Summer 2019

The Trojan Horse in Your Head: Cognitive Threats and How to Counter Them

Lora Pitman
Old Dominion University, lora.ilieva@yahoo.com

THE TROJAN HORSE IN YOUR HEAD:

COGNITIVE THREATS AND HOW TO COUNTER THEM

by

Lora Pitman
LL.M. May 2014, Sofia University, Bulgaria
M.A. May 2016, Old Dominion University

A Dissertation Submitted to the Faculty of
Old Dominion University in Partial Fulfillment of the
Requirements for the Degree of

DOCTOR OF PHILOSOPHY

GRADUATE PROGRAM IN INTERNATIONAL STUDIES

OLD DOMINION UNIVERSITY
August 2019

Approved by:

Regina Karp (Director)

Bryan Porter (Member)

Matthew DiLorenzo (Member)

ABSTRACT

THE TROJAN HORSE IN YOUR HEAD:
COGNITIVE THREATS AND HOW TO COUNTER THEM

Lora Pitman
Old Dominion University, 2019
Director: Regina Karp

Vulnerabilities of the human mind caused by the way it is designed to process information have always been exploited in warfare, since the dawn of humanity. History is marked with frequent use of deceits and manipulations over the centuries, with examples ranging from the use of the Trojan Horse to Facebook's user-profiling. While largely used over time, these tactics, that I call cognitive threats, have not been collectively examined. I hypothesize that they pose a security issue to which prevention strategies on different levels could be successfully applied. The research questions that this study asks are what the characteristics of these cognitive threats, and what specific techniques could be employed to counter them. To respond to them and to contribute to filling the gap in the literature, I describe four case studies that illustrate some of the most common types of cognitive threats in the 21st century - the case with Maria Butina, the case with Russian disinformation, the case with ISIS recruitment, and the case with Cambridge Analytica. Then I analyze them and suggest different approaches that are fit to respond to the contemporary political and psychological features of these cognitive threats. The findings from the study, the policy recommendations, and the additional measures I propose are grouped into six categories: creating alternatives, narrative change, official government statements, legislative measures, education, and awareness.

This dissertation is dedicated to Dr. Steve Yetiv who we lost in 2018 but who will always live in the minds of his students, mentees, colleagues and friends.

ACKNOWLEDGMENTS

There are many people who have contributed to the successful completion of this dissertation. First, I would like to thank my advisor – Dr. Regina Karp for teaching me to think critically, assess world events and facts analytically, and last but not least, for always believing in me in every step of my graduate studies at Old Dominion University. I would also like to thank Dr. Bryan Porter for introducing me to social psychology and for encouraging my interest to its application in politics. I am also very appreciative of the efforts of Dr. DiLorenzo for agreeing to share his valuable feedback for this work.

TABLE OF CONTENTS

CHAPTER 1

INTRODUCTION

The Trojan War, one of the most emblematic events in the ancient civilization still fascinates scholars and practitioners. It begins with the abduction of the Spartan queen Helen, by Paris – a Trojan prince. As a response, Menelaus, Helen's husband and the king of Sparta asked his brother Agamemnon, king of Mycenae to join him for a campaign aiming to return Helen to Sparta and to punish the brazen Trojans. This mission was, reportedly joined by various of the ancient Greek heroes, including Odysseus, Achilles, and Ajax. Writers and historians in the antiquity claim that the siege of Troy lasted for ten whole years. Desperate from the lack of success, the Greeks knew that traditional military means would not ensure completion of their goal. Instead, they decided to implement a well-developed plan intended to make the Trojans open their own gates since the efforts to do so with force were hopeless. It is claimed that the Greeks built a giant wooden horse in only ten days. This creature was left in front the Trojan gates, with only one person around it, as the Greek ships were seen to slowly sail away from Troy, leaving their tents surrounding Troy in flames as a sign of retreat. Sinon, a Greek soldier, who was the only person around the horse, pretended to be abandoned by his people. He explained to the Trojans that the horse was a gift to the goddess Athena and symbolized entreaty of the Greeks for a safe return home in an act of remorse for destroying one of her temples in Troy. Perceived as a truthful story, the Trojans let the colossal horse figure inside the gates thinking it was a souvenir of their victory. What they did not know was that inside of the horse, there were 30 of the best Greek soldiers, waiting for the enemy to bring them effortlessly inside the gates. Not a single casualty marked the penetration of Greeks inside Troy, not a single sword or a single weapon was used to get beyond the gates. When the night came, the Greeks returned with their ships to Troy. In the meantime, the Greek soldiers left the horse and opened the gates to the Greek army who defeated the Trojans, brought back Helen to Menelaus, and ended the war.

Some claim that this story is a legend more than a historical fact, although Homer, Sophocles, Herodotus and Virgil all contribute with some details about the Trojan War that testify for its potential authenticity. Legend or not, the conflict in Troy ended with the victory of the Greeks only to open the door to other types of wars – those of the mind. What appeared to be the key to the Greek success was not military superiority but a simple trick that made the Trojans welcome their enemies straight into their home. The reason for the defeat was not a lack of bravery, lack of material capabilities or poor quality of their fortress. After all, they endured a 10-year-long siege. It was something else – a Pandora's Box that all humans have in their heads. The idea that the Greeks acknowledged their defeat, went home and left a gift behind them was so tempting that it inevitably led Trojans to think that this charming idea was the truth. Psychological research overwhelmingly confirms the phrase, that *people see what they want to see*. In the case with the Trojan War, what the Trojans wanted to see in this giant horse figure – a triumph of their military superiority - was what brought their defeat. While this ancient story serves as a proverbial lesson for those who are too naïve, the history before the Trojan War and after this is full of examples of similar deceptions because an ultimate solution to the problem was never achieved. Access to perfect information is impossible, and people only have at their disposal a limited amount of it. In addition, human cognition can further obscure a more accurate judgment of facts. It is inclined to make deductions in a predictable way when influenced by certain emotions in certain situations. Such judgment looks objective and unimpeded for the social perceiver. What people frequently are not aware of is that it is quite enough an emotion in a particular social setting to be provoked, in order the cognition to produce a predictable reaction that corresponds to this emotion. What is more intimidating is that such barriers to independent thinking are not only inherent for individuals with medical conditions. They are typical for all individuals because each person has a *Pandora's box* that represents how vulnerable our cognition is when it processes information, as one simple trick of the mind, can always open the box. Such deceptions and manipulations, I call in the present work cognitive threats.

Centuries after the Trojan Horse deception, the problem with cognitive manipulation in warfare kept being present even in the 21st century. The issue was the same but manifested differently, as a lot has changed since the classical antiquity period, but not everything. Wars were still led, the desire to win them was as high as it once was. In spite of this, there were also new actors. They had new goals and new ways of using their old weapons – persuasion. The addictive nature of social networks and the mimicking of an in-person conversation made people eager to communicate more than ever. The basic human need for maintaining a particular social image, a distinct identity, made users share a wide variety of information not only with people with whom they are close but also, sometimes quite unconsciously, with people who they do not even know. It was not long before power elites started seeing value in social networks as a means of warfare. The involvement in all sorts of actors in society changed even modern diplomacy and how it is conducted. Disinformation as an old tool for deception gained new meaning for state and non-state actors. A rare combination between humans' cognitive mechanisms and the presence of a suitable platform for manifestation of the liabilities of those mechanisms gave birth to one of the most effective weapons in the 21st-century warfare - online disinformation.

The success of social media did not remain a secret for a different, post-Cold War type of threats coming from non-state actors in the face of radical organizations. The main kind of threat that they posed was related to their violent means of achieving their goals, but this was not exhausting all the ways in which they were endangering the peace. Their skillful use of the online space has become a powerful tool of recruitment of people. They were enticed to join these radical organizations by allegedly making an independent choice. That choice was, however, influenced to a large extent by manipulations and in many times by deception. The promises that the cause of the radical organization will fulfill a longing that the vulnerable target has was the key to the success of recruitment operations. At the same time, anti-terrorism units were failing to eliminate the ongoing online recruitment of new members because of the anonymity for which the online space allows. Only reasonable suspicion of illicit activities would be enough to restrict some of the online privacy of the users, as an essential human right guaranteed on both the national and international level in most states. The paradox was apparent: the more freedom people had to communicate and connect, the less independence they had in their thinking and decision-making because their judgment was exposed to even more cognitive threats than before.

Individuals have always been an important factor in the political scene but only if they had power or were members of collectively expressed interest. Generally, when thinking about powerful individuals, one would be most likely to imagine state leaders. With the proliferation of non-state actors, however, leaders of organizations and corporations became just as powerful as states, in some cases. They have tremendous assets at their disposal including material, non-material and human resources. They also have certain purposes and goals. One of them is related to profits, but there is also another factor of essence – support of specific policies that will most likely lead to even more profits in the future. Especially, with the current level of globalization, it was inevitable that big corporations stayed immune from the changes on the global political scene. They embraced these changes and employed them to work for them – as it is in the case with social media. Instead of letting political and social distractions take away the users' attention from social networks, they were used as an arena for discussing them. Social networks quickly became new sources of information about events of importance. The media outlets delivering the information were not the social platforms themselves, however, thus their owners are still not held accountable for the information that is disseminated through their products. Consequently, social media are providing only a fruitful environment in which political and corporate interests merge to benefit from cognitive vulnerabilities in humans. The so-called super-empowered individuals who own these companies have little to no interest in changing the current situation. It works for their goals – vivid discussions and exchange of information increases the popularity of their networks and generates a larger pool of topics for users to discuss. Moreover, once something is posted on social media, it becomes an asset belonging to the owner of the platform. This enormous volume of information collected through social media could help construct a map of an individual's or a group of individuals' cognitions. A map that could be easily sold to the highest bidder.

With every technological development in human history, there were also notable changes in society, politics, education, and culture. The changing environment made wars different, some of which not even *real* wars at all. The traditional and non-traditional wars required new weapons. Some of them were intelligence gathering, deception, and disinformation. With the growing numbers of democratic countries in the world, the meaning of the individual in the system also expanded. The mechanism for winning post-modern wars, that were not wars by definition but merely conflicts, was to know the individuals who create the system. Intelligence-gathering has always been a tool for getting acquainted with the enemy with the ultimate purpose of influencing them. Within the context of expanding democratization, it has the meaning of a preliminary step for gaining power over the individuals as a way to impact the state itself through them. In the digital age, the intelligence-gathering means simply the collection of data, most of which were even voluntarily shared by users on social media. Considering these circumstances, it was almost inevitable that these data were not weaponized. Individuals' personal information was directed against them in the global game of politics in which they were the vehicle for a change of the status quo, and thus the targets. In the era of democratization and with the increased importance of the individual, the states retain their role of central units in the system of international relations but with one limitation – their identities are malleable and a subject to citizens' preferences. With some exceptions, post-modern conflicts no longer lead to traditional *hot* wars against the enemy state directly, but against its people. Consequently, the protection of the individuals, their cognition and their independent decision-making should be a matter of national and global security. This argument also pertains to authoritarian countries that intentionally distribute disinformation to their population through government-owned outlets in order to support the state's goals (e.g. Russia). Regardless, democracies are much more exposed to cognitive threats since, while in autocracies, the perpetrator is only one – the state itself, in democracies the range of the perpetrators is much wider, due to the transparency and the treasured freedom of speech.

