interests change depending on actors, circumstances and perspectives. The behavior of both people and states can be affected by altering both their *perceived interests* as well as their *perception of interests*.[429]

[427] Wendt, 1992
[428] V. Schmidt, Speaking of change: why discourse is key to the dynamics of policy transformation, 2011.
[429] Béland and Cox, 2010.

7.3 Ideas and Discourse

I maintain that we must next look towards the unique theorizing of *ideational scholars* when looking at people's behavior (in Cyberspace) who claim that people's "choices are shaped by the ideas people hold and debate with others. These ideas, in turn, are based on interpretations people have of the world and those around them. There is an objective reality, but it lends itself to many interpretations that open endless options for human agency. For this reason, the outcomes of any process of change are contingent, and realities are created as perceptions become „real in their consequences"[430].

This is a position of a *socially constructive* understanding, not only are our opinions based on 'unreliable' interpretations of a fabricated world, but both our understanding of reality and reality itself is constructed. Or as Blyth articulated:

> The basic problem that social actors face is that we do not actually see the generators of reality, but we see only their outcomes. Those outcomes are always mediated by human agents, which invites variation and uncertainty into the mix. Recognizing this does not mean that we have to draw a hard and fast distinction between the physical and social worlds, however.[431]

I argue that this view is in line with Habermas's view of discursive democracy which: „is a primarily a theory of communicative responses to disagreement, preference formation, and collective will formation, focused on mediating conflict through the give and take of reasons."[432] What the recent Cyber-attacks have however given us a chance to explore is to view the ‚levers of power' that are at play in politics and track ideas through their spread online.[433]

While agreeing with Habermas on the importance of discourse I find his premise that people are interest seeking, reasonable and rational too simplistic, and argue instead along Constructive lines that people are governed by the ideas that they hold about the world, *including their ideas on self-interest*:

"Ideas are subjective claims about descriptions of the world, causal relationships, or the normative legitimacy of certain actions."[434]

---

[430] Merton 1948.
[431] Blyth, 2010, pp 89.
[432] Habermas 1996. in Warren, 2017.
[433] Starr, 2009.
[434] Campbell, 1998. pp 3.

Ideas shape identities, shape perceptions of interests, institutions and the actions people take. Ideas create a world-view and they're not all created equal. Ideas affect how actors align themselves on issues and they affect how actors evaluate their surroundings and choices. Ideas furthermore afford power to actors, and when the ideas are embedded in institutions, they also institutionalize, even legitimize power differentials.[435]

Applied here is the unique theorizing of ideational scholars that examine the importance of people's "choices [which] are shaped by the ideas people hold and debate with others. These ideas, in turn, are based on interpretations people have of the world and those around them. There is an objective reality, but it lends itself to many interpretations that open endless options for human agency. For this reason, the outcomes of any process of change are contingent, and realities are created as perceptions become „real in their consequences"[436]. They are not predetermined and cannot be predicted."[437]

The contribution of Discursive Democracy is focus on the *power of discourse* in building consensus and establishing legitimate decision-making institutions.[438]

> „Habermas distinguishes between opinion formation in the informal public sphere and will-formation in formal representative institutions, placing emphasis on the transmission mechanisms between the two spheres of activity.[439]

Some Democratic theorists have raised their objections to the deliberative democratic model of assembly and negotiation because it is used to "justify ideological domination because deliberation (in effect) alters individual consciousness under the coercive pressure of collective action"[440] This view assumes that humans contain some sort of ‚pure ideas' that must not be tampered with, which is an impossible ground to defend, given that humans are social beings that are unintentionally and intentional influenced by others. To assume a 'pure ideological state' is to assume idealistic anarchy, which leads to abuse when ungoverned as has been previously discussed.

[435] Béland and Cox, 2010.
[436] Quote from Thomas with similar theorizing in Blyth 2007, Merton, 1948, p1.
[437] Béland & Cox, 2010.
[438] Warren, 2017 pp 40
[439] Owen and Smith, 2015.
[440] Warren, 2017.

The spark for Constructivist theorizing towards the end of last century was reconcile the interaction between identities, ideologies and interests in International relations, a theory on how interests were not taken for granted but a social construct.[441]

The power of discourse to change minds and incite actors can be theorized as revolving around ideas alone, or as theorized by „[s]cholars such as Foucault (2000), Gramsci (1971), Lukes (1974) and Laclau and Mouffe (1985) [who] have similarly emphasized the central role of ideas in relations of power, be it as discursive formations, hegemony, ideology or the production of subjectivity.“[442]

In addition to inter-disciplinary findings, that include psychological, cognitive and media studies[443], I argue that more factors are at play such as human ‚blind spots', framing, actor's electability and convincing capabilities and the medium itself which in synergy help to influence people and reveal *the power of ideas to incite action*.[444]

Ideas are both *indigenous* and *exogenous* to institutions and attempts to influence ideas won't lead to the same outcomes at different junctions in time under different circumstances. This acknowledgement accounts for different outcomes in different countries that have been subjected to similar ideational assaults. Whether agents are incited through their own blind spots, other's convincing capabilities or the context, placement and phrasing of online ads, the bottom line is that somehow actor's *ideas have been influenced.*

This view reveals for examination *ideational power* above other types of power such as military, structural, institutional, economic etc. which certainly matter, but are not the focus of our examination.

[441] Wendt 1992.
[442] Carstensen and Schmidt, 2015.
[443] Kahneman & Tversky, Tversky & Aaronson
[444] Carstensen and Schmidt, 2015.

7.4 Ideational power

Ideational power is defined as: „the capacity of actors (whether individual or collective) to influence actors' normative and cognitive beliefs through the use of ideational elements." [445] I argue that ideational power has not only bottom-up and top-down elements but is three dimensional with peers influencing peers and 'thought bubbles' in one place influencing thought bubbles elsewhere

This connection between ideational power and power of discourse in Habermas' formation of *opinion*- and *will* is highly important for creating democratic norms and institutions – in creating democratic action.

Carstensen & Schmidt theorize that ideas have three types of „ideational power"; Power *through* ideas, power *over* ideas and *structural*/institutional power.[446] Carsten and Schmidt define *power through ideas* as the ideational convincing capabilities of actors to influence other actors' cognitive ideas and normative world-views. *Power over ideas* they outline as compulsory power or restraints over options or ‚imposition of ideas', which sounds close to what cognitive and linguistic scholars describe in relation to discourse as a ritualistic ceremony where some ideas fit and others simply aren't considered because they cause too much discomfort.[447]

Secondly in relation to of power over ideas are the imbalanced power-relations that arise when people don't have freedom of discourse; when one actor forbids others to express or broaden their ideas, when one group of people is shamed or punished for holding (a set of) ideas, typically those in power, refuse to consider alternative ideas. Third type of ideational power is institutional power when actors are able to force their ideas onto others through institutions and by institutionalizing their ideas. Our case demonstrates such power imbalances where users and voters have little power over the ideas that are being pushed onto them.

If people believe they operate in an environment where actions have no consequences Realism assumes that actors will act out of self-interests, and that contention will rule within the arena with weaker actors typically aligning themselves with stronger

[445] Carstensen & Schmidt, 2011.
[446] Ibid.
[447] Tavris and Aronson, 2007. Wardle and Derakhshan, 2017.

actors in order to seek protection. Realism also accounts for Institutionalism and behavior that fosters cooperative action as a sensible strategy for actors that hold less power. If actors operate in an environment where cooperation and the rule of law are norms, they are more likely to act according to institutional theory while trying to sway the behavior of institutions to represent their own self-interest through negotiations.[448]

> "Discursive institutionalism also lends insight into questions of power, including how ideational agents have been able to use their persuasive power *through* ideas to channel people's anger while challenging experts' power *over* ideas as they upended the long-standing power in ideas of the liberal order. "[449]

Russia has clearly managed to utilize the power of persuasion and privatized virtual realities to advance its Cyber-power – but *how*?

[448] Schmidt, 2011.
[449] Schmidt, 2017.

8 Constructive Theory & Cyberattacks

> The aide said that guys like me were "in what we call the reality-based community," which he defined as people who "believe that solutions emerge from your judicious study of discernible reality... That's not the way the world really works anymore," he continued. "We're an empire now, and when we act, we create our own reality. And while you're studying that reality — judiciously, as you will — we'll act again, creating other new realities, which you can study too, and that's how things will sort out." [450]

8.1 Constructive Theory

There is a significant harmony between the ideas of democratic theorists and constructive theorists in their view towards power; Democratic Theory views agents and 'communal power' as the force for change while Constructive Theory sees agent's ideas as the driving force: "In ontological terms, the basic tenet of the ideational perspective is that the social world is constructed: ideas form the foundation of this construction and are often the inspiration to act."[451]

„Discursive institutionalism lends insight into questions of power, including how ideational agents have been able to use their persuasive power through ideas to channel people's anger while challenging experts' power over ideas as they upended the long-standing power in ideas of the liberal order. "[452]

While certainly broad, I argue that a Constructed theoretical view is the premise to analyzing Russia's Information Influence Attacks. The goal of Russian state elites is to hold and gain power through any means possible and Cyberspace provided opportunities to exercise discursive power and control through manipulation of ideas. This is a clear attack on democracies foundation of communal power based on rules of fairness and equality and the belief that somehow 'the best' ideas will prevail because they'll be the ones that gain most communal support.[453]

In order to review the methods and ideas represented in the Russian IIA content I argue for the use of a two dimensional ideational framework that's well theorized within Constructive theory, and check against the framework whether specific types of arguments

[450] Suskind 2004.
[451] Béland and Cox, 2010. V. Schmidt, 2008. V. Schmidt, 2015.
[452] Schmidt, 2017.
[453] Flynn 2004, 3 (4)., Wendt 1992.

were being used on specific types of users in order to hit specific emotional triggers amongst those subjected to the political ads.[454]

8.2 Discursive Institutionalism

Constructive theory and studies on the role of ideas is a growing field within Political theory; in the past ideas have been treated as endogenous to institutions and without distinction, while conversely acknowledged as a force for change. Less is known about how ideas come about, how they spread, what influences them and what influence they have to empower citizens. Through the information collected on human discourse in Cyberspace, we have for the first time tools that can track ideas from utterance to action, but access to that data is highly restricted by its owners that are reportedly using it for monetary purposes, leaving scholars to infer effects through use of supplementary information.[455]

Vivien Schmidt outlines how ideas are the currency for discursive political processes. Discourse begins among people who hold different opinions and interpretations, and who learn and refine their ideas as they share them with others. Viewing politics as a discursive process means that it is not a mechanical process whereby actors formulate an interest or a goal, devise a strategy to achieve the goal, and struggle with others as they employ their strategy. Rather, drawing on existing cultural and ideological symbols, actors develop a set of ideas and share them with others, who may challenge these ideas and provide some alternatives. Discursive interactions prompt them to refine, reframe, and reinterpret these ideas. Not only is this iterative and sometimes contentious discourse in play between actors"[456]

For the discussion of ideas, we view them through a theoretical Constructivist framework that categorizes ideas according to a 'theory of mind' that assumes political ideas fall into a two dimensional framework for ideational analysis, distinguishing between *cognitive* and *normative* types of ideas, on the levels of *policy*, *programs* and *paradigms*.[457]

[454] Hay, 2019. Schmidt, 2017.
[455] O'Sullivan and Griffin, 2019. Naffi, 2017. US House of Representatives PSC on Intelligence, 2018.
[456] Béland and Cox, 2010.
[457] Schmidt, 2008.

"*Principled beliefs* are essentially the normative bases and justifications of particular decisions, while *causal beliefs* are beliefs about means-ends relationships."[458] Normative ideas attach values to political action and serve to legitimate the policies in a program through reference to their appropriateness", while cognitive ideas focus on *how*.[459]

„Whereas both policy ideas and programmatic ideas can be seen as foreground, since these tend to be discussed and debated on a regular basis, the philosophical ideas generally sit in the background as underlying assumptions that are rarely contested *except in times of crises*." [460]

The framework provides a scheme to (better) understand ideas, giving us a tool to analyze constructively what type of ideas are being attacked through Russian information and idealistic attacks.