I designed this study to respond to the following research questions: what cognitive threats are, and how to counter them. The preferred methodology is qualitative in nature and includes the exploration of four case studies of cognitive threats. Before directly analyzing them, I provide context to the problem by building upon the following three pillars: 1) psychological studies proving that human cognition is vulnerable; 2) political psychological research that underlines how internal experiences of humans are exploited for political gains; 3) historical overview of cognitive threat showing that different conditions matter for the magnitude and the success of these security threats. My hypothesis is that information always mattered in different periods of history, all the way to the present days. In order to gather information or/and change the opponent's behavior based on this information, actors skillfully took advantage of the basic information-processing mechanisms inherent for humans. In the contemporary political, technological and social environment, these threats represent an even more significant problem that finds expression in a wide range of scenarios in which one actor benefits politically from triggering a certain psychologically predictable reaction from the victim. This problem, I argue, is best addressed through prevention strategies based on the individual psychological and political elements that make the threat possible in the first place. They are inevitably intertwined in cognitive threats since the latter is a perceptual category that contains an intention by the perpetrator to inflict damages to a victim. The threat remains as such in the psyche of the perpetrator and takes the form of an actual attack when the perpetrator acts upon their intentions. Regarding the perception of the victim, they may have experienced the influence to their cognition as a threat or not. In the first case, even if the individual perceives the cognitive threat as such, it is almost always after the damages have been inflicted, which is when the victim becomes aware of the deception, if it is successful. In some more rare cases, the victim becomes aware of the cognitive threat before the damages have been inflicted. In other cases, the individual never realizes that their cognitions have been influenced. They consider their decision-making process as independent, and not influenced, as this is namely why cognitive threats are so secretive, difficult to expose and prevent. Moreover, they could be distributed and facilitated through various actors, state and domestic or international non-state ones, and different phenomena with systemic effect (e.g., globalization). Thus, cognitive threats could be studied on all levels of analysis. The level that always has to be present in every analysis, however, is the individual level since the threat is aimed at one or more persons' cognitions. This is also the reason that makes findings, derived from level one of analysis - about human cognition, relevant to all other levels of analysis.

Cognitive threats differ from non-cognitive ones through one essential component that has to be present in them – the purposeful attempt of a perpetrator to influence the individual's cognition through exploiting innate cognitive vulnerabilities in order to benefit politically. They could be labeled as vulnerabilities, however, only when they are being exploited by an interested party. Otherwise, they should simply be labeled as the human cognitive apparatus with all its inherent psychological mechanisms for reaction. That said, cognitive threats exist only when an actor intends to obtain gains by provoking a change in the behavior of an individual through exploiting the existing cognitive structures of the human mind. Relevant example would be instigating fear, stress and anxiety that will make the individual reacting defensively to a highlighted by the perpetrator threat. In this intentionally induced state of distress, the individual searches for more information which is typically provided by the perpetrator in the form of a solution that allegedly resolves the problem. To achieve this goal, very often there are other pre-existing conditions of the victim that the perpetrator exploits such as personal loss, financial need, ontological insecurity, and the immaturity of the victim.

While cognitive threats are not material in nature, but psychological, they may have material consequences. For instance, global warming is a non-material threat with material consequences but as opposed to cognitive threats, it does not involve an interested party that attempts to influence the victim's psyche. For cognitive threats to be constituted as such, it is only needed that the perpetrator (state, non-state actor or an individual) perceives them as threatening to the victim, who is almost always unaware of the influence that is exercised. In this sense, the cognitive threat can only disappear when it is not intended as a goal by the perpetrator who is ready to act upon their intention. Therefore, I argue that the best strategy against this kind of threats would be strategies such that are focused on prevention.

The study I am conducting seeks to contribute to the security studies literature. In particular, this work's goals align with the ones that the field of non-traditional security sets forth. It seeks to introduce the idea of cognitive threats and to fill a gap in the literature about the applicability of prevention strategies based on the concrete expressions that cognitive threats have in the contemporary environment. In terms of scholarly agenda, I advocate for the inclusion of cognitive threats in the security studies field literature, as their effectiveness and the seriousness of their consequences have been proven continuously throughout the centuries, even though they have not been officially part of traditional definitions of war. My intention for this work is to serve the needs of academics and policy-makers, nonetheless, some practitioners who see this study's applicability in their research as well. It is organized in the following way. In Chapter 1, I introduce the problem. In Chapter 2, I present the idea of cognitive threats and why they are so difficult to control. To explain why, I provide an overview of the basic mechanisms upon which the human cognition is built. Then, I outline some vulnerabilities that it has in terms of processing information. In addition, I follow what possible effects can emotion-inducing situations have on decision-making and overall behavior. Based on these deductions, I explain why such cognitive dynamics present threats to independent decision-making and behavior, and how this has an impact on political level. Next, in Chapter 3, I describe the evolution of cognitive threats to explore what factors changed them over time and how. I also discuss the value and the conditions of previously employed ways to combat them in different historical periods. I maintain that prevention strategies should be preferred in addressing cognitive threats rather than focusing on their consequences after they take the form of an active campaign (attack) and are no longer a just a threat. In Chapter 4, I offer four case studies that illustrate some of the most common types of cognitive threats in the 21st century. By studying them, I try to identify their elements, the reasons for their success, their effects and some contextual factors that are of importance. Chapter 5 consists of an analysis of the described scenarios, as its goal is to produce strategies that are fit to counter the contemporary features of cognitive threats. Chapter 6 summarizes the findings of the study, outlines policy recommendations, and discusses implications for the role of academia in studying cognitive threats as a conceptual category. Lastly, I suggest some potential factors that should be taken into consideration in thinking about the future of cognitive threats.

CHAPTER 2

COGNITION AND COGNITIVE THREATS

In Chapter 2, I introduce the idea of cognitive threats as a central element in this work. Since the focus of the current study is political in nature, I continue by exploring the academic dialogue between psychology and politics as I seek to identify what psychological concepts inform political psychology, how they are used, what are the methods and the theories that are interested in employing psychology in politics. Then, I provide an overview of one of the most central elements in political psychology – the human cognition, how it is constructed, what are its components, how they function and what is the relationship between them. It has to be mentioned that the literature on this topic is more than voluminous since it is one of the most critical questions in psychology. Therefore, I only selected foundational works that build the understanding of how cognition works regarding information – its selection, interpretations and reactions to it. Next, I link the cognition to its inevitable interaction with society and revisit the questions about cognitive processes but this time in a social context. For instance, how people make inferences and what factors affect them, how important is control for the aggregation of information and how social judgments and social stereotypes are formed based on the selection and the interpretation of certain information. After I outline the importance of the individual in the study of politics, I emphasize the dual role that they have – as an agent that can influence structures, and as a political tool for achieving specific goals. Consequently, I list some of the recognized in the literature cognitive mechanisms that make the individual both an influence and a subjugated instrument to political goals.

The emerging cognitive threat: a result of political moves and processes

In order to understand how the individual can be used as a tool for achieving political results, first, I will outline what is defined as a *threat* in the study of politics and international relations and what is the place of the individual in it. Next, I will explore how a threat to the individual can become a collective national and international threat, what are the characteristics of these emerging cognitive threats and their relationship with two phenomena already established in the literature such as propaganda and frauds, both possible in the physical and the cyberspace.

Individual security and national security. Similar to many questions in the study of politics and IR, the field is not unanimous about its understanding of what security studies agenda should include and based on this, what concepts are included in the notion of *threat*. Threat is defined by Rousseau and Garcia-Retamero as "a situation in which one agent or group has either the capability or intention to inflict a negative consequence on another agent or group"[1]. In the context of politics, this intention could be either explicitly demonstrated or implied. Stephen Walt[2] discusses this question in his work from the early post-Cold-War period and concludes that security is inevitably and immediately related to the concept of war. He refers to a definition by Nye and Lynn-Jones[3] that focuses on "the study of the threat, use, and control of military force"[4]. As the challenges discussed in the field multiplied, it became necessary that

[1] David L. Rousseau and Rocio Garcia-Retamero, "Identity, power, and threat perception: A cross-national experimental study," *Journal of Conflict Resolution* 51, no. 5 (2007): 745.

[2] Stephen M. Walt, "The Renaissance of Security Studies," *International Studies Quarterly* 35, no. 2 (1991).

[3] Joseph S. Nye Jr. and Sean M. Lynn-Jones, "International security studies: a report of a conference on the state of the field," *International security* 12, no. 4 (1988).

[4] Walt, "The Renaissance of Security Studies," 212.

new approaches are undertaken. Krause and Williams[5] observed that the discourse about expanding the security studies agenda either moves toward the study of the individual and human security, or toward more complex approaches about the global environment, regional, international security. At the same time, some neorealists[6] [7] [8] remained true to their systematic paradigm excluding the individual from equations of how anarchy affects the system. Aside from the realist school of thought, however, the figure of the individual became more and more important even for those pursuing an institutional sociological approach because “with the end of the Cold War, the mix of factors affecting national security is changing. Issues dealing with norms, identities, and culture are becoming more salient”[9]. In a chapter about human security, Fen Osler Hampson[10] refers to the definition offered in the report of the Commission on Human Security that states that its role is “to protect the vital core of all human lives in ways that enhance freedoms and human fulfillment. Human security means protecting fundamental freedoms - freedoms that are the essence of life. It means protecting people from critical (severe) and pervasive (widespread) threats and situations”[11]. When it comes to the cognitive abilities of an individual, it is important to delineate what are these fundamental freedoms and what these threats represent. Article 18 and 19 from the Universal Declaration of Human Right underline that first, “everyone has the right to freedom of thought…”[12] and “to freedom of opinion and

[5] Keith Krause and Michael C. Williams, "Broadening the Agenda of Security Studies: Politics and Methods," *Mershon International Studies Review* 40, no. 2 (1996).

[6] John J. Mearsheimer, "The false promise of international institutions," *International security* 19, no. 3 (1994).

[7] Walt, "The Renaissance of Security Studies."

[8] Kenneth Neal Waltz, *Theory of international politics*, 1st ed. (Boston, MA: McGraw-Hill, 1979).

[9] Peter J. Katzenstein, *The culture of national security: Norms and identity in world politics* (New York, NY: Columbia University Press, 1996), 2.

[10] Fen Osler Hampson, "Human Security," in *Security Studies: An Introduction*, ed. Paul D. Williams (New York, NY: Routledge, 2012).

[11] Commission on Human Security, "Human Security Now," (New York, NY 2003), 4.

[12] United Nations General Assembly, "Universal declaration of human rights," (1948), Article 18.

expression; this right includes freedom to hold opinions without interference…"[13]. That said the freedoms that human security protects include gathering and processing of information that is not in any way purposefully obstructed by external influences.

Regardless of the threat that an intentional manipulation of information conveyed to the individual can cause, there is something more than this being a question merely in the realm of human security. What if this threat to the individual could also constitute and is perpetrated with the purpose to harm a particular social group, a state or an entire region's security? Allowing for a discussion of these threats targeting the individual but only as means to harm a broader entity links the human security research agenda to the agenda followed by neorealists who exclude the study of the individual but are still concerned about the security of the state. A research question focusing on *cognitive threats* could bridge the agendas of both divisions in the field despite their different assumptions about the world of international relations since these kinds of threats include both the individual and the system as objects of a threat. The direct mechanism that makes the individual threat a collective one is manipulating one's perspective through their cognitive abilities and the related processes "that turn individual emotions collective, social public, and, thus, political"[14].

Cognitive threats. In the past, the field of security studies focused almost ultimately on military affairs and traditional threats as the extreme point in conflict was thought to be the beginning of a war. Nowadays, while wars still occur, the liberal order and the democratization of many countries made it unlikely that states go to war with each other using their militaries. This does not mean that conflicts do not occur. It does not even mean that wars do not occur.

[13] Ibid., Article 19.

[14] Emma Hutchison and Roland Bleiker, "Theorizing emotions in world politics," *International Theory* 6, no. 3 (2014).

They just have different forms and expression in the contemporary highly interconnected technological world in which ideas could be used as weapons in conflicts. These modern conflicts and modern wars do not involve casualties in the traditional sense, but they are still not victimless. However, the harm inflicted to the individuals is not the ultimate goal that these modern wars pursue. They seek to achieve political goals by manipulating the cognition of a person who will inflict some harm to others. Based on this, cognitive threats could be characterized as any type of information, written and/or verbal, in the cyber and physical space, purposefully conveyed to a recipient(s) with the intent to provoke a certain reaction that will cause harm to them and another party. This reaction is in nature inherently linked to cognitive processes, emotions and habits could be expressed in the form of a verbal or physical act or both. At the same time, the reaction could also be an intentional abstaining from verbal or physical acts, as an act of a protest, for instance. The recipient of the information could immediately express a certain reaction as a consequence of the conveyed information, or it could be delayed with seconds, minutes, months or even years – when the information acts as a trigger to the recollection of past events and associations. The recipient of the information is in the position of a victim and a perpetrator to harm to others. They are first and foremost a victim because their judgment is manipulated. It is manipulated through the delivery of a specific type of information that the author of the message suspects or knows, and hopes and intends, to enable a chain of cognitive processes that will make the recipient do something that benefits the cause of the author. Second, the recipient of the information acts also as an unconscious perpetrator of harm to third parties that could be another individual, an institution, an organization, a state or groups of states. The harm could be of physical, emotional, financial or political nature. To illustrate this theoretical concept, I would like to point to four examples that elucidate its components and its meaning.

The first most common scenario in which this concept finds application is the proliferating cases of disinformation on popular topics for political purposes. The second set of cases in which cognitive threats are present refers to political espionage conducted through intentional misleading of the recipient of the information. For instance, numerous cases show how humans can be exploited to give away secrets of national value and not even through extortion, blackmailing or other similar practices. Instead, a simple chain of cognitive processes in the brain of an individual can be stimulated as this could be enough to get results that other strategies may fail to deliver. The goals that such manipulations can pursue could pertain to trade secrets, classified/confidential information, passwords or any other ways to gain access to such. The third cluster of cognitive threats refers to recruiting practices of radical religious or extremist groups. In such cases, the individual is recruited through the purposeful induction of emotions and the offer of a powerful solution to various problems. The recruiters, however, do not only aim to change the individual's attitude about certain issues or to take them to the extremes but instead, they seek to provoke a certain behavior – joining the radical organization that aims to cause harm to third parties. The fourth type of scenarios are related to a new form of power concentrated in the hands of super-empowered individuals[15]. Many of them created companies through which a large amount of information is collected. For instance, in the case of Facebook and other social media, the users themselves are the ones providing the information. What they did not know, at least, not until recently is how their information could be used and to what end. One of them is, of course, profit. However, this does not mean that profit is the only goal of the

[15] Thomas L. Friedman, "DOScapital," *Foreign Policy*, no. 116 (1999).

collection of information. Instead, marketing and political purposes were frequently present after large amounts of information were sold to corporate or political entities. Thus, not only the individuals themselves suffered from the leaks of their own information, but the consequences had a much wider range – from tailored marketing messages according to one's personal preferences to political messages to targeted audiences whose final goal was influencing the outcome of elections and referendums. Since cognitive threats include only tools for influence on mental rather than the physical level, they should be compared and contrasted with two similar phenomena: frauds (traditional and cyber) and propaganda.

Cognitive threats and frauds. In order to discuss how fraud, as a crime, differs from cognitive threats, it should be first underlined what criteria I will use. Popular definitions of fraud generally incorporate four major elements: 1) an individual or a collective body presents a certain information to the recipient that is not true; 2) the information presented to the victim is believed to be true; 3) the victim perceives the information as true and exhibit behaviors that are activated by the information; 4) the behavior of the victim causes the latter to endure financial or property losses as a consequence from the untrue information that was conveyed to them[16]. The following comparison using these four categories seeks to identify to what extent fraud overlaps with cognitive threats. The first component from the definition of fraud slightly differs from the one of cognitive threats. While there is certain information conveyed by an individual or a collective body, in the case of cognitive threats, this information could be true or false. Second, for frauds, the information should be perceived as true but for cognitive threats it could be perceived as false and still to trigger some reaction in the recipient that is desired by the sender

[16] Babak Sadighi Firozabadi, Yao-Hua Tan, and Ronald M. Lee, "Formal definitions of fraud," in *Norms, logics and information systems-new studies in Deontic logic and computer science*, ed. Paul McNamara and Henry Prakken (Amsterdam, Netherlands: IOS Press, 1999), 279.

of the message. Third, regardless of whether the recipient thinks the information is true or untrue, there is some reaction that is provoked in them. Fourth, while for frauds, it is necessary that the victim suffer some economic loss, when it comes to cognitive threats, the loss could be of any other kind as well as of financial/property nature. Based on this juxtaposition, a logical question follows: could a fraud constitute a cognitive threat? The answer to this question is affirmative. In some cases, the same elements that characterize fraud as a crime could also present a cognitive threat. For instance, an employee in a company in the defense sector responds to an e-mail allegedly sent by their supervisor and discloses trade secrets. As a result, the employee is fined or fired thus suffering financial losses, as well as the company itself. So far, this constitutes fraud. But what if the company from which the trade secrets were stolen was a contractor for a state's defense project and the trade secrets were stolen for political rather than merely economic purposes? In this case and in other similar ones the fraud merges into the broader understanding of cognitive threats. That said cognitive threats are not necessarily frauds but could include them in some specific cases.

Cognitive threats and propaganda. When thinking about disinformation, as an example of a cognitive threat, one can easily confuse it with the notion of propaganda. Lasswell characterizes the latter as "the management of collective attitudes by the manipulation of significant symbols"[17]. This definition captures a variety of elements that can also carry meaning for cognitive threats. However, for cognitive threats, only one person can be the target of the manipulation, rather than a group of people. Regardless, the most significant difference between propaganda and cognitive threats is that the main purpose and the end goal of propaganda are to shape particular moods toward an idea or a person. In the case of cognitive threats, shaping

[17] Harold D. Lasswell, "The Theory of Political Propaganda," *American Political Science Review* 21, no. 3 (1927).

moods, habits and emotions are not the final destinations that the threat reaches. Instead, it seeks to go further by making the individual do something more than just changing their attitude about a particular matter. Propaganda could be used as a tool to manipulate certain judgments and opinions but only with the aim to achieve another goal. For instance, one of the goals of disinformation could be the defamation of a particular political party and the reorientation of the voters toward another – the change of their attitude is needed but only as long as it serves also to change their behavior when the elections come. It is possible that propaganda is employed indirectly in this process, but in comparison to cognitive threats, it lacks concrete objectives different than changing one's mind on its own. Consequently, propaganda could be part of a cognitive threat, but it does not overlap fully with it.

Free choice and cognitive threats. Since cognitive threats are so widespread then what is the place of the free choice considering the politicization of almost every issue in society? Free choice is a complex category of philosophical questions that will not be by itself an object of discussion in the current section. Instead, I would like to emphasize that cognitive psychology has proven that there is a multitude of factors that drive our attitudes, behaviors, opinions, and habits – a fact that makes it very difficult to talk about an entirely free, independent choice. However, there must be some free will that is independent of factors influencing people's judgment. A compromise between the ideal scenario of a free choice and all the elements that affect one's decision-making would be the informed choice. In the context of the idea of cognitive threats, an informed choice would be when the individual is aware that the information conveyed to them with certain intentions by the author, and with a certain goal. Moreover, an informed choice should include knowing who the real author of the message is, the intentions of the author to send the message, and how the reaction to the message is intended to affect the recipient and other parties. If the recipient has all this information or a good idea about these questions, then this could be defined as making an informed choice. An informed choice excludes the existence of cognitive threats because the cognitive manipulation element will be substituted by consent to specific consequences that the recipient of the information knows will or might follow from their actions.

The individual in the study of politics

When thinking about politics, the image of the individual immediately emerges in one's mind. That is because politics will be impossible without the presence of people – leaders and followers, and their opponents. While these people all have cognitive apparatuses that are, as described already, somewhat similar, their behavior can be governed by different rules – the ones of social psychology. While it is very challenging to construct an exact formula about political behavior and politically-motivated or driven acts by people, cognitive and social psychology to a large extent contribute to a deepened understanding of the world of politics. As Rose McDermott[18] underlines, while efforts were made by political scientists to contribute to the field of psychology, it is to a large extent recognized that it is the psychology field that imports its theories into the political science realm.