[458] Blyth, 2007 pp 14. Hall 2003. Goldstein and Keohane, 1993. Bottici, C. and Challand, B. 'Rethinking Political Myth. The Clash of Civilizations as a Self-Fulfilling Prophecy', European Journal of Social Theory 9(3), 2006, pp. 315-336.
[459] V. Schmidt, Discursive Institutionalism: Understanding Policy in Context, 2015. Schmidt, 2011.
[460] V. Schmidt, Discursive Institutionalism: Understanding Policy in Context, 2015. pp. 306

The following framework is in line with similar Constructive theorizing made by scholars such as Campbell, Hall, Hay, Goldstein & Keohone and Mark Blyth.[461]

Table 4 - Adjusted Constructive Framework for Ideational Analysis[462]

	⇒ **Types of ideas** ⇒ ⇓ **Level of generality** ⇓	**Cognitive ideas** - are constitutive of interests -"what is and what to do,"	**Normative ideas** - appeal to values. - "what is good or bad in light of "what ought to do."
Foreground ideas	**1. Policies** or "policy solutions" proposed by policy makers. (first order)	Cognitive ideas speak to how policies offer solutions to the problems at hand.	How policies (appear to) meet the aspirations and ideals of the general public.
	2. Programs that underpin policy ideas. (second order) Programmatic ideas define the problems to be solved by policies; the issues to be considered; the goals to be achieved; the norms, methods, and instruments to be applied; and the ideals that frame the more immediate policy ideas.	Cognitive ideas speak to "problem definitions" that set the scope of possible solutions to the problems that policy ideas address. how (second level) programs define the problems to be solved and identify the methods by which to solve them, and how both policies and programs mesh with the deeper core of philosophies (third order)	*Normative ideas* speak to how programs as well as policies resonate with a deeper core of (third level) principles and norms of public life, whether the newly emerging values of a society or the long-standing ones in the societal repertoire.
Background ideas	**3. Paradigms** are constitutes of philosophies that reflect the underlying assumptions or organizing principles orienting policy (Third order)	Serve as as f*rames of reference* that enable policy actors to (re)construct visions of the world that allow them to (re)situate themselves in the world; *as "programmatic beliefs" that operate in the space between worldviews and specific policy ideas;as "policy cores" that provide sets of diagnostics and prescriptions for action;	*Normative principles* that represent a deeper core of (third level) principles and norms of public life, whether the newly emerging values of a society or the long-standing ones in the societal repertoire.

Schmidt has used the Discursive Institutional framework above to analyze the discourse surrounding the Brexit referendum and in the following chapter I follow her treatment on evidence provided by Facebook on advertisements and content distributed by Russian trolls in the 2016 US presidential elections.

[461] Blyth, 2010., Blyth, 2006., Hall, 1993. .

[462] Complemented version of Schmidt's 2008 model for discursive institutionalismand ideational analysis. Schmidt, 2008., Hay, International relations theory and globalization, 2013.

8.3 Ideational Analysis of Russia's Information influence Attacks

Table 5 shows the results of an Ideational Analysis of content posted by Russia on Facebook 2015 to 2017.[463] Access to more data would give scientists deeper insights into the tactics used to attack discourse, but the data-sets provided by Facebook to the US Congress were sufficient for analysis. In the following discussion it is supplemented by evidence, testimonials and reports by law enforcement, intelligence agencies and public institutions.[464]

Table 5 - Applied Constructive Framework for Ideational Analysis[465]

[466] ⇓	**Types of ideas ⇒** **Level of generality ⇓**	**Cognitive ideas** - are constitutive of interests -"what is and what to do,"	**Normative ideas** - appeal to values. - "what is good or bad in light of "what ought to do."
Foreground ideas	**1. Policies** or "policy solutions" proposed by policy makers. (first order)	The material did not speak on or criticize *details* in policy, rather it painted a picture of sysemic failure and abuse by the system towards certain groups e.g. black people, women, LGBT and white supremacists invoking feelings of self-protection.	The material targeted how policies *failed* to meet the aspirations and ideals of the targeted public. Examples included emotionally charged posts on immigration, police brutality, sex crimes and inequality.
	2. Programs that underpin policy ideas. (second order)	The content used emotionally charged content, faces and lies to demonize programs but did not discuss details of policies. Distrust in institutions and their data. Inciting feelings that the system is a failure	The posts used charged language on controversial programs, programs failing in emotional language with frustration ("something must be done")
Background ideas	**3. Paradigms** are constitutes of philosophies that reflect the underlying assumptions or organizing principles orienting policy (Third order)	*Systematic destruction of benchmarks on truth*, facts and f*rames of reference.* Instead *Paradigm confusion* is designed to deny actors a firm standing and to situate themselves in reality. It demonstrated attacks on "programmatic beliefs" and "policy cores" through confusion, trolling and denial of public records and verified info	Targeting *Normative principles* with emotional language: Us vs. Them, demonizing a messenger Aggregating frustions, normalizing charged discourse, re-enforcing social rifts and inciting confrontation

An analysis of ads and posts by Russian agents on Facebook, Twitter and other SM platforms show that the material is remarkably simple in its polarizing message. The content

[463] US House of Representatives PSC on Intelligence, 2018.
[464] See R. Mueller, 2019. and bibliography
[465] Complemented version of Schmidt's 2008 model for discursive institutionalismand ideational analysis. Schmidt, 2008., Hay, International relations theory and globalization, 2013.
[466] Schmidt, 2008.

whether it's text, video or imagery appeals to *normative ideas* and *feelings* rather than *cognitive-rational* decision making, this is for example done by triggering fear amongst minorities and indignation amongst racial extremists.[467]

The content analysis reveals that Russia's propaganda is extremely focused on *demonizing leaders* and '*shooting messengers'*. It viciously targets groups, political candidates, journalists, the media and unnamed individuals through truth and outrageous lies by appealing to impulsive feelings of anger, disgust, superiority etc.*[468]*

That does not mean the content didn't contain ideas or idealistic attacks on *programs*, *policies* and *paradigms*: Looking at the level of *policies* the posts rarely discuss practicalities or nuances of policies that appeal to cognitive evaluation of practices. When the posts address policies*,* they highlight practical failures that demonstrate *flaws in the system* that invoke emotional responses; for example that S-American gang members are invading the USA or that Muslim terrorists are infiltrating Europe, putting the reader in danger for their physical safety (rather than their economic security or interests). The rhetoric is normative and contains language and imagery that is intended to appeal to feelings of outrage, superiority, indignation, fear and anger.[469]

> The votes in the UK and the USA attest to strong desires to register protest against the sitting parties, the elites and the establishment. The votes were also a protest against citizens' growing sense of loss of control as a result of the removal of more and more decisions from the national to supranational level, whether to international institutions because of increasing globalization in the case of the USA, or to the EU because of increasing Europeanization in the case of the UK.[470]

This is in harmony with Constructive works on people's innate fear of 'The Other' and how those ideas have repeatedly been invoked *through the use of idols* as part of political agenda and propaganda aimed at pitting groups together. History and Constructive theory have both demonstrated how this polarization of groups and creation of 'political myth' can easily lead to societal discord and violence. [471]

Looking at propaganda relating to *programs* the message is focused on the failure of programs, pushing for new programs based on normative paradigm shift. They claim

---

[467] US House of Representatives PSC on Intelligence, 2018.
[468] Zabrisky, 2017. Pomeranzev and Weiss, 2013.
[469] Wardle and Derakhshan, 2017.
[470] Schmidt, 2017.
[471] Bottici and Challand, 2006.

immigration programs have failed and that new programs are needed to solve the pressing problems that immigration poses to society by misrepresenting both the danger and the performance of these programs. The language is normative and calls for new solutions to made up problems, that cannot be solved because they don't really exist.

> Support for leave has now been shown to correlate strongly (whether using individual or district-level data) with low educational attainment, low income, age, recent increases in (but not aggregate levels of) in-migration, anti-migrant sentiment, political disaffection, prior UKIP and Conservative support, national (as opposed to European or British) identification and, perhaps more surprisingly, low (not high) self-reported Internet and smartphone usage (see Alabrese et al., 2018; Clarke et al.,2017; Goodwin and Milazzo, 2017; Hobolt, 2016). Finally, and in part through these various analyses, the vote for leave has come to be widely characterised as a vote of those 'left behind' by globalisation (Goodwin and Milazzo, 2017; Hopkin, 2017; see also Ford and Goodwin, 2014).[472]

It is my view that the *ad hominem attacks* of Russian IIA are ill fitted for the Idealistic Framework of Discursive Institutionalism because the attacks lack ideas. Whatever Russia's motives may be for launching the attacks I argue that in order to analyze them we need to study them less as *ideas* and more as virtual-reality-making *propaganda* and seek future contributions from Cognitive, Communication and Psychology studies. [473]

Russian *ad-hominem* attacks on journalists and politicians appeal to human prejudice, stereotypes and non-cognitive processes in the human psyche. These ad hominem attacks undermine ideas of human equality and attack democratic norms and institutions. Just like propaganda delivered towards minorities, that often involved news of mistreatment and abuse by the hands of police. They are intended to appeal to human impulses and incite disorder; *to get people to set logic aside and act violently out of prejudice*.[474]

> The most 'successful' of problematic content is that which plays on people's emotions, encouraging feelings of superiority, anger or fear. That's because these factors drive re-sharing among people who want to connect with their online communities and 'tribes'. When most social platforms are engineered for people to publicly 'perform' through likes, comments or shares, it's easy to understand why emotional content travels so quickly and widely, even as we see an explosion in fact-checking and debunking organizations [475]

[472] Hay, 2019.
[473] Zabrisky, 2017. Wardle and Derakhshan, 2017. Tavris and Aronson 2007.
[474] Pomeranzev and Weiss, 2013.
[475] Wardle and Derakhshan, 2017.

8.4 Post-Truth: Deconstruction of Discourse

Looking at cognitive-paradigm ideas the rhetoric focuses on *deconstructing reality* and creating a normative narrative of its own in order to make it impossible to have a meaningful discussion based on a common interpretation of reality.

It can be complicated to connect evidence of *influence, agency* and *change* in political events as we've previously discussed, but it is even harder to measure the gradual *deconstruction of reality* that seems to have taken place particularly in the USA where political leaders and their allied media reject established facts and procedures, demonize alternative messengers and predicate a version of reality that fits their own political agenda.[476]

In her analysis of the UK and US 2016 election discourse Schmidt concludes: "Using rhetorical strategies and 'uncivil' language in a 'post-truth' environment that rejects experts and the mainstream media, they have reshaped the political landscape by framing the debates in new ways while using new and old media to their advantage as they upend conventional politics."[477]

A good example of this deconstruction of reality is a demonization of the media by US president Trump, who has repeatedly called the mainstream media "enemies of the people" and been caught publicly lying over 10.000 times.[478] At the same time attacks against journalists have greatly increased worldwide but especially in the USA and journalist reporting has been elemental in bringing facts to the global public.[479]

> These misinformation strategies may seek to convince people to adopt particular opinions or take particular actions. However, they may also aim to systematically exhaust citizens' search for truth or their trust in political institutions by using a "firehose of falsehood" propaganda model (Paul & Matthews 2016), which can lead people to see "question the integrity of all media as equally unreliable" (Citizen Lab 2017).[480]

What makes the Russian Cyber-Information Influence Attacks and deconstruction of reality especially successful in the case of the US is the supplemental domestic dialogue that involves a multi-media IIA with the assistance of Fox television, the US National Enquirer and

[476] Mayer, 2019.
[477] Schmidt, 2017.
[478] Politifact, 2019. Kessler, Rizzo and Kelly, 2019.
[479] Thomas, 2018. Committee to Protect Journalists, 2019.
[480] Tenove, et al., 2017.

real and false Internet outlets that amplify the message.[481] The Mueller report and ample additional evidence shows that Russian 'history makers' proposed to help Trump get elected if the US would get sanctions lifted and leave Russia to carve out pieces of Ukraine.[482] Similar events seem to have taken place in the UK as Schmidt and Hay have analyzed, but apparently Russia did not manage to secure help from domestic political leaders, which some claim is the 'secret ingredient' needed for the Information Influence Attack illusion to properly take hold.[483]

However, there are sure signs that populism and similar propaganda tactics are on the rise in democracies in Europe and elsewhere, causing great concerns of law-makers, politicians and citizens being under-prepared for future elections:

> The rise of populism, in particular on the extreme right, constitutes a challenge to political stability and democracy not seen since the 1920s and 1930s (Judis 2016; Mudde and Kaltwasser 2012; Mu€ller 2016). The victories of Trump in the USA and Britain out of the EU have given populist leaders of extremist parties throughout Europe hope to emulate Britain in leaving the EU and Trump in gaining power, including Marine Le Pen in France, Geert Wilders in the Netherlands, and Beppe Grillo in Italy. [484]

Because Constructivism accounts for this beforementioned *deconstruction of reality* I argue that it shows much promise to contribute further to the theorization of Cyberspace. In my opinion more research is needed from Political Science, Cognition and Media studies on this de-construction and re-construction of reality through Cyberspace. This is an area Russia has been exploring for decades and based on its recent success Russia is actively hiring multi-lingual staff to work on future attacks on democratic elections and processes all over the world.[485]

The situation is alarming for democracies and action is needed to prevent looming attacks on upcoming elections.