Theories and the place of the individual in them. In order to provide an accurate overview of the place of psychology in political science and international studies, I will first outline what place different IR theories assign to the individual, followed by the methods mostly used in the field. One of the most prominent theories in IR is undoubtedly the realist school of

[18] Rose McDermott, *Political psychology in international relations* (Ann Arbor, MI: University of Michigan Press, 2004).

thought. Classical realists such as Machiavelli[19], Thucydides[20] and Morgenthau[21] place an emphasis on human nature as a source of political conflict. As opposed to this, the structural realism that later became the more prevalent realist way of thinking made a drastic turn in terms of the place of the individual in politics. Assigning a great role to the system, rather than to the individual, Waltz[22] divided the three levels of analysis in the contemporary study of politics to an individual, domestic and systemic. He stresses that it is the systemic level on which scholars should focus as it carries the most importance for understanding how the international relations shape the world.

Similar to realists, liberalists[23] [24] [25] look at the system in general but through a different lens – not how it inevitably hinders cooperation but how cooperation can emerge between the units in the system. In this theory, states are also seen as the main actors with the only difference that an accent is placed on domestic politics and their characteristics as well as on the system itself, thus leaving the role of the individual somewhat underappreciated. Constructivists such as Wendt[26], Kratochwil[27] and Katzenstein[28], on the other hand, explore topics such as identity, traditions, culture and any other elements that help the individual to perceive and assess events

[19] Niccolò Machiavelli, *The prince*, ed. Harvey C. Mansfield, 2nd ed. (Chicago, IL: University of Chicago Press, 1998).

[20] Thucydides, *The complete writings of Thucydides. The Peloponnesian war*, ed. Richard Crawley and Joseph Gavorse (New York, NY: The Modern Library, 1934).

[21] Hans Joachim Morgenthau, *Politics among nations the struggle for power and peace*, 4th ed. (New York, NY: Knopf, 1967).

[22] Waltz, *Theory of international politics*.

[23] Robert O. Keohane and Joseph S. Nye, *Power and interdependence*, 4th ed.. ed. (Boston, MA: Longman, 2012).

[24] Helen V Milner, *Interests, institutions, and information: Domestic politics and international relations* (Princeton, NJ: Princeton University Press, 1997).

[25] Bruce M. Russett and John R. Oneal, *Triangulating peace democracy, interdependence, and international organizations* (New York, NY: Norton, 2001).

[26] Alexander Wendt, *Social theory of international politics* (Cambridge, UK: Cambridge University Press, 1999).

[27] Friedrich V. Kratochwil, *Rules, norms, and decisions: on the conditions of practical and legal reasoning in international relations and domestic affairs*, vol. 2 (New York, NY: Cambridge University Press, 1991).

[28] Peter J. Katzenstein, ed. *The culture of national security: Norms and identity in world politics* (New York, NY: Columbia University Press, 1996).

and other people. Katzenstein[29], in particular, advocates for an approach that may not necessarily be limited to one theory or one problem-solving technique thus enhancing the field with a perspective oriented toward leaving theoretical parsimony concerns aside. A relatively newer wave in the study of IR has presented the field with contributions focusing on rational choice[30], psychobiography and social psychology[31] [32] [33]. A central element within these contributions is the attention on the individual and their mental and decision-making processes, values, interests, and emotions. For instance, one of the scholars who stands out with high accuracy of his prediction models, based on expected utility, is Bruce Bueno De Mesquita[34]. His design rests on four pillars: 1) individuals interested on the outcome of the negotiations; 2) the initial bargaining preferences of the participants; 3) bargaining power of the participants; 4) significance of the issue at hand for the stakeholders. In spite of the success of this model and such that are relying on rational choice and expected utility theories, some doubt has been cast in regarding their reliability since "such assumptions lack empirical descriptive accuracy in real tests of human behavior and decision making"[35]. As McDermott underlines, in some more complex political situations that require a more detailed look into how human's cognition and social interaction work, rational choice theories could be of little help. Therefore, to assure relatively broad applicability of the implications and conclusions of this work I will rely on more general

[29] Peter J. Katzenstein and Nobuo Okawara, "Japan, Asian-Pacific security, and the case for analytical eclecticism," *International Security* 26, no. 3 (2002).
[30] Bruce Bueno De Mesquita, *Principles of International Politics* (Thousand Oaks, CA: SAGE Publications, 2013).
[31] Daniel L. Byman and Kenneth M. Pollack, "Let us now praise great men: Bringing the statesman back in," *International Security* 25, no. 4 (2001).
[32] Jerrold M. Post, "Current concepts of the narcissistic personality: Implications for political psychology," *Political Psychology* 14, no. 1 (1993).
[33] Ofer Feldman and Linda O. Valenty, *Profiling political leaders: Cross-cultural studies of personality and behavior* (Westport, CT: Greenwood Publishing Group, 2001).
[34] Bruce Bueno de Mesquita, David Newman, and Alvin Rabushka, *Forecasting political events the future of Hong Kong* (New Haven, CT: Yale University Press, 1985).
[35] McDermott, *Political psychology in international relations*, 57.

theoretical and empirical underpinnings from political psychology than on the assumptions of rational choice theories.

Methods. When analyzing the relationship between political science and international studies, and psychology, it is important to mention what are the methods that the former employs in order to study the latter. The methods established in the literature of political psychology are mainly five, and they can be used alternatively or jointly to study the research question interesting the scholar[36]. Political psychology finds expression mostly in the literature about American politics, but there is no reason why the same tools should not be used to extend the knowledge produced in other fields of IR/political science. The first kind of methods that scientists implement is the one involving experimentation and simulations. These research design instruments include an environment that is observed and controlled by the person(s) conducting the experiment. They manipulate one or more conditions of this environment and document how other conditions in the environment will change as a consequence of the manipulation of the first one. While experiments are not so common in the field of political science, they are still utilized by some researchers and even claimed to be even more and more commonly encountered over time[37].

The second group of methods in political psychology engages with questionnaires through which a group of random or non-anonymous interviewees offers their oral or written responses to various questions. Despite the fact that the higher level of convenience and accessibility to such research designs due to budget and time constraints, as opposed to

[36] Ibid.

[37] Ronald Rogowski, "The Rise of Experimentation in Political Science," in *Emerging Trends in the Social and Behavioral Sciences*, ed. Robert A. Scott, Marlis C. Buchmann, and Stephen M. Kosslyn (New York, NY: John Wiley & Sons Inc., 2016).

experimentation, this method has some downsides underlined by the scholarly community[38]. On the one hand, the interviewee may possess some biases that will inevitably find reflection in the answers provided. Moreover, it is possible that the responders are oriented toward providing answers that will, allegedly, be satisfactory to the interviewers. On the other hand, the interviewees, their preferences and predispositions may be determined by experiences for which the survey does not account – thus producing an omitted variable that could affect the final conclusions of the study. As it was outlined previously, a significant problem with this kind of research instruments is the one related to biases and instability of the provided answers by respondents over time. Also, in accordance to the implications of the prospect theory, reviewed previously in this chapter, depending on how the surveyors asked the question, the answers may vary[39].

The third method that has its role in studying political psychology is the content analysis. This tool employs psychological techniques to understand political processes and political figures through speech and non-verbal acts. One of the caveats of using content analysis is that the materials used to record speeches and other public performances are not always reflective of the persona of the political leader that is being studied[40].

The fourth kind of research technique is observer ratings that individuals provide for politicians. The perceptions include mostly traits and other impressions that politicians leave in the observers. Similar to the other methods in political psychology this one is not without any flaws. Observer ratings usually suffer from a high level of biased responses by the observers who frequently make the fundamental attribution error. They tend to assign to the object of evaluation

[38] McDermott, *Political psychology in international relations*.

[39] John Zaller and Stanley Feldman, "A simple theory of the survey response: Answering questions versus revealing preferences," *American Journal of Political Science* 36, no. 3 (1992).

[40] Robert Jervis, "Political psychology: Some challenges and opportunities," *Political Psychology* 10, no. 3 (1989).

characteristics that they think are a product of one's personality rather than of situational factors that could change the perceptions if the object was observed throughout a more continuous amount of time[41].

A fifth possible research tool for conducting political psychology inquiries is the use of case studies – an approach very well established in the field of political science and IR. It is common that a single case study research designs are employed – through which a higher number of details is covered but at the expense of breadth of the study. As opposed to this, multiple case studies allow for a greater breadth of the research conclusions but at the cost of some depth of the analysis. McDermott advocates that case studies are used "in the early stages of a research project, when it is still unclear which aspects of a particular event or problem are important, what evidence should be sought, and which factors may play a role in explaining outcomes"[42]. However, she warns that the analysis may be vulnerable to these very same biases that are valid for other kinds of research designs. They, she underlines, should be overcome by a number of case studies that are first, more than one, and second, complemented with experiments that will prove the causation between the independent and the dependent variables.

Having in mind these insights, the current study that I conduct will be based on the following methodology. First, considering the subject matter, it will rely on case studies rather than on other research tools since it is a new topic for the field. It also marks a theoretical contribution that has not been explored to a sufficient extent and aims to achieve at this point of the political psychology research agenda a certain breadth rather than depth. Regardless, the number of case studies that will be greater than one will provide some depth of the implications.

[41] Lee Ross, "The Intuitive Psychologist And His Shortcomings: Distortions in the Attribution Process," in *Advances in Experimental Social Psychology*, ed. Leonard Berkowitz (New York, NY: Academic Press, 1977).
[42] McDermott, *Political psychology in international relations*, 37.

The chosen methodology also will guarantee that the hypothesis will be properly tested in various case studies whose characteristics differ.

As the individuals are main objects of analysis in this work, it is important to explain what are the elements of the human cognition, and in what ways it is vulnerable to cognitive threats by actors intending them in order to benefit politically. The following sections, informed by the study of psychology reveal that cognition is a very complex structure affected by multitude of factors whose influence vary in different social situations. Much of the ongoing processes regarding information storing and aggregation happen also unconsciously – which is why individuals may not be aware of how a particular inference was made by their cognition. In particular, they may not be aware what factors impacted their decision-making, and what subtle influence may have been exercised over them, as they allegedly conducted an independent cognitive reasoning. Moreover, the information for this reasoning may even be improperly stored by the mind as the social elements responsible for the memorization could vary, as well as the quality and the reliability of the memories themselves. Consequently, individuals may not even have a perception about the threats that actors pose to their cognition and independent decision-making. Regardless, the way human cognition operates demonstrates a certain predictability that is not a threat by itself but only if manipulated purposefully in a direction to benefit a certain political entity. To trace these predictable mechanisms of information-processing, decision-making and behavior, first, I outline the concept of cognition and explain the elements that constitute it. Then I add the role of the social environment in which human cognition is operating and its importance for the manner in which people use, produce and exchange information through verbal and non-verbal cues. In the end of this chapter, I explain how these psychological experiences shape the world of politics in which the individual is both influencing the system, and an actor being influenced by it.