[481] Mayer, 2019.
[482] R. Mueller, 2019.
[483] Ioffie, 2017. Schmidt, 2017. Hay, 2019.
[484] Schmidt, 2017.
[485] Maynes, 2019. The Daily Beast, 2018. Shuster and Ifraimova, 2018.

8.5 Construction of a Virtual Reality

Russian Cyber IIA attacks have been taken very seriously by most states and expertise shared amongst democratic nations. NATO and European Cyber-defense alliances are currently developing their arsenal against IIA and foreign interference into domestic discourse through Social Media.[486]

A key element in Constructive theory is that whether actors perceive their interests and circumstances correctly or not, *situations become real when people act on them*, and through those world-beliefs ideas and circumstances their actions *become real in their consequences*.[487]

This deconstruction of reality fits Bottichi & Challand's Constructive analysis of a political myth where: "political myth as the continual process of work on a common narrative by which the members of a social group can provide significance to their political conditions and experience."[488] Content-bubbles on social media can very easily feed into political myth's and re-enforce them to dangerous levels as mass-shootings by white-supremacists that claim to be responding to an ongoing attack that real-world evidence shows that *does not exist*.[489]

This relates to a uniquely Constructive theorizing on self-fulfilling prophecies; on events that become true if people believe they are true. The very same effect that Russia is counting on in its use of personalized propaganda: that whether people believe what's being said or not, what lingers is a *feeling that influences behavior*. Russia is playing a 'long game' striking democracies a blow when the Information Influence Attack becomes real in its consequences.[490]

Here Constructive theory explains "the role that perceptions and misperceptions can play in shaping the mindsets of key decision-makers."[491]

[486] Pamment, Nothhaft, et al., 2018. Wardle and Derakhshan, 2017.
[487] M. Blyth, 2010. Blyth, Routledge Handbook of International Political Economy IPE. IPE as a global conversation, 2009.
[488] Bottici and Challand, 2006.
[489] Ibid. Warzel, 2019.
[490] Bottici and Challand, 2006.
[491] Robert Jervis, 1976 in Cohen, 2009. Wendt, 1992. Suskind 2004.

The Russian propaganda playbook is confirmed by numerous whistleblowers who report that Russia's *spetspropaganda* machine uses Cyber-surveillance, social-engineering of virtual realities, content targeting and stolen information from campaigns on voters and candidates, while adding more staff and expanding its operations.[492]

The Russian spetspropaganda playbook includes philosophy and practical approaches based on studies of human cognition and psy-ops, such as smear-campaigns that repeat false accusations often enough for automatic instinctive subconscious disdain start to attach to the target.[493] Relying on cognitive bias and subliminal processes people are tricked into thinking that the feelings they feel for someone must be deserved based on their merits, and not the results of calculated psychological manipulation.[494]

How this alternative reality becomes possible is a subject for further inquiry on discourse and human cognition. Here I would like to point to the scholar James Carey who studied and theorized the *ritualistic power of communication*:

> A key argument within this report [...] is that we need to understand the ritualistic function of communication. Rather than simply thinking about communication as the transmission of information from one person to another, we must recognize that communication plays a fundamental role in representing shared beliefs. It is not just information, but drama — "a portrayal of the contending forces in the world."[495]

Communication studies show that while the content of language is information its purposes are manyfold and that people will seek information on the same issue from more then one source, but mostly if that information fits our pre-existing world-views.[496]

Data on Cyber-discourse and information-bubbles supports Carey's theorization on discourse. Similar to brain-cells that will wire together if they frequently fire together, Artificial Intelligence connects people to information that fits their world view, exposing people to more of the same, thus re-enforcing their world-view and eliminating others. These content bubbles affect the decisions people make in real life, and through those executions creating a self-fulfilling prophecy. [497]

---

[492] D. T. Gilbert 1991.
[493] Zabrisky, 2017.
[494] Surkov, 2019.
[495] Wardle and Derakhshan, 2017.
[496] Tavris and Aronson 2007. Pratkanis and Aronson 2001.
[497] Merton 1948.

Many users will not check or care if the information they read or shared was correct, rather ritualistically repeating and self-assuring themselves of a certain world view. This is backed up by psychological studies on humans that reveal a real brain-pain when people encounter cases that contrast their world-view, causing cognitive dissonance and a mentally painful moment for that individual. [498]

> These techniques, and the actors who use them, leverage people's cognitive limitations, psychological pre-dispositions and biases, political and cultural polarization, as well as deficits in media systems and democratic institutions. As a result, *solutions* to digital interference cannot simply be technical, nor can solutions be directed solely at foreign actors. [499]

Research by the renowned psychological scholars Tavris and Aronson on confirmation bias and cognitive dissonance indicates that people are not receptive to material that counters their world-views, and that normative ideas and world-views can make people blind to opposing view-points. [500]

Human's don't compute information the same way a computer does, to assume constant rationality is to deny our existence as a mammal on the tree of evolution.

> a ritual view of communication does not consider the act of reading a newspaper to be driven by the need for new information. Rather, it likens it to attending a church service. It's a performance in which nothing is learned, but a particular view of the world is portrayed and confirmed. In this way, news reading and writing is a ritualistic and dramatic act.[501]

Those human weaknesses were acknowledged during the writing of this academic work and I made a conscious effort to investigate alternative points of view and review raw data in order to deliver an accurate analysis of reality according to the evidence. Keeping in mind that it is extremely hard to prove a negative, there is no evidence that a) those Cyber-attacks were fabricated and b) that they originated somewhere else than in Russia. Hacks and Information Influence Attacks took place in cyberspace and they originated in Russia[502]

Russia used lies, stolen and distorted material to manipulate social Cyber-discourse through mixed-media Information Influence Attacks. In Cyberspace, particularly through on Social Media, Russia used system weaknesses and cognitive fallacies to create false realities through a torrent of false political and politicized messages. Russia's method was to

[498] Suskind 2004. Wardle and Derakhshan, 2017.
[499] Tenove, et al., 2017.
[500] Tavris and Aronson 2007.
[501] Wardle and Derakhshan, 2017.
[502] The Intelligence Community FBI, CIA & NSA., 2017.

influence people's actions and state politics before elections and cause political upheaval and social rifts within key democratic countries.[503]

When the amplified message increases violence and attacks on specific groups it reveals a massive problem for modern societies and public discourse. Historical examples teach us that societies can easily spiral into violence if certain sentiments are allowed to foster. The catastrophe of the second World War teaches us the power of propaganda and how easily it turns to violence.[504]

Utilizing *weaknesses in social media*, the *open nature of Cyber-communications* and *blind spots in international law*, Russian state actors managed strike a unique blow to Western democratic institutions, parties and candidates on a scale that's never been seen before. Some even argue that Russia's 2016-2018 operations, which I might add are still ongoing, as part of the first new cyber-war that the world has ever seen.[505]

[503] R. Mueller, 2019.
[504] Lucas and Pomeranzev, 2016. Pratkanis and Aronson 2001.
[505] de Jong, et al., 2018.

9 Conclusions

> is this a moment of great transformation, in which a new paradigm will emerge out of the ashes of the liberal order, with neo-liberal economics and social liberalism succumbing to the closing of borders to immigrants, rising protectionism, and social conservatism? [506]

This thesis addresses a new type of Cyber-Information-Influence Attacks that pose serious problems for democracies. Here, I have researched the international Cyber-environment and how it enables actors to use Cyberattacks to affect Democratic institutions, particularly elections and media.

The thesis connects Constructivist theorization and Ideational studies with contributions of Democratic scholars using a framework to identify democratic social actions that are (likely to be) targeted by enemies through Cyberspace.

After introducing the subject, methodology, operating hypothesis and theory, we defined Cyber-concepts and the environment for International Cyber Relations, including an overview of the global legal and institutional setup, outlining the Multistakeholder model the influence of Social Media.

Before discussing Cyberattacks, I outlined democratic theory and the role of discourse, identified main political social actions and the pillars of democracy – the elements needed for a functioning democratic society; *empowered inclusion*, *collective agenda and will formation*, and *collective decision making*.

Next, we examined the emergence of Cyberspace as a new space of operations, defined main Cyber-aggressors and examined evidence of attacks, establishing '*a case*' for theoretical examination where we reviewed *how* Russian Cyberattacks undermined *empowered inclusion*, *will formation* and crippled governments and *decision-making* bodies in the process. Examples of the effects the Russian attacks have had are unprecedented including a 6 week US government shut-down, the UK parliament and executive branch preoccupied in normative and technical Brexit debate, a French national-debate, and politicians in several other democracies preoccupied dealing with the aftermath of Russian Information Influence Attacks on their elections. As previously examined, the attacks were customized to local sentiments, used various methods as *established through application of*

[506] Schmidt, 2017.

Warren's framework, and had different effects in different places, with the general trend emerging that populists are gaining power within democracies.

An examination of Cyberattacks was followed by discussion of IR theory, an underpinning for selecting Constructivism for the appropriate theoretical contributions to further understanding of Cyberspace. We analyzed Russian propaganda, according to a Discursive Institutionalist framework, for an *ideational analysis of discourse*, in order to identify and analyze trends in Russian Information Influence Attacks.

In the next chapter we examined *what* effects through outcome of the ideational analysis for theoretical insights into the underlying message behind the Russian attacks, leading into this summary of the main elements at play, broad findings and conclusions. The content was found to be *polarizing* and *emotionally charged*, designed to incite violence against certain people or groups and invoke strong feelings, all of whom constitute an attack on democratic discourse and democratic processes.

In my opinion the attacks are undeniably damaging to democracy, but of *special concern are attacks on journalists and media outlets that foster free and fact-checked reporting*. Those attacks further escalate confusion and aggravating violent sentiments. When desperate people start believing in a distorted view of society there is real reason to be concerned as countless recent violent attacks have demonstrated.

Russia's Cyberthreats are in many ways old propaganda in new bottles. With that said I maintain that the medium itself is exasperating the danger in numerous ways, particularly through construction of a *personalized virtual reality*.

This includes an acknowledgement of the human element as an underestimated element and of Cyberspace as more than a tool, an actual virtual reality where people need protection by governments. This calls for inclusion of theories like Constructivism that provide insights into the construction of discourse and virtual experiences.

The social media and institutional framework of Cyberspace is lagging far behind its technical capabilities, prolonging a Wild-West situation of lawlessness in Cyberspace. The future development of Cyberspace depends on the capabilities of all the stakeholders in the Multistakeholder-model to shoulder their responsibility.

Leaving that discussion for another day I fear that Social Media is not taking the problem or its role as mediator of public discourse seriously enough. SM has done a great job capitalizing off' public discourse but does not seem to understand the implications and responsibilities of a public space.

I agree with critics that claim a coordinated government-lead effort is needed.