What is cognition and how does it work?

The psychological literature does not offer a unanimous, commonly accepted definition for cognition. However, scholars unite around what should be understood by this term. George[43] defines it as "the way human beings *perceive* and *learn*, how they reason and think, even how they remember and imagine; and how their 'minds' work in the ordinary day-to-day activities of life"[44]. Perception, he continues, is possible through the senses of the human's body that convey some information to the brain through specific mechanisms. Many psychologists argue that the perception of information could be occurring in both conscious and unconscious state, as the latter is also referred to as a "behavioralistic" way of studying cognition, which excludes introspection as a means of inquiring about how cognitive processes work. Behavioralism is especially valuable in scientific research since humans are not capable of accounting for every step of the cognitive processes taking place in the brain, why they occur, how and what influences them[45]. In a slightly different definition about cognition, Drever[46] describes it as a term that encompasses "perceiving, imagining, remembering, conceiving, judging and reasoning" as he contrasts cognitive processes to others that are based primarily on sensations rather than on a logical chain of mental steps. As opposed to perception, deception would

[43] Frank George, *Cognition* (London: Methuen, 1962).
[44] Ibid., 11.
[45] George, *Cognition*.
[46] James Drever, *A dictionary of psychology* (Oxford, England: Penguin Books, 1952), 42.

represent an effort to stimulate the creation of a false perception about facts or events in an individual[47]. It could be involuntary but also purposeful.

In the following paragraphs, I will break down the study of cognition into different components that either compound it or have some function that is essential to cognition. The first element that is central to the study of cognition is the mind. In this section, it will be viewed not that much in the context of neuro-psychology or philosophy but rather in a psychological context that supplements some aspects of the political science focus of this work. The mind characterized as a "processor of information"[48] used to be depicted only in terms of the human's ability to perceive information, and to guide their behavior based on this information. Nowadays, with the rapid development in the Artificial Intelligence (AI) technologies, the mind and its complexity are discussed in two different types of systems: the traditional cognitive system of humans and animals (living organisms), and the cognitive apparatuses of AI creations. Garnham writes about the widespread at the time belief that "machines will never be really intelligent until they can learn"[49]. The learning process of machines and its continuous enhancement is already a fact in 2019 and not a possibility as it used to be a few decades ago, with all of the upsides and downsides that this progress entails. While not excluding AI from the study of cognition, the following sections focus on the individual's cognition and its elements.

The mind serves as the operator for cognitive processes thanks to its ability to store information and create memories and a logical chain of steps. This is accomplished through processing the perceived through the senses information (thinking), then sending signals to other parts of the body in order to trigger a certain action or abstain from such and to create

[47] Ray Hyman, "The psychology of deception," *Annual review of psychology* 40, no. 1 (1989).
[48] João Branquinho, "The foundations of cognitive science," (Oxford: Clarendon Press, 2001), xvii.
[49] Alan Garnham, *The Mind in Action: A Personal View of Cognitive Science* (London: Routledge, 1991), 86.

associations between events and notions thus stimulating a learning process and creativity. Three other factors that also contribute to the functioning of the mind and are included in this section of the chapter are also the emotions, the feelings, and the language.

Memory. The memory acts like an archive that ensures the conscious revival of old events, or at least the ones perceived as such by the brain[50]. A tremendous amount of the information that is stored and processed by the memory serves to guide human behavior. However, the memories that represent the information stored in the brain could be conscious and unconscious as they all create what is called *knowledge* but in the first case, it will be labeled as *explicit* and in the second as *implicit* knowledge. Regardless of this theoretical division, both types of memory predetermine one's behavior. It is important to be noted that memories are not an accurate and full reflection of the reality but are selective. That said, human behavior is driven by selective memories that could be both conscious or unconscious. Searching for the information that these memories represent takes very little time but still longer than it takes a computer, for instance[51]. Scientists attempted to model the human memory, and one of the first efforts in this direction was called the *modal model* – a representation that accounts for two departments in the memory. The first one is the short-term memory and the second – the long-term memory. When new information enters the cognitive branch of the human's body, it is immediately stored in the short-term department, and if it is considered that it has to be memorized for longer periods of time, then the information is transferred to the long-term memory section. Because human memories are selective and everyday life requires a significant amount of information in order to ensure proper decision-making, cognitive science considers the importance of some supplemental materials. Notes, diaries and other written and non-visual

[50] Ibid.
[51] Ibid.

tools that could construct an individual's perception of past and present events reflecting the reality, as the individual sees it, serve as an external memory storage.

Atkinson and Shiffrin[52] add one more department to the memory map that other scholars use, called a *sensory register*. This department contains short-lived memories that store information collected through sensory organs – for instance, scholars identify the iconic store of the human memory that represents the capabilities for recalling a written content. Another part of the sensory store is the echoic store that preserves for a short amount of time memories about speech[53].

Another distinction of the memory types is the one that focuses on the nature of the memories created[54]. Based on this, the memory could be episodic and semantic. The first kind represents memories that are related to the recipient of the information and have a distinctly autobiographical character. The semantic memory, on the other hand, contains information about the world that is not so closely pertaining to the recipient. This discrepancy also serves as an answer to the question of why some memories are brighter than others. Wagenaar[55] emphasizes that it is the emotional element in both kinds of memories that makes them so durable over time. Eysenck and Keane[56] label these memories as "self-reference" memories and "flashbulb" memories. While both carry some symbolic value to the owner of the memories, the self-reference memories are important for the individual because they store information directly

[52] Richard C. Atkinson, and Richard M. Shiffrin, "Human memory: A proposed system and its control processes.," in *Psychology of Learning and Motivation* ed. Kenneth W. Spence, and Janet Taylor Spence (London: Academic Press, 1968), 14.
[53] Michael W. Eysenck and Mark T. Keane, *Cognitive psychology: A student's handbook*, 3 ed. (Hillsdale, NJ, US: Larence Erlbaum Associates Ltd. Publishers, 1995).
[54] Endel Tulving, "Episodic and semantic memory," in *Organization of memory*, ed. Endel Tulving and Wayne Donaldson (London: Academic Press, 1972).
[55] Willem A. Wagenaar, "My memory: A study of autobiographical memory over six years," *Cognitive psychology* 18, no. 2 (1986).
[56] Eysenck and Keane, *Cognitive psychology: A student's handbook*, 186.

pertaining to them. Contrary to this, the flashbulb memories embody information about publicly relevant events with a significant value to society in general.

Emotions. The emotions' main function is to produce accurate body and brain responses to changes in the environment or within the organism. In other words, they represent coping mechanisms for survival. A vital part in these coping mechanisms are the emotions that together with the feelings have a crucial role for reasoning and decision-making. The nature of these responses to the changing environment could be mental or entirely physical. While there are cultural reasons that could affect the occurrence of emotions, they still could be defined as "chemical and neural responses, forming a pattern…(that) have some kind of regulatory role to play, leading in one way or another to the creation of circumstances advantageous to the organism exhibiting the phenomenon"[57]. The emotions that trigger a certain reaction after signals were sent to the brain could be divided into three main groups: primary, secondary and "background" emotions[58]. The primary emotions are an immediate result of an existing phenomenon, the secondary emotions (guilt, pride, embarrassment), also called *social* are chemical and neural reactions that occur after a primary emotion has already taken place. Some authors attribute the existence of secondary emotions to representatives of in-groups as opposed to lack of such when it comes to individuals from an out-group[59]. As for the *background emotions* (e.g., love, wellbeing, affection, etc.), it could be said that they are much less researched and difficult to be described as they "refer to the contour of affect as it is played out in time"[60]. These emotions could be conscious or unconscious, and they drive one's behavior in a

[57] Antonio R. Damasio, "Reflections on the neurobiology of emotion and feeling," in *The foundations of cognitive science*, ed. João Branquinho (Oxford: Clarendon Press, 2001), 102.

[58] Ibid.

[59] Jacques-Philippe Leyens et al., "The emotional side of prejudice: The attribution of secondary emotions to ingroups and outgroups," *Personality and social psychology review* 4, no. 2 (2000).

[60] Ruth Feldman, "On the origins of background emotions: From affect synchrony to symbolic expression," *Emotion* 7, no. 3 (2007): 601.

very subtle way[61]. The relationship between emotions and cognition could be mapped in three consecutive steps. First, an evaluation of the change in the environment or within the organism, second, adjusting the body to respond to these changes, and third, the occurrence of a feeling[62].

Feeling. As a part of the emotions, feelings are described in the literature as a perceived state of the body and the mind at a time at which the brain is processing certain thoughts. A logical question following the definition of *feelings* would be how they differ from emotions, despite their obvious similarities. Feelings are a component of emotions whose ultimate goal is delivering a *report* about the state of the body and the mind to the brain. The emotions, on the other hand, are a preliminary step to the feeling making it possible by sending signals to the brain in an effort the latter to adjust the body according to changes in the environment and within the organism. In other words, emotions could be conceptualized as a process that captures external elements and internalizes them, while feelings are an entirely internal process that provides information about the body and the mind to another organ - the brain.

Thinking. As evident from the definition provided previously, cognition has a lot to do with thinking. The latter, according to some researchers[63], is built on a perceptual mechanism, called *categorizing behavior* that: 1) is intended to simplify the multitude of conditions in the surrounding environment, 2) enhances processes of identification, 3) sends signals to the brain for a required action, 4) shortens the learning process, and 5) captures the common pattern between different events from life. All of these functions demonstrate the need of the human's cognition to make generalizations possible in a quick, easy way in order to ensure efficiency.

[61] Martha C. Nussbaum, *Upheavals of thought: The intelligence of emotions* (New York: Cambridge University Press, 2003).
[62] Damasio, "Reflections on the neurobiology of emotion and feeling."
[63] Jerome S. Bruner, Jacqueline J. Goodnow, and George A. Austin, *A study of thinking* (New York: John Wiley, 1956), 8.

Other psychologists call these generalizations *mental models* that reflect on perceptions about the world while at the same time they allow for alterations following the ever-changing circumstances so that they help the brain with problem-solving[64].