> "Post-truth in politics is one of the drivers of populism and it is one of the threats to our democracies, [w]e have reached a fork in the road: we have to choose whether to leave the internet like it is, the wild west, or whether it needs rules that appreciate the way communication has changed. I think we need to set those rules and this is the role of the public sector."[507]

Currently NATO, EU, IGF and democratic institutions are preparing themselves for these changes in Cyberspace and working on educating democratic governments on Cybersecurity and *preparing for a new kind of war*. Several key policy reports have been published and accepted into strategy by the European Union and member states (see bibliography). NATO has put together the NATO-accredited Cyber defense hub that supports its member nations and NATO with Cyber defense expertise in addition to other operational changes. The setup of new democratic Cybersecurity institutions and the addition of information as the seventh joint function reflects an acknowledgement of a new virtual war. These changes are part of the toolkit used in what is now called hybrid, asymmetrical, or unconventional warfare.

I believe that NATO's change to include Cyberspace as the fourth space marks more than just the seamless integration of 'the digital domain' into military operations. *It represents an understanding of the Cyberthreat*. NATO has published guidelines for states to help them set up and implement cyber-strategies but reports on progress are harder to locate. While progress on domestic implementation is unclear a key element for success is missing in many places: public discussion. The human element is repeatedly under-estimated in Cybersecurity and Cyber-users need to know the dangers and how to 'Cyber'-safely. Education and a national dialogue are needed on how we can fight 'post-truths' and what counter-measures to take.

During the months that this dissertation was written there was a marked change in public discourse with the revelations of the US Mueller report and a growing consensus of

[507] Politi, 2016.

what took place. There is also a growing discussion on what actions must be taken to prevent repeated attacks come next election time. Over the past month Social Media has shifted its position, banned esteem discourse and is clearly in internal discord over what actions to take and how much transparency to include.

I believe we are moving into a time period marked by increased contention and development of a new asymmetrical Cyber-Cold-War of Mutually Assured (Cyber) Destruction where states test each other's capabilities, patience and resourcefulness. This will probably also include a repetition of MAD Cold-War-like situations, increases in financial crime and state-backed attacks on financial systems with more actors than Russia making their mark. In addition to that Russia will continue its IIA in more countries and at more occasions.

'Swift and systemic action' must be taken by democracies, stakeholders of the Multistakeholder model to protect themselves against Cyberthreats on all four levels of Cyberspace, and to implement laws and regulations that cover cyber-crime and external influence in internal affairs. Recommendations have already been published (see addendum) and should be updated as needed, as implementation *should* be ongoing. There is however considerably less news on that progress from law-makers and stakeholders with the verdict on social media performance still out.

I predict that Russia's 2016 Brexit and Trump campaigns will take their place in history as the first major 'Cyber-war' that the world has experienced. The attacks were better coordinated and different than anyone expected, but very effective, nonetheless. The objective of causing confusion, financially harming and destabilizing your enemy has worked perfectly and Western states seem more or less uncapable of preventing a repeat attack. This match goes to Russia, but the question looms whether democracy is ready for the next round.

Reykjavik, May 2019

Thorlaug Borg Agustsdottir

10 Tables, Figures and Images

Table 1 – Warrens' Outline of Essential Democratic Functions, p. 61 [508]

Table 2 - Examples of Weaknesses of Democratic Cyber Activities, p. 62. [509]

Table 3 - The Kremlin Tool Kit, p. 81 [510]

Table 4 - Table 4 - Adjusted Constructive Framework for Ideational Analysis, p. 112. [511]

Table 5 - Applied Constructive Framework for Ideational Analysis, p. 113. [512]

Figure 1: The Multistakeholder Model of Internet Governance, p.36. [513]

Figure 2: Active Social Media Users 2018, p37. [514]

Figure 3: Cyber Users by Country 2018, p.38. [515]

[508] Warren, 2017.
[509] ibid
[510] Pomeranzev and Weiss, 2013.
[511] Complemented version of Schmidt's 2008 model for discursive institutionalismand ideational analysis. Schmidt, 2008., Hay, International relations theory and globalization, 2013.
[512] Complemented version of Schmidt's 2008 model for discursive institutionalismand ideational analysis. Schmidt, 2008., Hay, International relations theory and globalization, 2013.
[513] Internet Society (ISOC), 2016.
[514] Brandwatch, 2019.
[515] ibid

11 Addendum

Suggestions for action from Wardle and Derakhshan[516]

What could technology companies do?

1. Create an international advisory council.
2. Provide researchers with the data related to initiatives aimed at improving public discourse.
3. Provide transparent criteria for any algorithmic changes that down-rank content.
4. Work collaboratively.
5. Highlight contextual details and build visual indicators.
6. Eliminate financial incentives.
7. Crack down on computational amplification.
8. Adequately moderate non-English content.
9. Pay attention to audio/visual forms of mis- and dis-information.
10. Provide metadata to trusted partners.
11. Build fact-checking and verification tools.
12. Build 'authenticity engines'.
13. Work on solutions specifically aimed at minimizing the impact of filter bubbles:
    a. Let users customize feed and search algorithms.
    b. Diversify exposure to different people and views.
    c. Allow users to consume information privately.
    d. Change the terminology used by the social networks.

What could national governments do?

1. Commission research to map information disorder.
2. Regulate ad networks.
3. Require transparency around Facebook ads.
4. Support public service media organizations and local news outlets.
5. Roll out advanced cybersecurity training.
6. Enforce minimum levels of public service news on to the platforms.

What could media organisations do?

1. Collaborate
2. Agree policies on strategic silence.
3. Ensure strong ethical standards across all media.
4. Debunk sources as well as content.
5. Produce more news literacy segments and features.
6. Tell stories about the scale and threat posed by information disorder.
7. Focus on improving the quality of headlines.
8. Don't disseminate fabricated content.

[516] Wardle and Derakhshan, 2017.

What could civil society do?

1. Educate the public about the threat of information disorder.
2. Act as honest brokers.

What could education ministries do?

1. Work internationally to create a standardized news literacy curriculum.
2. Work with libraries.
3. Update journalism school curricula.

What could funding bodies do?

1. Provide support for testing solutions.
2. Support technological solutions.
3. Support programs teaching people critical research and information skills.

12 Bibliography

Abdelal, Rawi. 2009. "Constructivism as an approach to international political economy." In *IPE as a global conversation*, by Mark Blythe ed., 62-77. New York: Ruthlidge.

Agence France-Presse Moscow. 2019. *Russia passes bill to allow internet to be cut off from foreign servers - The Guardian.* April 11. Accessed April 23, 2019. https://www.theguardian.com/world/2019/apr/11/russia-passes-bill-internet-cut-off-foreign-servers.

Al Jazeera News. 2019. *Russia passes legislation banning state criticism, fake news Critics see the legislation as part of Kremlin efforts to stifle criticism and tighten control.* March 9. Accessed April 22, 2019. https://www.aljazeera.com/news/2019/03/russia-passes-legislation-banning-state-criticism-fake-news-190307194308089.html.

Applebaum, Anne. 2019. "The Washington Post." *Opinions The more we learn about Brexit, the more crooked it looks.* March 8. Accessed March 12, 2019. https://www.washingtonpost.com/opinions/global-opinions/the-more-we-learn-about-brexit-the-more-crooked-it-looks/2019/03/08/b011517c-411c-11e9-922c-64d6b7840b82_story.html.

Aro, Jessikka. 2015. "My Year as a Pro-Russia Troll Magnet: International Shaming Campaign and an SMS from Dead Father." *Kioski.* Nov 9. Accessed March 11, 2019. http://kioski.yle.fi/omat/my-year-as-a-pro-russia-troll-magnet.

Ashford, Warwick. 2014. *Snowden revelations have changed attitudes to cloud, study claims.* March 31. Accessed April 23, 2019. https://www.computerweekly.com/news/2240217235/Snowden-revelations-have-changed-attitudes-to-cloud-study-claims.

Balsamo, Michael, and Tucker Eric. 2018. *North Korean programmer charged in Sony hack, WannaCry attack.* September 6. Accessed April 22, 2019. https://www.pbs.org/newshour/nation/north-korean-programmer-charged-in-sony-hack-wannacry-attack.

Baraniuk, Chris. 2016. *Why the forgotten Russian Intenet was doomed from the start - BBC.* October 26. Accessed April 23, 2019. http://www.bbc.com/future/story/20161026-why-the-forgotten-soviet-internet-was-doomed-from-the-start.

BBC. 2018. *Facebook stops sending staff to help political campaigns.* September 19. Accessed April 28, 2019. https://www.bbc.com/news/technology-45599962.

BBC News. 2019. *Russia internet freedom: Thousands protest against cyber-security bill - BBC News.* March 10. Accessed April 22, 2019. https://www.bbc.com/news/world-europe-47517263.

Béland, D., and R. Cox. 2010. *Ideas and Politics in Social Science Research.* Oxford: Oxford University Press.

Béland, Daniel, and Mitchell Orenstein. 2013. "International organizations as policy actors: An ideational approach." *Global Social Policy* 125-143.

Bisen, Arjun. 2019. *Disinformation Is Drowning Democracy In the new age of lies, law, not tech, is the answer - Foreign Policy.* April 24. Accessed April 29, 2019. https://foreignpolicy.com/2019/04/24/disinformation-is-drowning-democracy/.

Blaikie, Norman. 2000. *Designing Social Research, The Logic of Anticipation.* Cambridge: Blackwell Publishers ltd.

Blyth, Mark. 2002. "Great Transformations: Economic Ideas and Institutional Change in the Twentieth Century." *Cambridge University Press* 17-45.

Blyth, Mark. 2010. "Ideas, Uncertainty and Evolution." In *Ideas and Politics in Social Science Research*, by Beland and Cox, 83-101. Oxford : Oxford University Press.

—. 2009. *Routledge Handbook of International Political Economy (IPE) IPE as a global conversation.* New York: Ruthlidge.

Bottici, Chiara, and Benoît Challand. 2006. "Rethinking Political Myth The Clash of Civilizations as a Self-Fulfilling Prophecy." *European Journal of Social Theory* 315-336.

Bradshaw, Samantha, Laura DeNardis, and Fen Osler Hamps. 2015. *The Emergence of Contention in Global Internet Governance.* Global Commision on Internet Governance, Centre for International Governance Innovation and Chatham House.

Brandwatch. 2019. *123 Amazing Social Media Statistics and Facts - Brandwatch.* March 1. Accessed April 15, 2019. https://www.brandwatch.com/blog/amazing-social-media-statistics-and-facts/.

Broniatowski, Michal. 2018. *Tusk makes scathing attack on Russian influence Council president says Russia will do 'whatever it can' to undermine European unity.* June 10. Accessed April 22, 2019. https://www.politico.eu/article/donald-tusk-poland-russia-latvia-makes-scathing-attack-on-russian-influence/.

Buckland, Benjamin S., Fred Schreier, and Theodor H. Winkler. 2015:1. *Democratic Governance Challenges of Cyber Security.* Geneva: The Geneva Centre for the Democratic Control of Armed Forces.

Bump, Philip. 2018. *All the ways Trump's campaign was aided by Facebook, ranked by importance - The Washington Post.* March 18. Accessed April 28, 2019. https://www.washingtonpost.com/news/politics/wp/2018/03/22/all-the-ways-trumps-campaign-was-aided-by-facebook-ranked-by-importance/?utm_term=.dc0628b12a3a.

Cadwalladr, Carole. 2018. *Parliament seizes cache of Facebook internal papers - The Observer.* November 21. Accessed April 24, 2019. https://www.theguardian.com/technology/2018/nov/24/mps-seize-cache-facebook-internal-papers.

Canongia, C., and R. Mandarino. 2013. "Cybersecurity: The new challenge of the information society." In *Crisis Management: Concepts, Methodologies, Tools and Applications*, 60-80. Hershey, PA: IGI Global.

Carroll, Oliver. 2019. *Russia is playing with the West's minds says Putin advisor -The Independent.* February 12. Accessed March 15, 2019. https://www.independent.co.uk/news/world/europe/putin-russia-kremlin-vladislav-surkov-grey-cardinal-moscow-a8773661.html.

Carstensen, M.B., and V. Schmidt. 2015. "Power through, over and in ideas: conceptualizing ideational power in discursive institutionalism." *Journal of European Public Policy* 318-337.