Thinking as an information handling process is indeed mostly intended for problem-solving which is best accomplished through concepts. They incorporate a specific set of common elements across material objects or notions. Creating this mental pool called *concepts* helps the brain and the body to react to the same phenomena similarly since they fall into one perceptual group. Davidson[65] claims that it is a matter of assessment and beliefs that help the individual classify objects and other non-material phenomena into concepts. These two mental processes could be shaped by physical experiences but also by cultural norms and beliefs. An essential part of the thinking – the reasoning mechanism - is an object of study by researchers as they try to find what elements could be an obstacle to this activity. Garnham[66] lists three situations in which the construction of mental models could be obscured. In the first case, thinking is related to a desired abstract mapping of a phenomenon and the concepts that the cognition uses are built on specific circumstances rather than on general. In the second case, the mental-modeling is related to instances in which memories stored in the long-term cognitive branch are needed, and some of them cannot be retrieved or there are no experiences that created them. Thus the necessary information from the memory is missing. The last problem that can occur when using mental models for reasoning is that people tend to simplify the models and use one single model rather than multiple models that could embed applicable information for the decision-making.

[64] Garnham, *The Mind in Action: A Personal View of Cognitive Science*.
[65] Donald Davidson, "What thought requires," in *The foundations of cognitive science*, ed. João Branquinho (Oxford: Clarendon Press, 2001).
[66] Garnham, *The Mind in Action: A Personal View of Cognitive Science*.

Another aspect of thinking refers to emotions and how they alter the perception of information. The *network theory*[67] suggests that when an individual is under the influence of a particular type of emotion, positive or negative, they are more likely to trigger thoughts of the same nuance. For instance, positive attitude brings associations of other happy events, negative attitude – of negative events. In addition to this, while there is no categorical proof from studies confirming the tendency of the negative memory bias in individuals who suffer from depression and/or anxiety, scholars predominantly support the notion that in according to this bias, "negative or threatening information is recalled relatively better than positive or neutral information"[68]. Series of studies by Eysenck and his colleagues[69] [70] [71] confirmed the existence of an interpretive bias, stating that people with anxiety are more likely to perceive some signals of unclear nature as threatening.

An intriguing question is also how people problem-solve and make judgments when they do not have enough information. A classical study by Tversky and Kahneman[72] exploring heuristics and biases poses three factors influencing decision-making processes. First, the decision-maker assigns the object a place in a particular group that will help classifying it and simultaneously transfer other characteristics from the group to the object. Second, the number of scenarios and situations to which the decision-maker can relate determines the frequency or likelihood of an imagined event happening. Third, the starting point from which predictions are made is also of importance during decision-making. Complementary to these findings are the

[67] Gordon H. Bower, "Mood and memory," *American psychologist* 36, no. 2 (1981).
[68] Eysenck and Keane, *Cognitive psychology: A student's handbook*, 449.
[69] Michael W. Eysenck, Colin MacLeod, and Andrew Mathews, "Cognitive functioning and anxiety," *Psychological research* 49, no. 2-3 (1987).
[70] Michael W. Eysenck, *Anxiety: The cognitive perspective* (Hove, UK: Lawrence Erlbaum Associates Ltd. Publishers, 1992).
[71] Michael W. Eysenck et al., "Bias in interpretation of ambiguous sentences related to threat in anxiety," *Journal of abnormal psychology* 100, no. 2 (1991).
[72] Amos Tversky and Daniel Kahneman, "Judgment under Uncertainty: Heuristics and Biases," *Science* 185 (1974).

ones refuting the expected utility theory and substituting it with one called *prospect theory*[73]. According to it, people seek to avoid risks when the choice involves guaranteed gains and take risks when one of the choices likely involves certain losses. In addition, Kahneman and Tversky outline that it matters greatly how the choice is presented to the social perceivers because their final decisions, based on gains and losses, may be predetermined by how the question is asked.

Creativity. Another question that deserves attention when discussing thinking is the one about creativity. Mainly, the issue that I want to address in this section is what is creative thinking, and to what extent it follows the same rules that are valid for thinking in general. Scholars overall agree on the fact that creative thinking does not differ substantially from the conventional thinking that constructs mental models and utilizes them in decision-making. When it comes to a precise definition of creative thinking, however, such is lacking in the scholarship on cognition. Responsible for this is the complex idea of *creative thinking* that will largely depend on specific circumstances that will distinguish a regular idea from a creative one. Once the creative idea becomes part of the mental model, future solutions of problems will become less creative since the creative idea has entered a social realm of realistic and applicable concepts. This is possible thanks to existing information that could have been previously considered inapplicable to the problem at hand that was later validated by the creation of a new, adjusted mental model[74]. Other scholars categorize creative thinking as a result of cognitive processes of association and analogy-making[75], as the latter constitutes "mapping of the

[73] Daniel Kahneman and Amos Tversky, "Prospect Theory: An Analysis of Decision under Risk," *Econometrica* 47, no. 2 (1979).
[74] Garnham, *The Mind in Action: A Personal View of Cognitive Science*.
[75] Margaret A. Boden, "Précis of the creative mind: Myths and mechanisms," *Behavioral and brain sciences* 17, no. 3 (1994).

conceptual structure of one set of ideas (called a base domain) into another set of ideas (called a target domain)”[76].

Learning. One part of people’s cognitive functions is developed already when a baby is born, but the vast majority of their cognitive skills humans acquire later through learning. A very long and vivid debate about the nature of the learning process is one of the core topics in psychology and philosophy, whose beginning dates back to works by René Descartes and Immanuel Kant and still continues in the present. The debate offers two opposing conceptualizations of how people learn. Rationalists maintain that learning is occurring not through experience but rather through mechanisms that are already in existence in the human body. Contrary to this view is the one held by empiricists who claim that the learning process is made possible by experiences that help the brain construct links (called associations) between the obtained through senses information, grouped into concepts. The repetition of experiences involving similar circumstances leads to a more manageable process of categorizing information and building faster both cognitive concepts and the associations between them[77]. Both schools of thought are encountering series of questions that their theory is not capable of addressing and to this day, neither perspective could be considered more prevalent in the field.

While sharing some similarities, it is important to distinguish between knowledge and learning, as the latter represents a process and the former – the result of this process. As for how thinking is different than learning they relate to each other in the following way. In order learning to take place, thinking has to be present first. However, with the speed with which human cognition is working, a lot of these processes and the results from them would seem almost simultaneously occurring.

[76] Eysenck and Keane, *Cognitive psychology: A student's handbook*, 393-94.
[77] Garnham, *The Mind in Action: A Personal View of Cognitive Science*.

Language. One definition of language poses that it is “a cognitive ability that depends on a store of specialized information in long-term memory – information specifically about language”[78]. This does not mean, however, that non-language-specific knowledge is not used in utilizing the language skills. A controversial issue in cognitive science that has not yet been answered is the one asking the question about the extent of language-specific information stored in the brain and at what point does it mix with non-language-specific information. An insight with which both psychologists and linguists agree is that languages are means of exchanging information between individuals that presupposes two conditions. The first one is that the person conveying information can efficiently express their thought in verbal or written form. The second condition relates to the recipient’s ability to understand the information that is being conveyed to them thanks to a “mental lexicon”[79] where words are being searched. An area, regarding the question of language, in which scholars tend to disagree with each other is if the language is used independently to convey certain information to the recipient or the message is inevitably influenced by some linguistic specificities.

Rationality. The concept of rationality is discussed in this essay not only because it has a significant meaning for the study of cognition in psychology and thus is a topic of a major debate, but furthermore, rationality is a building block in political science, economics, modeling and simulation, and other fields. Every science defines rationality slightly different as the goals that these sciences pursue are not the same, though they are sometimes similar. For the purposes of this work, I will focus first on its meaning for the study of cognition and will transition to the implications that psychology provides for the same topic but situated in a political science context.

[78] Ibid., 56.
[79] Ibid., 58.

The foundations of rationality in psychology are laid by the *Classical Model* that states that rationality is present when desires and beliefs drive actions. These two elements constitute reasons for controlled by desires actions[80]. More recent works dedicated to this problem do not see desire and belief as the only factors that engender a certain behavior. Instead, they propose a desire-independent model based on judgment rather than on desires and beliefs[81] [82] [83]. Other scholars, such as Harvey Siegel[84] connect both the assumptions of the Classical Model in terms of desires and beliefs to judgment.

The same debate about rationality in the field of political science has slightly different dimensions than the one in psychology. The Utility Maximization Model that political science borrows from economics underlines the importance of achieving results that will benefit the individual the most and thus the behavior is oriented toward achieving these goals. Very frequently in discussions about foreign policy, political rivals whose goals are different than the ones of the discussants are labeled as *irrational* simply because of a misunderstanding of their goals, desires and beliefs and often the ethnocentric thinking of the decision-makers[85]. For instance, Simon[86] argues that even selfish or altruistic behavior does not make an individual's thinking more or less rational. Furthermore, he claims that the rationality of the behavior should be assessed based on the connection between desires, beliefs, judgment, cultural norms and the goal that is intended, because access to information is always imperfect and the individual's thinking will only consider the amount of information that they have available. This and other

[80] John R. Searle, "Rationality and Action," in *The Foundations of Cognitive Science*, ed. João Branquinho (Oxford: Clarendon Press, 2001).
[81] Ibid.
[82] Harold I. Brown, *Problems of philosophy: Their past and present. Rationality.* (New York: Routledge, 1988).
[83] Trudy Govier, *The Philosophy of Argument* (Newport News, VA: Vale Press, 1999).
[84] Harvey Siegel, "Rationality and judgment," *Metaphilosophy* 35, no. 5 (2004).
[85] Ken Booth, *Strategy and Ethnocentrism* (New York: Routledge, 2014).
[86] Herbert A. Simon, "Rationality in political behavior," *Political psychology* (1995).

reasons make Simon[87] conclude that an applicable simplified model of costs-and-benefits deliberations relevant in a large number of cases would be inevitably flawed without the necessary empirical research that accounts for all the elements that are present in a certain cognitive process for decision-making. Recent innovations in neuroscience suggest that instead of the rationality-bound theories that political scientists use to explain political behavior it is also the emotions that carry significant meaning for the decision-making and actions, especially risk-taking[88].