Casey, Henrik. 2016. *Internet of Scary Things: IoT Hacking Tool Goes Public - Tom's Guide.* October 6. Accessed April 25, 2019. https://www.tomsguide.com/us/iot-hack-tool-public,news-23579.html.

Cavelty, Myriam Dunn , and Manuel Suter. 2009. "Public–Private Partnerships are no silver bullet: An expanded governance model for Critical Infrastructure Protection." *International Journal of Critical Infrastructure Protection, Vol. 4, No. 2,* 179-187.

Cavelty, Myriam Dunn. 2018. "Cybersecurity Research Meets Science and Technology Studies." *Politics and Governance* 22-30.

Chen, Adrian. 2015. *The Agency - New York Times Magazine.* June 2. Accessed April 22, 2019. https://www.nytimes.com/2015/06/07/magazine/the-agency.html.

—. 2018. *What Mueller's Indictment Reveals About Russia's Internet Research Agency - The New Yorker.* February 16. Accessed April 22, 2019. https://www.newyorker.com/news/news-desk/what-muellers-indictment-reveals-about-russias-internet-research-agency.

Churchill, Winston. 1947. *International Churchill Society, The Worst Form of Governance.* November 11. Accessed April 2, 2019. https://winstonchurchill.org/resources/quotes/the-worst-form-of-government/.

Citron, Danielle. 2014. *Hate Crimes in Cyberspace.* Cambridge, MA: Harvard University Press.

Clinton, Hillary. 2019. *Hillary Clinton: Mueller Report Shows That The Russians Were Successful | Rachel Maddow | MSNBC.* May 1. Accessed May 2, 2019. https://www.youtube.com/watch?v=JqfQ_kDOrIY.

Coats, Daniel. 2019. *Worldwide Threat Assessment of the US Intelligence Community.* Statement for the Record, Senate Select Committee on Intelligence, Washington DC: Office of the Director of National Intelligence.

Cohen, Benjamin J. 2009. "The multiple traditions of American IPE." By ed. Mark Blythe, 23-39. New York: Ruthlidge.

Collier, Jamie. 2018. "Cyber Security Assemblages: A Framework for Understanding the Dynamic and Contested Nature of Security Provision ." *Politics and Governance* 13-21.

Committee on Foreign Relations, US State Senate. 2018. "Putin's Assymmetric Assault on Democracy in Russia and Europe: Implications for U.S. National Security." *US Senate, Comittee on Foreign Relations.* January 10. https://www.foreign.senate.gov/imo/media/doc/FinalRR.pdf.

Committee to Protect Journalists. 2019. *47 Journalists Killed in Russia between 1999 and 2019 / Motive Confirmed or Unconfirmed.* April 10. Accessed April 10, 2019. https://cpj.org/data/killed/europe/russia/?status=Killed&motiveConfirmed%5B%5D=Confirmed&motiveUnconfirmed%5B%5D=Unconfirmed&type%5B%5D=Journalist&cc_fips%5B%5D=RS&start_year=1999&end_year=2019&group_by=location.

Confessore, Nicholas, Gabriel Dance, Richard Harris, and Mark Hansen. 2018. *The Follower Factory Everyone wants to be popular online. Some even pay for it. Inside social media's black market - The New York Times.* January 21. Accessed May 2, 2019. https://www.nytimes.com/interactive/2018/01/27/technology/social-media-bots.html.

Constine, Josh. 2018. *Facebook and Instagram launch US political ad labeling and archive - Techcrunch.* June. Accessed April 24, 2019. https://techcrunch.com/2018/05/24/facebook-political-ad-archive/.

Council of Europe. 2004/2019. *Budapest Convention and related standards.* https://www.coe.int/en/web/cybercrime/the-budapest-convention.

Craig Timberg, Elizabeth Dworskin. 2018. *Twitter is sweeping out fake accounts like never before, putting user growth at risk - The Washington Post.* July 6. Accessed April 22, 2019. https://www.washingtonpost.com/technology/2018/07/06/twitter-is-sweeping-out-fake-accounts-like-never-before-putting-user-growth-risk/.

Craigen, Dan, Nadia Diakun-Thibault, and Randy Purse. 2014, Oct. "Defining Cybersecurity." *Technology Innovation Management Review.*

Crootof, Rebecca. March 1, 2016. *International Cybertorts: Expanding State Accountability in Cyberspace.* Ithaca: Cornell Law Review.

Crosby, Alan. 2019. *Q&A: Hurdles Ahead As Russia Surges On With 'Sovereign Internet' Plan - Radio Free Europe.* February 19. Accessed April 22, 2019. https://www.rferl.org/a/q-a-hurdles-ahead-as-russia-surges-on-with-sovereign-internet-plan/29766229.html.

Dahlgren, Peter. 2005. "The Internet, Public Spheres, and Political Communication: Dispersion and Deliberation." *Political Communication* 147-162.

de Jong, Sijbren, Tim Sweijs, Katarina Kertysova, and Roel Bos. 2018. *Inside the Kremlin House of Mirrors: How Liberal Democracies can Counter Russian Disinformation and Societal Interference.* Hague: The Hague Centre for Strategic Studies. https://hcss.nl/sites/default/files/files/reports/Inside%20the%20Kremlin%20House%20of%20Mirrors.pdf.

Deibert, Ron. 2015. "The Geopolitics of Cyberspace After Snowden." *Current History* 9-15.

Deibert, Ronald J, and Rafal Rohozinski. 2010. "Risking Security: Policies and Paradoxes of Cyberspace Security." *International Digital Sociology* 15-32.

DHS & FBI. 2016-2018. *US-CERT / CISA (Cyber-Infrastructure).* Accessed February 6, 2019. https://www.us-cert.gov/GRIZZLY-STEPPE-Russian-Malicious-Cyber-Activity.

Digital Forensic Research Lab. 2018. *Logical Fallacies Fuel Kremlin Disinfo How the Kremlin and its disinformation networks use logical fallacies to dismiss, dismay, distract, and distort.* April 22. Accessed April 22, 2019. https://medium.com/dfrlab/logical-fallacies-fuel-kremlin-disinfo-e4185bb455e6.

Digital Forensics Research Lab. 2018. *#TrollTracker: Bots, Botnets, and Trolls Everything you ever wanted to know about bots, botnets, and trolls, but were too afraid to ask.* October 8. Accessed April 22, 2019. https://medium.com/dfrlab/trolltracker-bots-botnets-and-trolls-31d2bdbf4c13.

DiResta, Renee. 2018. *The Digital Maginot Line.* November 28. Accessed May 5, 2019. https://www.ribbonfarm.com/2018/11/28/the-digital-maginot-line/.

Dorell, Oren. 2017. *Alleged Russian political meddling documented in 27 countries since 2004-USA Today.* September 27. https://eu.usatoday.com/story/news/world/2017/09/07/alleged-russian-political-meddling-documented-27-countries-since-2004/619056001/.

Douglas, Nick. 2017. *Facebook Isn't Recording Your Conversations, But It May as Well Be - LifeHacker.* August 11. Accessed April 27, 2019. https://lifehacker.com/facebook-isn-t-recording-your-conversations-but-it-may-1820193946.

Dryzek, John S. 2017. "The Forum, the System, and the Polity: Three Varieties of Democratic Theory." *Political Theory* 610–636.

Dunne, Tim. 2013. "The English School." In *International Relations Theories*, by Tim Dunne, Milja Kurki and Steve Smith, 132-152. Oxford: Oxford University Press.

Elder, Miriam. 2013. *Russian guard service reverts to typewriters after NSA leaks This article is more than 5 years old Leaks by US whistleblower Edward Snowden have fuelled Russian suspicions over electronic communications.* July 11. Accessed April 22, 2019. https://www.theguardian.com/world/2013/jul/11/russia-reverts-paper-nsa-leaks.

Eligon, John. 2018. *Hate Crimes Increase for the Third Consecutive Year, F.B.I. Reports - New York Times .* November 18. Accessed April 22, 2019. https://www.nytimes.com/2018/11/13/us/hate-crimes-fbi-2017.html.

Emerson, Josh. 2017. *Work space for @UsHadrons @toolmarks and @josh_emerson.* October . Accessed April 22, 2019. https://medium.com/@ushadrons.

Facebook. 2019. *Facebook Group Community Standards.* March 29. Accessed April 28, 2019. https://www.facebook.com/communitystandards/dangerous_individuals_organizations.

—. 2019. *Remove, Reduce, Inform: New Steps to Manage Problematic Content.* April 10. Accessed April 14, 2019. https://newsroom.fb.com/news/2019/04/remove-reduce-inform-new-steps/.

—. 2018. *Standing Against Hate.* May 17. Accessed April 23, 2019. https://newsroom.fb.com/news/2019/03/standing-against-hate/.

Federal Bureau of Investigation. 2017. "Federal Bureo of Investigation, Senate Report." *Assessing Russian Activities and Intentions in Recent Elections.* June 17. Accessed March 11, 2019. https://www.fbi.gov/news/testimony/assessing-russian-activities-and-intentions-in-recent-elections.

Field, Matthew. 2018. *WannaCry cyber attack cost the NHS £92m as 19,000 appointments cancelled.* October 11. Accessed April 22, 2019. https://www.telegraph.co.uk/technology/2018/10/11/wannacry-cyber-attack-cost-nhs-92m-19000-appointments-cancelled/.

Flynn, Jeffrey. 2004, 3 (4). "Communicative Power in Habermas's Theory of Democracy." *European Journal of Political Theory* 433–454.

Foster, David. 2014. "On the open internet and the free web." *CERN, The European Organization for Nuclear Research.* March 12. Accessed February 22, 2019. https://home.cern/news/opinion/computing/open-internet-and-free-web.

Fowler, Geoffrey A., and Chiqui Esteban. 2019. *14 years of Mark Zuckerberg saying sorry, not sorry - The Washington Post.* April 9. Accessed April 28, 2019. https://www.washingtonpost.com/graphics/2018/business/facebook-zuckerberg-apologies/.

Francheschi-Bicchierai, Lorenzo. 2014. *The 10 Biggest Revelations From Edward Snowden's Leaks - Mashable.* June 5. Accessed April 4, 2019. The 10 Biggest Revelations From Edward Snowden's Leaks.

Frenkel, Sheera, Nicholas Confessore, Cecilia Kang, Matthew Rosenberg, and Jack Nicas. 2018. *Delay, Deny and Deflect: How Facebook's Leaders Fought Through Crisis - The New York Times.* November 18. Accessed April 27, 2019. https://www.nytimes.com/2018/11/14/technology/facebook-data-russia-election-racism.html.

Gerovitch, Slava. 2002. *From newspeak to cyberspeak : a history of Soviet cybernetics.* Cambridge, MA: Massachusetts Institute of Technology.

Gershkovich, Evan. 2019. *The Moscow Times > 'Point of No Return': Russia's Libertarians Lead Protest Against 'Sovereign Internet'.* March 10. Accessed March 30, 2019. https://www.themoscowtimes.com/2019/03/10/point-of-no-return-russias-libertarians-lead-protest-against-sovereign-internet-a64758.

Gertz, Matt, and Rob Savillo. 2019. *Study: Major media outlets' Twitter accounts amplify false Trump claims on average 19 times a day - MediaMatters for America.* May 3. Accessed May 4, 2019. https://www.mediamatters.org/blog/2019/05/03/study-major-media-outlets-twitter-accounts-amplify-false-trump-claims-average-19-times-day/223572.

Gilbert, Daniel T. 1991. "http://dx.doi.org/10.1037/0003-066X.46.2.107." *American Psychologist, Vol 46* 107-119.

Gilbert, David, and Vice News. 2019. *Cyberattacks: Why Russia is about to disconnect itself from the internet.* February 11. Accessed April 22, 2019. https://news.vice.com/en_us/article/59xdmq/why-russia-is-about-to-disconnect-itself-from-the-internet.

Giles, Keir. 2015. *Putin's troll factories: How Moscow controls access to western media.* London: Chatnam House, The Royal Institute of International Affairs.

Global Commission on Internet Governance. 2019. *Global Commission on Internet Governance.* https://www.cigionline.org/initiatives/global-commission-internet-governance.

Gomez, Miguel Alberto, and Eula Bianca Villar. 2018. "Fear, Uncertainty, and Dread: Cognitive Heuristics and Cyber Threats." *Politics and Governance* 61-72.

Greenberg, Andy. 2017. *Russian Hackers are using 'Tainted' Leaks to sow Disinformationi - Wired.* May 25. Accessed April 22, 2019. https://www.wired.com/2017/05/russian-hackers-using-tainted-leaks-sow-disinformation/.

—. 2017. *The NSA Confirms it: Russia hacked French Election 'Infrastructure' - The Wired.* September 5. Accessed April 29, 2019. https://www.wired.com/2017/05/nsa-director-confirms-russia-hacked-french-election-infrastructure/.

Grimes, David Robert. 2017. *Russian fake news is not new: Soviet Aids propaganda cost countless lives - The Guardian.* June 17. Accessed April 29, 2019. https://www.theguardian.com/science/blog/2017/jun/14/russian-fake-news-is-not-new-soviet-aids-propaganda-cost-countless-lives.

Grynkewich, Alexus G. 2018. "Paradigm Change Operational Art and the Information Joint Function." *Joint Force Quarterly*, April 11.

Habermas, Jurgen. 1996. *Between Facts and Norms: Contributions to a Discourse Theory of Law and Democracy.* Cambridge, MA: MIT Press.

Hadlington, Lee. 2017. "Human factors incybersecurity; examining thelink between[3_TD$DIFF]Internetaddiction, impulsivity,attitudes towardscybersecurity, and riskycybersecurity behaviours." *Heliyon, Elsevier* issue 3.

Hardy, Catherine. 2016. *Euronews.* June 06. Accessed February 6, 2019. https://www.euronews.com/2016/06/15/cyberspace-is-officially-a-war-zone-nato .

Harford, Tim. 2019. *Political change can feel elusive, until the dam bursts.* March 28. https://www.ft.com/content/7211ce52-5147-11e9-9c76-bf4a0ce37d49.

Hay, Colin. 2019. "Brexistential Angst and the Paradoxes of Populism: On the Contingency, Predictability and Intelligibility of Seismic Shifts." *Political Studies* 1-20.

Hay, Colin. 2013. "International relations theory and globalization." In *International Relations Theories, Discipline and Diversity*, by Tim Dunne, Milja Kurki and Steve Smith, 287-305. Oxford: Oxford university press.

Heyer, ulia Amalia. 2019. *France's Golden Boy Learns How to Fight Macron Debates His Way Out of The Yellow-Vest Crisis - Der Spiegel.* March 29. Accessed April 22, 2019.

https://www.spiegel.de/international/europe/macron-debates-his-way-out-of-the-yellow-vest-crisis-a-1259762.html.

Higgins, Andrew. 2016. "Effort to Expose Russia's 'Troll Army' Draws Vicious Retaliation." *New York Times.* May 30. Accessed March 11, 2019. https://www.nytimes.com/2016/05/31/world/europe/russia-finland-nato-trolls.html.

Hodge, Karl. 2018. *If it's free online, you are the product.* April 19. Accessed April 24, 2019. https://theconversation.com/if-its-free-online-you-are-the-product-95182.

Hu, Jayne. 2018. *Social networks make the world's largest nations seem small - Quartz.* September 18. Accessed April 25, 2019. https://qz.com/1386649/social-networks-make-the-worlds-largest-nations-seem-small/.

Hudson, Laura. 2013. *Facebook Apologizes for Tolerating Violent Imagery Toward Women - Wired.com.* January 7. Accessed April 11, 2019. https://www.wired.com/2013/01/facebook-violence-women-2/.

Internet Live Stats. 2016. *Internet Users by Country (2016).* December. http://www.internetlivestats.com/internet-users-by-country/.

Internet Society (ISOC). 2016. "Internet Society (ISOC)." *Internet Governance - Why the Multistakeholder Approach Works.* August 16. Accessed March 9, 2019. https://www.slideshare.net/InternetSociety/internet-governance-why-the-multistakeholder-approach-works.

Internet Society. 2001. *Internet Governance – Why the Multistakeholder Approach Works.* Accessed February 21, 2019. https://www.internetsociety.org/resources/doc/2016/internet-governance-why-the-multistakeholder-approach-works/.

Ioffie, Julia. 2017. "It Took Two to Make Russian Meddling Effective." *The Atlantic.* June 23. Accessed March 31, 2019. https://www.theatlantic.com/international/archive/2017/06/obama-response-russia-election-interference/531486/.

Isasc, Mike, and Daisuke Wakabayashi. 2017. *Russian Influence Reached 126 Million Through Facebook Alone - New York Times.* October 30. Accessed April 4, 2019. https://www.nytimes.com/2017/10/30/technology/facebook-google-russia.html.

Ivanova, Irina. 2018. *Facebook let some companies exploit users' friends data, U.K. email dump alleges - CBS News.* December 8. Accessed April 8, 2019. https://www.cbsnews.com/news/facebook-gave-some-companies-preferential-user-data-according-to-uk-parliament/.

Jacobson, Louis. 2018. *Donald Trump says there's 'substantial evidence of voter fraud.' There isn't - Politifact.* January 4. Accessed April 22, 2019. https://www.politifact.com/truth-o-meter/statements/2018/jan/04/donald-trump/donald-trump-says-theres-substantial-evidence-vote/.

Jensen, Benjamin, Brandon Valeriano, and Ryan Maness. 2019. "Fancy bears and digital trolls: Cyber strategy with a Russian twist." *Journal of Strategic Studies.*

Jones, Dean Sterling. 2018. *The Russian Troll Factory is Recruiting English-Speaking Journalists to Fight "Political Censorship" After Facebook Ban - .* April 19. Accessed April 3, 2019. https://shootingthemessenger.blog/2018/04/19/the-russian-troll-factory-is-recruiting-english-speaking-journalists-to-fight-political-censorship-after-facebook-ban/.

Kayali, Laura. 2019. *Inside Facebook's fight against European regulation Dozens of Commission documents show how the tech giant pushed back against rules on issues ranging from copyright to privacy.* January 23. Accessed April 23, 2019. https://www.politico.eu/article/inside-story-facebook-fight-against-european-regulation/.

Kessler, Glenn, Salvador Rizzo, and Meg Kelly. 2019. *Fact Checker: President Trump has made 9,451 false or misleading claims over 801 days. - Washington Post.* April 1. Accessed May 2, 2019. https://www.washingtonpost.com/politics/2019/04/29/president-trump-has-made-more-than-false-or-misleading-claims/.

Ketchum, Richard. 1980. "Plato on Real Being." *American Philosophical Quarterly* 213-220.

Kirshner, Jonathan. 2009. "Realist political economy Traditional themes and contemporary challenges." In *Routledge Handbook of International Political Economy (IPE), IPE As a Global Conversation*, by Mark Blyth ed., 36-48. New York: Routledge.

Klimburg, Alexander, and Philipp Mirtl. 2012. *Cyberspace and Governance—A Primer.* Vienna: Austrian Istitute for International Affairs.

Kotlyar, Evgenia. 2017. *"We had a goal ... to cause unrest": an interview with an ex-employee of the Troll Factory in St. Petersburg.* October 21. Accessed April 22, 2019. https://tvrain.ru/teleshow/bremja_novostej/fabrika-447628/.

Kozlowska, Hanna. 2018. *The "female blackout" is what happens when Facebook activism doesn't work - Quartz.* October 1. Accessed April 22, 2019. https://qz.com/1408978/the-female-blackout-is-what-happens-when-facebook-activism-doesnt-work/.

Kramer, F., Stuart Starr, and Larry Wentz. 2009. "Cyber Influence and International Security." In *Cybersecurity and National Security*, by Kramer, Starr and Wentz, 343-361. Potomac.

Kramer, Franklin D. ed. 2009. *Cyberpower and National Security.* Vol. 1, in *Cyberpower and National Security*, by Franklin D Kramer, Stuart H. Starr and Larry K. Wentz, 3-23. Washington DC: Potomac Books.

Kuehl, Daniel T. 2009. "From Cyberspace to Cyberpower: Defining the Problem." In *Cyberpower and National Security*, by Franklin D. Kramer, Larry K. Wentz and Stuart H. Starr, 24-42. Dulles: University of Nebraska Press, Potomac Books.

Kurki, Milja, and Colin Wight. 2007. "International Relations and Social Sciense." In *International Relations Theories, Discipline and Diversity*, by Tim Dunne, Steve Smith and Kurki Milja, 14-35. Oxford: Oxford University Press.

Lake, David. 2010. "Rightful Rules: Authority, Order, and the Foundations of Global Governance." *International Studies Quarterly* 587–613.

Le Drian, Jean-Yves. 2018. "Le Monde / France Diplomatie (en)." *Minister Jean-Yves Le Drian: "We must take action to restore effective multilateralism." Le Monde Interview (23-24 September 2018).* September 23. Accessed 13 Mars, 2019. https://www.diplomatie.gouv.fr/en/the-minister-and-the-ministers-of-state/jean-yves-le-drian/press/article/minister-jean-yves-le-drian-we-must-take-action-to-restore-effective.

Le Gouvernment Francoise. 2018. *Le grand débat national - Gouvernment.fr.* December 10. Accessed April 22, 2019. https://www.gouvernement.fr/le-grand-debat-national.

Levin, Sam. 2018. *'They don't care': Facebook factchecking in disarray as journalists push to cut ties This article is more than 4 months old Journalists paid to help fix Facebook's fake news problem say they have lost trust in the platform - The Guardian.* December 18. Accessed April 28, 2019. https://www.theguardian.com/technology/2018/dec/13/they-dont-care-facebook-fact-checking-in-disarray-as-journalists-push-to-cut-ties.

Lipman, Maria, and Wilson Institute. 2019. *Russia's New Consensus: Acquiescence, Not Unanimity - The Russia File.* March 19. Accessed April 22, 2019. https://www.wilsoncenter.org/blog-post/russias-new-consensus-acquiescence-not-unanimity.

Lubenow, Jorge Adriano. 2012. "Public Sphere and Deliberative Democracy in Jürgen Habermas: Theorethical Model and Critical Discourses." *American Journal of Sociological Research* 58-71.

Lucas, Edward, and Peter Pomeranzev. 2016. *Winning the Information War Techniques and Counter-strategies to Russian Propaganda in Central and Eastern Europe.* Washington DC: Center for European Policy Analysis' (CEPA) Information Warfare Initiative.

Macaskill, Even, and Gabriel Dance. 2013. *NSA Files Decoded: What the revelations mean for you - The Guardian.* November 1. Accessed April 23, 2019. https://www.theguardian.com/world/interactive/2013/nov/01/snowden-nsa-files-surveillance-revelations-decoded#section/1.

Matlack, Carol, and Robert Williams. 2018. "France to Probe Possible Russian Influence on Yellow Vest Riots." *Bloomberg.* December 8. Accessed March 11, 2019. https://www.bloomberg.com/news/articles/2018-12-08/pro-russia-social-media-takes-aim-at-macron-as-yellow-vests-rage.

Matthew Field, Mike Wright. 2018. *Russian trolls sent thousands of pro-Leave messages on day of Brexit referendum, Twitter data reveals.* October 17. Accessed April 23, 2019. https://www.telegraph.co.uk/technology/2018/10/17/russian-iranian-twitter-trolls-sent-10-million-tweets-fake-news/.

Mayer, Jane. 2018. *How Russia Helped Swing the Election for Trump.* October 1. https://www.newyorker.com/magazine/2018/10/01/how-russia-helped-to-swing-the-election-for-trump.

—. 2019. *The Making of the Fox News White House Fox News has always been partisan. But has it become propaganda? - The New Yorker.* March 5. Accessed April 29, 2019. https://www.newyorker.com/magazine/2019/03/11/the-making-of-the-fox-news-white-house.

Maynes, Charles. 2019. *The trolls are winning, says Russian troll hunter.* March 13. Accessed May 4, 2019. https://www.pri.org/stories/2019-03-13/trolls-are-winning-says-russian-troll-hunter.