Action. It is also important to explore the relationship between cognitive functions and actions in their two forms: physical actions and actions that are entirely verbal in nature. For both types, it is valid that the brain has to send some signals to the muscles in order to perform an action, even if only verbal. Learning a physical skill such as a particular activity differs from cognitive tasks as memorizing, for instance. While they both have a particular action as a goal, they require different kind of knowledge to execute the function. The first kind of knowledge that is needed in order for an individual to acquire physical skills and perform physical actions is called procedural knowledge, and the second type – declarative knowledge[89]. An interesting question in the field of cognitive science is whether the procedural knowledge helps the individual to execute specific tasks better with repetition of these acts, having in mind the results from previous attempts. Scholars claim that while it is possible, this is not necessarily a rule because people cannot control physical functions entirely. At the same time, repetitive performance could help the individual become better but thanks to unconscious processes that

[87] "Human nature in politics: The dialogue of psychology with political science," *American Political Science Review* 79, no. 2 (1985).
[88] Rose McDermott, "The feeling of rationality: The meaning of neuroscientific advances for political science," *Perspectives on politics* 2, no. 4 (2004).
[89] Garnham, *The Mind in Action: A Personal View of Cognitive Science*.

provide “sensory feedback to the body”[90]. To define the link between actions and cognition, another component also should be taken into consideration - how the cognition *orders* actions. Mental reasons that people have to make verbal or physical acts should be distinguished from the causes of these actions. While they could match in ideal cases, reasons for actions and causes of actions could be quite different in practice. Sometimes, when actions are undertaken without a logical explanation, it is likely that the individual who committed the act tries to reconstruct the event that happened and to rationalize their actions so that they correspond with the event[91].

Social cognition

In the current section, I will explain how the main elements from the human cognition are affected when another component is considered – the social one. No cognition exists in a vacuum. It is always influenced by the interaction between people, or the thinking of other individuals. It has an important meaning for politics mainly regarding the construction of identity, social networks, exchange of information (and disinformation), and the perception of social events and facts delivered to the recipient by a secondary source. Since these factors are important to politics, they frequently become targets of actors intending to score political gains by exploiting feelings of fear, anger, empathy, pain, trauma, shame, and habits.

The scientific field studying the social context of cognition is called social psychology. While cognition provides the scholarship with important insights about how human’s mind is wired and what processes determine attitudes and behaviors, social cognition, a branch from social psychology, focuses on *social conventions, rules and norms* as people are social creatures

[90] Ibid., 103.
[91] Ibid.

influenced by the environment in which they live[92]. The social component plays an important role in understanding attitudes and behaviors and, though separate from the study of cognition it is nevertheless intertwined with it. Thus, psychologists label the research dedicated on cognitive processes influenced by social factors as *social cognition*, a category interested in “how people make sense of other people and themselves”[93]. A more detailed definition by Hamilton[94] emphasizes that social cognition constitutes “a consideration of all factors influencing the acquisition, representation, and retrieval of person information, as well as the relationship of these processes to judgments made by the perceiver”. Both explanations of the term incorporate many different categories including the study of social interactions, perception, and processing of information, stereotyping, leadership and other branches. For the purposes of this chapter, I will focus only on 1) attribution; 2) control and behavior; and 3) social judgments and stereotypes.

Attribution. A central element in the field of social cognition is how the recipient of information forms causal relationships between the information that was presented to them and different phenomena from social life. This research question gave birth to the *attribution theory*. The latter seeks to explain what factors contribute to a chain of logical thinking that connects a certain event in the social environment to its cause. Constructing inferences about social events and attributes of other people is possible through analyses that the recipient of information creates, in order to make sense of the surrounding environment and to better adjust themselves to it.

[92] Ibid., 117.

[93] Susan T. Fiske and Shelley E. Taylor, *Social cognition* (Reading, MA: Addison-Wesley Publishing Company, 1984), 12.

[94] David L. Hamilton, "Cognitive representations of persons" (paper presented at the Social cognition: The Ontario Symposium, Ontario, CA, 1981), 136.

Emotions, feelings, judgments, and perception to a large extent shape reactions in a social setting. For instance, when emotions are concerned, a preliminary step to experiencing them is arousal that should be accompanied by an acknowledgment (cognition) that categorizes it and sends the necessary signals to the brain. However, as Bargh[95] reminds, *awareness of the stimulus* is different than the *awareness of its influence*. In this regard, a study by Schachter[96] concluded that in order to adapt better to an upcoming phenomenon that brings negative emotions to a person, one seeks the company of other people who also expect a stressful event in their life. The explanation that Schachter gave was that people tend to affiliate with others experiencing similar stressors to adjust to the event better by enriching the knowledge they have about it so that they can form appropriate reactions to it. A further study by Schachter and Singer[97] highlighted another finding: when lacking information about the cause of the arousal, people could attribute it to different factors as that could result in a positive or negative mood depending on interaction with a person in a positive or in a negative mood, respectively. The test of Schachter's theory of emotional lability has its limits, however. Scientists tried over time to determine if a lack of information about one's arousal can lead to positive, negative or neutral moods depending on exposure to social influences of different kind. For instance, Maslach[98], and Marshall and Zimbardo[99] emphasize that the lack of information about arousal leads to a negative mood rather than to a positive one. Regardless of the variations in the exact results of the study of this theory,

[95] John A. Bargh, "The four horsemen of automaticity: Awareness, intention, efficiency, and control in social cognition," in *Handbook of social cognition*, ed. Robert S. Wyer Jr, and Thomas K. Srull, Basic Processes (New York: Psychology Press, 1994), 11.

[96] Stanley Schacter, "The psychology of affiliation: Experimental studies of the sources of gregariousness," (Stanford, CA: Stanford University Press, 1959).

[97] Stanley Schachter and Jerome Singer, "Cognitive, social, and physiological determinants of emotional state," *Psychological review* 69, no. 5 (1962).

[98] Christina Maslach, "Negative Emotional Biasing of Unexplained Arousal," *Journal of Personality and Social Psychology* 37, no. 6 (1979).

[99] Gary D. Marshall and Philip G. Zimbardo, "Affective consequences of inadequately explained physiological arousal," ibid.

it could be inferred that social influence has a vital role in a state of no information about phenomena that evoke arousal in the recipient. Furthermore, without social influence providing attribution cues for the recipient of this information, as Maslach and Marshal and Zimbardo conclude, it is more likely that the lack of information will entail anxiety and frustration.

While some studies about attribution focus on an ideal situation where people use the normative cognitive process that interprets social cues logically and unbiasedly, other studies underline more practical conditions that take into consideration that some perceivers' cognitive process may be disrupted due to disabilities or individual factors. An example that illustrates the second type is what is known in the social psychology as the *fundamental attribution error*, according to which people tend to "attribute other people's behavior to his or her own dispositional qualities, rather than to situational factors"[100]. People see other people's behavior frequently as objective and not influenced by situational norms and conditions but instead as a stable pattern of qualities and personality traits. In addition to these findings, studies exploring defensive attributions emphasize that observers ascribe much higher responsibility to people whose behavior caused incidents of substantial significance than to those whose behavior inflicted less significant consequences[101] [102] [103]. While this finding has not remained unchallenged, Shaver[104] [105] accepts that individual and situational characteristics matter a lot and can cause variations across studies. However, he accentuates on the fact that the greater the

[100] Fiske and Taylor, *Social cognition*, 72.

[101] Kelly G. Shaver, "Defensive attribution: Effects of severity and relevance on the responsibility assigned for an accident," *Journal of Personality and Social Psychology* 14, no. 2 (1970).

[102] "Redress and conscientiousness in the attribution of responsibility for accidents," *Journal of Experimental Social Psychology* 6, no. 1 (1970).

[103] Elaine Walster, "Assignment of responsibility for an accident," *Journal of personality and social psychology* 3, no. 1 (1966).

[104] Shaver, "Defensive attribution: Effects of severity and relevance on the responsibility assigned for an accident."

[105] "Redress and conscientiousness in the attribution of responsibility for accidents."

similarity between the observer and the perpetrator and the situational factors, the higher the likelihood of the observer becoming defensive to the behavior of the perpetrator.

Another bias that can distort a normative inference-making process pertains to the consensus information – the opinions and beliefs of other people. The social perceiver tends to conceptualize the consensus information not as what other people actually think but what the perceiver considers to be the case. By doing so, the social perceiver attributes a large number of their own values and beliefs to others thus thinking that the consensus information is much more similar to the social perceiver's own views[106] - a phenomenon also known as the false *consensus effect*[107]. Hence, social perceivers tend to accept that others share their beliefs even if they do not know if this is not necessarily the case[108]. The self-serving bias, on the other hand, makes the social perceiver more likely to attribute success, as an outcome, to their own behavior rather than to acknowledge responsibility in cases of failure. The explanation could refer to the ego-boosting tendency of people in addition to cognitive mechanisms that perceive expected outcome as a consequence from one's efforts in this regard. It is important to be noted also that in cases in which people assume responsibility for a failure, people tend to attribute it to conditions that they can control in further attempts[109]. The self-centered bias, inherent for one's social cognition explains why individuals are more likely to assume responsibility for positive and negative outcomes of a collective work. First, human cognition has the ability to remember much more information pertaining to one's own actions, as opposed to actions of others. Second, the

[106] Fiske and Taylor, *Social cognition*.
[107] Joachim Krueger and Russell W. Clement, "The truly false consensus effect: An ineradicable and egocentric bias in social perception," *Journal of personality and social psychology* 67, no. 4 (1994).
[108] Brian Mullen and George R. Goethals, "Social projection, actual consensus and valence," *British Journal of Social Psychology* 29, no. 3 (1990).
[109] Bernard Weiner et al., "Perceiving the causes of success and failure," in *Attribution: Perceiving the Causes of Behavior*, ed. Edward E Jones, et al. (Morristown, N.J.: General Learning Press, 1972).

possibility that one has done more amount of work, regardless of the outcome, could be quite flattering for the self-esteem.

Control and behavior. A central function of the social cognition is constructing causality, as it was highlighted previously. In order for this process to happen, the social perceiver has to assume that the observed behavior is a product of controlled mental and physical activity[110]. Furthermore, if the social perceiver is not under the impression that they have control over some situation, they will be unlikely to attribute any outcome to their own behavior. Instead, they will rather ascribe the outcome to other factors that are beyond the perceiver's control. Lerner[111] for instance, claims that people have the need to believe in a just world where everything that happens to individuals is deserved. This coping mechanism is developed to protect the cognition from the stress resulting from the idea that unpleasant events happen to people who did not do anything to provoke them. A very intriguing question in this regard is what happens with the human cognition when there is a loss of control. In this case, loss of control means that the individual previously had control over some circumstances that they have lost. The four major coping mechanisms that human cognition uses to adapt to a situation, especially a threatening one on an emotional or/and physical level, are related to the need to obtain more information, the increased sensitivity to stress, the reactance, and the feelings of helplessness[112]. Usually, the first stage after a loss of control by the social perceiver is namely the search for information so that the individual forms an idea about the appropriate reaction to the event. Two of the most common consequences in this scenario are the vulnerability that the perceiver experiences to

[110] Fritz Heider, *The psychology of interpersonal relations* (New York: Wiley, 1958).
[111] Melvin J. Lerner, "The desire for justice and reactions to victims," in *Altruism and helping behavior: Social psychological studies of some antecedents and consequences*, ed. Jacqueline Macaulay and Leonard Berkowitz (New York: Academic Press, 1970).
[112] Fiske and Taylor, *Social cognition*.

social influence and the decreased amount of attention that the perceiver pays to offered information and alternative solutions when a heightened level of stress is experienced[113] [114].