McCarthy, Daniel R. 2018. "Privatizing Political Authority: Cybersecurity, Public-Private Partnerships, and the Reproduction of Liberal Political Order ." *Politics and Governance (ISSN: 2183–2463)* 5-12.

McDonald, Allison. 2018. *The web really isn't worldwide – every country has different access.* December 6. Accessed April 15, 2019. https://theconversation.com/the-web-really-isnt-worldwide-every-country-has-different-access-106739.

McGuinness, Damien. 2017. *How a cyber attack transformed Estonia - BBC News.* April 27. Accessed April 22, 2019. https://www.bbc.com/news/39655415.

McNeil, Rob. 2019. *In Europe, media narratives about migration are deeply shaped by national press culture.* April 30. Accessed May 2, 2019. https://www.niemanlab.org/2019/04/in-europe-media-narratives-about-migration-are-deeply-shaped-by-national-press-culture/.

Mearsheimer, John J. 1900. *The False Promise of International Institutions.* ny.

Merton, R K. 1948. "The Self-Fulfilling Prophecy." *The Antioch Review 8(2)* 193-210.

Miller, Greg, Ellen Nakashima, and Adam Entous. 2017. *Obama's secret struggle to punish Russia for Putin's election assault - The Washington Post.* June 23. Accessed April 28, 2019. https://www.washingtonpost.com/graphics/2017/world/national-security/obama-putin-election-hacking/.

Mueller, Benjamin. 2019. *What Is Brexit? A Simple Guide to Why It Matters and What Happens Next - New York Times.* March 29. Accessed April 22, 2019. https://www.nytimes.com/interactive/2019/world/europe/what-is-brexit.html.

Mueller, Robert. 2019. *Report on the Investigation Into Russian Interference in the 2016 Presidential Election.* FBI Special Report, Washington DC: U.S. Department of Justice.

Naffi, Nadia. 2017. *The Trump effect in Canada: A 600 per cent increase in online hate speech.* November 1. Accessed April 24, 2019. https://theconversation.com/the-trump-effect-in-canada-a-600-per-cent-increase-in-online-hate-speech-86026.

NATO Committee on the Civil Dimension of Security. 2018. *Countering Russia's Hybrid Threats: An Update.* Security Report, Brussel: NATO.

NATO Cooperative Cyber Defense Center of Europe CCDCE. 2018. *Guide to Developing a National Cybersecurit - CCDCE NATO.* Accessed April 23, 2019. https://ccdcoe.org/uploads/2018/10/D-STR-CYB_GUIDE.01-2018-PDF-E.pdf.

—. 2019. *Tallinn Manual 2.0 The most comprehensive guide for policy advisors and legal experts on how existing International Law applies to cyber operations.* Accessed April 23, 2019. https://ccdcoe.org/research/tallinn-manual/.

NATO. 2018. *Cyber defense.* July 6. Accessed February 8, 2019. https://www.nato.int/cps/en/natohq/topics_78170.htm.

—. 2018. *NATO Member Countries.* January 4. Accessed April 4, 2019. https://www.nato.int/cps/en/natohq/nato_countries.htm.

—. 2019. *NATO's role in cyberspace.* February 2. Accessed May 4, 2019. https://www.nato.int/docu/review/2019/Also-in-2019/natos-role-in-cyberspace-alliance-defence/EN/index.htm.

Newman, Nic, Richard Fletcher, Antonis Kalogeropoulos, David A. L. Levy, and Rasmus Kleis Nielsen. 2018. *Reuters Institute Digital News Report 2018.* Research Report, London: The Reuters Institute.

Nichols, Chris. 2018. *Pants On Fire for Trump's claim about 'serious voter fraud' in California - Politifact.* November 28. Accessed April 22, 2019.

https://www.politifact.com/california/statements/2016/nov/28/donald-trump/pants-fire-trumps-claim-about-california-voter-fra/.

Noack, Rick. 2018. *New government leaflets tell Swedes to be prepared for war.* May 22. Accessed April 15, 2019. https://www.washingtonpost.com/news/world/wp/2018/05/22/new-government-leaflets-tell-swedes-to-be-prepared-for-war/?utm_term=.179bb308f311.

Obar, Jonathan A., and Anne Oeldorf-Hirsch. 2018. "The Biggest Lie on the Internet: Ignoring the Privacy Policies and Terms of Service Policies of Social Networking Services." *Information, Communication & Society* 1-20.

O'Sullivan, Donie, and Drew Griffin. 2019. *Cambridge Analytica ran voter suppression campaigns, whistleblower claims - CNN.* May 17. Accessed April 23, 2019. https://edition.cnn.com/2018/05/16/politics/cambridge-analytica-congress-wylie/index.html.

Owen, David, and Graham Smith. 2015. "Survey Article: Deliberation, Democracy, and the Systemic Turn." *The Journal of Political Philosophy* 213-234.

Pamment, James, Howard Nothhaft, Henrik Agardh-Twetman, and Alicia Fjällhed. 2019. *Countering information influence activities A handbook for communicators.* Research Report, Lund: Swedish Civil Contingencies Agencies & University of Lund. https://www.msb.se/RibData/Filer/pdf/28698.pdf.

Pamment, James, Howard Nothhaft, Henrik Agardh-Twetman, and Alicia Fjällhed. 2018. *The Role of Communicators in Countering the Malicious use of Social Media.* NATO Policy Brief, Riga: Department of Strategic Communication, Lund University.

Pasha-Robinson, Lucy. 2018. *Russian politician says 'let's hit Trump with our Kompromat' on state TV - The Independent.* September 5. Accessed April 3, 2019. https://www.independent.co.uk/news/world/europe/russia-donald-trump-kompromat-nikita-isaev-new-russia-movement-state-tv-us-president-a7929966.html.

Peters, Benjamin. 2012. "Normalizing Soviet Cybernetics." *Information & Culture* 145-175.

Petriczko, Ada. 2019. *Who was behind the Female Blackout?* October 3. Accessed April 23, 2019. https://newsmavens.com/news/aha-moments/1993/who-was-behind-the-female-blackout.

Politi, James. 2016. *Italy antitrust chief urges EU to help beat fake news Competition chief calls for regulation of false information on social media sites - The Financial Times.* December 30. Accessed May 3, 2019. https://www.ft.com/content/e7280576-cddc-11e6-864f-20dcb35cede2?mhq5j=e2.

Politifact. 2019. *All False statements involving Donald Trump.* April 3. Accessed April 27, 2019. https://www.politifact.com/personalities/donald-trump/statements/byruling/false/.

Pomeranzev, Peter, and Michael Weiss. 2013. *The Menace of Unreality: How the Kremlin Weaponizes Information, Culture and Money.* Special Report on Russian Foreign Policy, New York: The Interpreter, Institute of Modern Russia.

Popken, Ben. 2018. *Factory of lies: Russia's disinformation playbook exposed - NBC News.* November 6. Accessed April 29, 2019. https://www.nbcnews.com/business/consumer/factory-lies-russia-s-disinformation-playbook-exposed-n910316.

Poushter, Jacob. 2017. *Russians Say Their Government Did Not Try to Influence U.S. Presidential Election Most say Russia is playing an increasingly important role in world affairs.* Report on International Cyber Affairs, New York: Pew Research Center.

Pratkanis, A. R., and E. Aronson. 2001. *Age of propaganda: The everyday use and abuse of persuasion. (6ed).* New York: W.H. Freeman.

Pratkanis, Anthony, and Elliot Aronson. 2007. *Age of Propaganda, The Everyday Use and Abuse of Pesuasion.* New York: Henry Holt and company.

Qiu, Linda. 2017. *Fingerprints of Russian Disinformation: From AIDS to Fake News - The New York Times.* December 2. Accessed April 29, 2019. https://www.nytimes.com/2017/12/12/us/politics/russian-disinformation-aids-fake-news.html.

Qiu, Xiaoyan, Diego Oliveira, Alireza Shirazi, Alessandro Flammini, and Filippo Menczer. 2017. "Limited individual attention and online virality of low-quality information." *Nature Human Behaviour* id: 132.

Rapoza, Kenneth. 2017. *These Two Russian 'Fake News' Outfits Get Billions Of Hits On Facebook - Forbes.* September 17. Accessed April 22, 2019. https://www.forbes.com/sites/kenrapoza/2017/09/22/these-two-russian-fake-news-outfits-get-billions-of-hits-on-facebook/.

Reporters without Borders for Freedom of Information. 2019. *2019 World Press Freedom Index – A cycle of fear.* Annual World Press Freedom Index, Paris: Reporters without Borders.

Rescheto, Juri. 2019. *Opinion: The 'Russian internet' is Soviet-era oppression.* March 11. Accessed April 22, 2019. https://www.dw.com/en/opinion-the-russian-internet-is-soviet-era-oppression/a-47860717.

Reuters - The Guardian. 2015. *NSA tapped German Chancellery for decades, WikiLeaks claims.* July 8. Accessed April 23, 2019. https://www.theguardian.com/us-news/2015/jul/08/nsa-tapped-german-chancellery-decades-wikileaks-claims-merkel.

Reuters. 2018. *Facebook to drop on-site support for political campaigns - Reuters.* September 21. Accessed April 24, 2019. https://www.reuters.com/article/us-facebook-election-usa/facebook-to-drop-on-site-support-for-political-campaigns-idUSKCN1M101Q.

—. 2016. *Russia withdraws backing for International Criminal Court treaty.* November 16. Accessed April 15, 2019. https://www.reuters.com/article/us-russia-icc-withdrawal-idUSKBN13B1KJ.

Richard Ashworth, MEP. 2019. *BREXIT STANDING OVATION: No UK Prime Minister ever explained to British people what EU did for them .* March 28. https://www.youtube.com/watch?v=oh4xPvRR2oA&fbclid=IwAR3fkPovYNOCXrSrW65XKMXiPvXllYXkxkn0EIrvTgBfXW0eQ-3SYUb7Ib0.

Rodrik, Dani. 2014. "When Ideas Trump Interests: Preferences, Worldviews, and Policy Innovations." *Journal of Economic Perspectives* 189–208.

Russian Media VGTRK . 2015 . "Anatoly Ivanovich Kitov ." *Internet of Colonel Kitov.* https://www.youtube.com/watch?v=Wt2X1UsD3O4.

Sandberg, Sheryl. 2019. *By Working Together, We Can Win Against Hate - Instagram Press Release.* March 29. Accessed April 28, 2019. https://instagram-press.com/blog/2019/03/29/by-working-together-we-can-win-against-hate/.

Sanger, David E. 2018. *The Perfect Weapon War, Sabotage, and Fear in the Cyber Age.* New York: Random House Audio.

Sauer, Jeremy, Francisco Vega, Allisa Walker, and Carlos Haddock. 2017. *The Case for a New Joint Function: Operationalizing the Human Domain through Engagement.* https://smallwarsjournal.com/jrnl/art/the-case-for-a-new-joint-function-operationalizing-the-human-domain-through-engagement.

Schmidt, Michael. 2017. "Peacetime Cyber Responses and Wartime Cyber Operations Under International Law: An Analytical Vade Mecum." *Harvard National Security Journal*, 8: 239-280.

Schmidt, Vivien. 2017. "Britain-out and Trump-in: a discursive institutionalist analysis of the British referendum on the EU and the US presidential election." *Review of International Political Economy* 248–269.

Schmidt, Vivien. 2008. “Discursive Institutionalism: The Explanatory Power of Ideas and Discourse.” *Annual Review of Political Science* 11: 303-326.

Schmidt, Vivien. 2015. "Discursive Institutionalism: Understanding Policy in Context." In *Handbook of Critical Policy Studies*, by Vivienne Schmidt. Cheltenham: Edward Elgar Publishing, 2015.

Schmidt, Vivien. 2010. “Reconciling Ideas and Institutions through Discursive Institutionalism.” In *Ideas and Politics in Social Science Research*, by Robert Henry Cox and Daniel (editors) Béland, ch. 2. Oxford Scholars hip.

Schmidt, Vivien. 2011. "Speaking of change: why discourse is key to the dynamics of policy transformation." *Critical Policy Studies* 106-126.

Schofield, Hugh. 2019. *Gilets jaunes: Will Macron's Grand Debate tackle French crisis? - BBC.* January 15. Accessed April 22, 2019. https://www.bbc.com/news/world-europe-46878317.

Schreier, Fred. 2015. *On Cyberwarfare.* Geneva: The Geneva Centre for the Democratic Control of Armed Forces.

Schreier, Fred, Barbara Weekes, and Theodor H. Winkler. 2015. *Cyber Security: The Road Ahead.* Geneva: The Geneva Centre for the Democratic Control of Armed Forces.

Seddon, Mark. 2014. *Documents Show How Russia’s Troll Army Hit America.* June 14. https://www.buzzfeednews.com/article/maxseddon/documents-show-how-russias-troll-army-hit-america.

Shanley, Paul. 2017. *Producing a tool that will automatically verify UGC - Associated Press .* July 20. Accessed April 28, 2019. https://insights.ap.org/whats-new/producing-a-tool-that-will-automatically-verify-ugc.

Shea, Jamie. 2017. "How is NATO Meeting the Challenge of Cyberspace? ." *PRISM* , December 21: Volume 7, No 2.

Shuster, Simon, and Sandra Ifraimova. 2018. *A Former Russian Troll Explains How to Spread Fake News - Time.* March 14. Accessed May 4, 2019. http://time.com/5168202/russia-troll-internet-research-agency/.

Silverman, Henry. 2019. *The Next Phase in Fighting Misinformation - Facebook Operations Specialist.* April 10. Accessed April 23, 2019. https://newsroom.fb.com/news/2019/04/tackling-more-false-news-more-quickly.

Siudak, Robert. 2017. "Redefining cybersecurity through processual ontology of the cyberspace." *POLITEJA The Journal of the Faculty of International and Political Studies of the Jagiellonian University* 193-213.

Solon, Olivia. 2016. *In firing human editors, Facebook has lost the fight against fake news.* August 29. Accessed April 23, 2019.

https://www.theguardian.com/technology/2016/aug/29/facebook-trending-news-editors-fake-news-stories.

Spence, Alex, and Mark Di Stefano. 2019. "Buzzfeed.com." *A Mysterious Hard Brexit Group Run By A Young Tory Writer Is Now Britain's Biggest Spending Political Campaign On Facebook.* March 9. Accessed March 12, 2019. https://www.buzzfeed.com/alexspence/mysterious-facebook-brexit-group-britains-future-tim-dawson.

Starr, Stuart H. 2009. "Toward a Preliminary Theory of Cyberpower." In *Cyberpower and National Security*, by Franklin D Kramer, Stuart H. Starr and Larry K. Wentz, 43-55. Washington DC: Potomac books.

Stevens, Tim. 2010. *Cyber Security and the Politics of Time.* Cambridge: King's College .

Stevens, Tim. 2018. "Global Cybersecurity: New Directions in Theory and Methods." *Politics and Governance* 6 (2): 1-4.

Stoltenberg, Jens. 2017. *Doorstep statement by NATO Secretary General Jens Stoltenberg prior to the informal meeting of EU Ministers of Defense, Tallinn, Estonia,.* September 7. Accessed April 14, 2019. https://www.nato.int/cps/en/natohq/opinions_146642.htm?selectedLocale=en.

—. 2018. *Why cyber space matters as much to Nato as land, sea and air defence Jens Stoltenberg on Article 5 and why cyber defence has become core to the alliance.* July 12. Accessed May 5, 2019. https://www.ft.com/content/9c3ae876-6d90-11e8-8863-a9bb262c5f53.

Studdart, Amy. 2018. *Cybersecurity for Political Campaigns in the Digital Age.* September 20. https://www.power3point0.org/2018/09/20/cybersecurity-for-political-campaigns-in-the-digital-age/.

Sukhankin, Sergey. 2017. *The "Trump cards" of the Russian Propaganda and Disinformation Operations - Barcelona Centre for International Affairs.* June. Accessed April 22, 2019. https://www.cidob.org/en/publications/publication_series/notes_internacionals/n1_176/the_trump_cards_of_the_russian_propaganda_and_disinformation_operations.

Surkov, Vladislav. 2019. *Nezavisimaya Gazeta (Independent Newspaper).* February 2. http://www.ng.ru/ideas/2019-02-11/5_7503_surkov.html.

Suskind, Ron. 2004. "Without a doubt." *New York Times Magazine.* October 17. Accessed March 8, 2019. http://ronsuskind.com/without-a-doubt/.

Tavris, Carol, and Elliot Aronson. 2007. *Mistakes were made (but not by me).* London: Pinter & Martin.

Tenove, Chris, Jordan Buffie, Spencer McKay, and David Moscrop. 2017. *Digital Threats to Democratic Elections.* Academic Report, Vancouver, British Columbia: Centre for the Study of Democratic Institutions.

The Daily Beast. 2018. *Russia's Internet Research Agency Troll Farm Is Recruiting 'English-Speaking Journalists' - The Daily Beast.* April 3. Accessed April 3, 2019. https://www.thedailybeast.com/russias-internet-research-agency-troll-farm-is-recruiting-english-speaking-journalists.

The Daily Mail. 2012. *A Facebook crime every 40 minutes: From killings to grooming as 12,300 cases are linked to the site.* June 4. Accessed April 14, 2019. https://www.dailymail.co.uk/news/article-2154624/A-Facebook-crime-40-minutes-12-300-cases-linked-site.html.

The Intelligence Community (FBI, CIA & NSA). 2017. *Assessing Russian Activities and Intentions in Recent US Elections: The Analytic Process and Cyber Incident Attribution.* Intelligence Community Assessment ICA 2017-01D, Washington DC: US Director of National Intelligence.

The Regional Anti-Terrorist Structure of Shanghai Cooperation Organization. 2017. *RATS SCO.* September 17. Accessed April 12, 2019. http://ecrats.org/en/.

The Russia File, A blog of the Kennan Institute . 2018. *Putin's Managed Democracy Falters.* September 27. https://www.wilsoncenter.org/blog-post/putins-managed-democracy-falters.

The Washington Post. 2019. *The Washington Post - ABC News Poll April 22-25 2019 - The Washington Post.* Aprii 26. Accessed April 28, 2019. https://www.washingtonpost.com/page/2010-2019/WashingtonPost/2019/04/26/National-Politics/Polling/release_547.xml.

Thomas, Adam. 2018. *EJC joins forces with DataScouting to counter hate speech directed at journalists online We're building open source detection models, databases, training curricula and platform policy recommendations.* May 22. Accessed April 25, 2019. https://medium.com/we-are-the-european-journalism-centre/ejc-joins-forces-with-datascouting-to-counter-hate-speech-directed-at-journalists-online-60ed1c857a17.

Trudolyubov, Maxim. 2018. *Putin's Managed Democracy Falters (Op-ed) While Putin is credited with swinging the 2016 U.S. vote, electoral troubles are brewing at home - Moscow Times.* September 29. Accessed April 25, 2019. https://www.themoscowtimes.com/2018/09/29/putins-managed-democracy-falters-a63030.

U.S. Department of State. 2019. *NATO.* Accessed March 8, 2019. https://www.state.gov/p/eur/rt/nato/.

United Kingdom Parliament Committee. 2018. *Committee publishes Facebook answers - UK Parliament.* May 15. Accessed April 23, 2019. https://www.parliament.uk/business/committees/committees-a-z/commons-select/digital-culture-media-and-sport-committee/news/fake-news-facebook-evidence-17-191/.

United Nations. 2017. *International Covenant on Civil and Political Rights.* December 11. Accessed Aprril 20, 2019. https://www.equalityhumanrights.com/en/our-human-rights-work/monitoring-and-promoting-un-treaties/international-covenant-civil-and.

—. 1948. "Universal Declaration of Human Rights." *United Nations, Universal Declaration of Human Rights.* Accessed April 4, 2019. https://www.un.org/en/universal-declaration-human-rights/index.html.

United States of America. 2018. *Criminal Indictment of 14 Organizations and Individuals re. Cyber Crimes.* Washington, District of Columbia, February 16.

US Department of Defense. 2007. "US Department of Defense." *Irregular Warfare (IW) Joint Operating Concept (JOC).* September 11. Accessed March 11, 2019. https://fas.org/irp/doddir/dod/iw-joc.pdf.

US House of Representatives PSC on Intelligence. 2018. *Social Media Advertisments.* Accessed April 22, 2019. https://intelligence.house.gov/social-media-content/social-media-advertisements.htm.

Valeriano, Brandon, and Ryan Maness. 2019. "Fancy bears and digital trolls: Cyber strategy with a Russian twist." *Journal of Strategic Studies* https://www.researchgate.net/publication/330292030.

Valor, Onur. 2017. *Analyzing Social Big Data to Study Online Discourse and its Manipulation. Doctorate dissertation.* Columbus: Indiana University, June.

van Eeten, Michel JG , and Milton Mueller. 2012. "Where is the governance in Internet governance?" *new media & society* 720–736.

Walsh, Bryan. 2011. *Bursting the Bubble: Are We Isolated in a World Wide Web of One?* Mai 16. Accessed April 24, 2019. http://content.time.com/time/arts/article/0,8599,2071746,00.html.

Waltz, Edward L. 1998. *Information Warfare Principles and Operations.* Norwood: Artech House.

Wardle, Claire, and Hossein Derakhshan. 2017. *INFORMATION DISORDER: Toward an interdisciplinary framework for research and policy making.* Council of Europe report DGI(2017)09, Strasbourg: Council of Europe Report. https://rm.coe.int/information-disorder-toward-an-interdisciplinary-framework-for-researc/168076277c.

Warren, Mark E. 2017. "A Problem-Based Approach to Democratic Theory." *American Political Science Review* 111 (1): 39–53.

Warrick, Bobby, and Anton Troianovski. 2018. *Agents of doubt How a powerful Russian propaganda machine chips away at Western notions of truth.* December 10. Accessed April 22, 2019. https://www.washingtonpost.com/graphics/2018/world/national-security/russian-propaganda-skripal-salisbury/.

Warzel, Charlie. 2019. *The New York Times.* March 15. https://www.nytimes.com/2019/03/15/opinion/new-zealand-shooting.html.

Waters, Gwendolyn. 2012. *Social Media and Law Enforcement Potential Risks - FBI.* November 1. Accessed April 11, 2019. https://leb.fbi.gov/articles/featured-articles/social-media-and-law-enforcement.

Way, Lucan Ahmad, and Adam Casey. 2018. *Russia has been meddling in foreign elections for decades. Has it made a differene?* January 8. Accessed December 14, 2018. https://www.washingtonpost.com/news/monkey-cage/wp/2018/01/05/russia-has-been-meddling-in-foreign-elections-for-decades-has-it-made-a-difference.

Weinbaum, Courtney, and John N.T. Shanahan. 2018. "Intelligence in a Data-Driven Age." *Joint Force Quarterly*, July 3.

Wendt, Alexander. 1992. “Anarchy is what States Make of it: The Social Construction of Power Politics.” *International Organization* (MIT Press) (2): pp. 391-425.

Whyte, Christopher. 2018. "Crossing the Digital Divide: Monism, Dualism and the Reason Collective Action is Critical for Cyber Theory Production." *Politics and Governance* 73-82.

Zabrisky, Zarina. 2017. *Russian Cyberwar and Propaganda - Zarina Zabrisky - The Medium.* September 17. Accessed April 27, 2019. https://medium.com/@ZarinaZabrisky/russian-cyberwar-and-propaganda-f80e9ebe3280.

Zarate, Juan C. 2017. "The Cyber Attacks on Democracy." *The Catalyst, A Journal of Ideas from the Bush Centre.* Fall. https://www.bushcenter.org/catalyst/democracy/zarate-cyber-attacks-on-democracy.html.

Zhakarova, Maria. 2019. *Is Russia a guarantor of stability and security?* March 10. Accessed April 22, 2019. https://www.stopfake.org/en/is-russia-a-guarantor-of-stability-and-security/.