A second consequence from loss of control that follows the lack of information is the increased vulnerability to stress. An increased heart rate, loss of ability to concentrate, or other adverse physiological conditions are also among the common symptoms in events that entail a loss of control in the social perceiver who is exposed to stressors.

Reactance is another phenomenon following the loss of control or a restriction pertaining to the options available to the social perceiver. It has an emotional and behavioral expression[115]. Emotionally, reactance is very similar to stress. Individuals suffer from increased adrenaline levels which frequently results in antagonistic and hostile moods that illustrate the behavioral expression of reactance. These behaviors can be followed by a pursuit to restore previous options that were available to the social perceiver. If this attempt turns out to be unsuccessful, it is very likely that the option that is no longer available becomes much more appealing than the options that were left. In other words, what was taken away attracts the social perceiver to a much higher level than what is achievable. Another possible behavioral opportunity for the social perceiver is that they commit an act of protest so that the lost freedom of the individual is, at least partially, regained.

Another component that gives its reflection on the social cognition when a loss of control is experienced is the feeling of helplessness. The latter, contrary to reactance, causes anxiety because of a lack of options available to the social perceiver. A consequence from the

[113] Harold H. Kelley, "Attribution theory in social psychology" (paper presented at the Nebraska symposium on motivation, Lincoln, NE, 1967).

[114] Irving L. Janis and Leon Mann, *Decision making: A psychological analysis of conflict, choice, and commitment* (New York: Free Press, 1977).

[115] Rex A. Wright and Sharon S. Brehm, "Reactance as impression management: A critical review," *Journal of Personality and Social Psychology* 42, no. 4 (1982).

helplessness condition is that the individual may cease to make efforts in a direction to regain control because they see the elements of the surrounding environment as impossible to be managed. A study by Wortman and Brehm[116] explored under what conditions reactance and helplessness will occur, having in mind that they are not mutually exclusive, and they can both be observed. They concluded that increased perceptions of control in a situation evokes reactance and then feelings of helplessness while not so strong expectations of control will merely result in helplessness.

Now that the consequences of loss of control were reviewed, I would like to highlight what are some of the strategies for reducing the anxiety that the loss of control triggers. Probably the most effective technique for behavior control is the perceived sense of control that the social perceiver can construct[117]. It is especially useful when it occurs before the stressful event manifests itself in reality[118] [119]. Another stress-reducing strategy is cognitive control. It consists either of reorientation of one's attention to thoughts that are not related to the anticipated event that may entail a loss of control or of adjusting how one thinks about the event. These strategies have been proven successful for situations before, during and after situations connected to a loss of control[120] [121] [122]. A third strategy is decision control. This technique suggests that the social perceiver awaiting a stressful event should make some decisions about it (its length, duration,

[116] Camille B. Wortman and Jack W. Brehm, "Responses to Uncontrollable Outcomes," in *Advances in experimental social psychology*, ed. Leonard Berkowitz (New York: Academic Press, 1975).
[117] Fiske and Taylor, *Social cognition*.
[118] Ezra Stotland and Arthur L. Blumenthal, "The reduction of anxiety as a result of the expectation of making a choice," *Canadian Journal of Psychology/Revue canadienne de psychologie* 18, no. 2 (1964).
[119] Jack A. Szpiler and Seymour Epstein, "Availability of an avoidance response as related to autonomic arousal," *Journal of Abnormal Psychology* 85, no. 1 (1976).
[120] David S. Holmes and B. Kent Houston, "Effectiveness of situation redefinition and affective isolation in coping with stress," *Journal of Personality and Social psychology* 29, no. 2 (1974).
[121] B. Kent Houston, "Dispositional anxiety and the effectiveness of cognitive strategies in stressful laboratory and classroom situations," in *Stress and anxiety*, ed. C D Spielberg and Irwin G Sarason (New York: Wiley, 1977).
[122] Michel Girodo and Douglas Wood, "Talking yourself out of pain: The importance of believing that you can," *Cognitive Therapy and Research* 3, no. 1 (1979).

and/or conditions) so that some of the control is regained and potential adverse outcomes of the event are seen as not so detrimental once a certain choice is made[123]. Naturally, the sense of control that the individual regains could be illusory, but this does not affect the ultimate quality of the decision control strategy even if the sense of control was not real. Information control, as obtaining more information about the exact dimensions of the future stressor bolsters the sense of control in the recipient of the information. In particular, information about how the event will affect the social perceiver serves as a mechanism to adjust both the body and the cognition to consequences from the event. Research shows convincing support that this type of technique alleviates stress caused by upcoming negative events[124]. However, it should be kept in mind that according to the concept of *premature cognitive commitment*[125], it is difficult for a recipient of information to use it for different purposes once it was presented to them and thus stored in the human's brain with a particular goal.

Social judgments and stereotypes. When it comes to social judgments, while the process of attribution and causality generally looks the same for all cognitively developed individuals who reached a mature age, it can still vary across people. This could be due to personal characteristics, different values they hold and belonging to a particular culture that reflects on the way social judgments are made[126]. In addition, social perceivers select information for the social judgment in various ways. It is typical that the individual focuses on a certain amount of information about other people and events thus excluding other types of information that pertain

[123] Charles A. Kiesler, Barry A. Collins, and Norman Miller, *Attitude Change: A Critical Analysis of Theoretical Approaches* (New York: Wiley, 1969).

[124] Jean E. Johnson, "Psychological interventions and coping with surgery," in *Handbook of Psychology and Health*, ed. Andrew Baum, Shelley E. Taylor, and Jerome E. Singer (Hillsdale, NJ: Erlbaum, 1984).

[125] Benzion Chanowitz and Ellen J. Langer, "Premature cognitive commitment," *Journal of Personality and Social Psychology* 41, no. 6 (1981).

[126] Daniel M. Wegner and Robin R. Vallacher, *Implicit psychology: An introduction to social cognition* (New York: Oxford University Press, 1977).

to the social perception. The focus of the information selected by the recipient should help them explain behaviors and occurrences. A study by Dornbusch, Hastorf, Richardson, Muzzy, and Vreeland[127] found that for the selection of information, the perceiver's personality matters more than the one of the perceived individual. The perceiver seeks to identify a unique set of categories for which they search in a person. Wegner[128] labels these groups of information as "general attributes", while "specific attributes", he defines, as a particular type of information that carries a certain meaning to a specific person. In addition to individual characteristics, another factor that influences the social judgment involves situational elements. The latter could not only determine the type of information that is collected but also its amount. For instance, a research project conducted by Vallacher[129] highlighted that self-consciousness about being observed makes the observer more likely to use categorical judgments. Contrary to this, observers who were not self-conscious about being observed, demonstrated a wider range of judgments on the scale between the two categorical judgments made by the other group of participants in the experiment who were self-conscious. On a more general level, these findings point to the following conclusion: the more attention is directed to the social perceiver, of which they are aware, the more limited the collection of information about the social setting becomes.

Complementary to this contribution is the one that was reached through a series of experiments: in making judgments, social perceivers tend to assign much more importance on negative rather than on positive impressions[130]. Thus, in building an impression about a person, it

[127] Sanford M. Dornbusch et al., "The perceiver and the perceived: Their relative influence on the categories of interpersonal cognition," *Journal of Personality and Social Psychology* 1, no. 5 (1965).

[128] Daniel M. Wegner, "Attribute generality: The development and articulation of attributes in person perception," *Journal of Research in Personality* 11, no. 3 (1977): 93.

[129] Robin R. Vallacher, "Objective self awareness and the perception of others," *Personality and Social Psychology Bulletin* 4, no. 1 (1978).

[130] David E. Kanouse and L. Reid Hanson Jr, "Negativity in evaluations," in *Attribution: Perceiving the Causes of Behavior*, ed. Edward E Jones, et al. (Morristown, N.J.: General Learning Press, 1972).

is the negative characteristics that take prevalence over the positive ones and shape the overall impression. Two explanations that try to explain this phenomenon are present in the literature: the figure-ground and vigilance explanation[131]. According to the first one, people are adjusted to see positive things in life and thus are much more impressed when something negative occurs. The second explanation accentuates on themes such as jeopardy and survival[132]. This theory seeks to explain why people are more impressed by negative rather than by positive characteristics of the social environment through the vigilance that is required of humans in order to ensure preservation and wellbeing.

When it comes to making social judgments the amount and the kind of information that the social perceiver obtains is essential. A logical question is how the information that is necessary for judgments selected. People distinguish between information that is pertaining to the decision-making process and such that is irrelevant. In order to do so, they assess the nature of the information presented to them as either rewarding or punishing, as both kinds lead to the relevance of the information for its recipient. Through the first impression, the social perceiver has either a rewarding, pleasant experience or a negative and unpleasant one, based on which they make further judgments. One of the most central elements of the impression management is physical attractiveness, as it is highly related to positive qualities such as being smart and kind. Another element that contributes a lot to forming impressions is someone's similarity or dissimilarity to the person making the judgment. The more similar the person is to the perceiver, the more positive the impression, and vice versa. This pattern inadvertently leads to a subjective evaluation that equals dissimilarity to abnormality. Moreover, there is another component that adds details to these dynamics:

[131] Wegner and Vallacher, *Implicit psychology: An introduction to social cognition*.
[132] Ibid., 145.

> “Quite often, our attitudes are based on ambiguous or conflicting evidence. On almost any issue, there is a surplus of “facts” supporting conflicting positions. Ambiguity and uncertainty, however, are psychologically uncomfortable; the individual desires unequivocal evidence regarding the correctness or validity of his opinions. Because the validity of one’s opinions often cannot be unequivocally assessed with objective evidence, the individual must judge the correctness of his attitudes by comparing them with the attitudes of others. The evidence regarding one’s attitudes, in other words, is largely social. Hence anyone who expresses an opinion contrary to that of the individual is in effect providing him with contradictory evidence. People with dissimilar attitudes thus pose a threat to the validity of our thoughts and feelings”[133].

Very commonly identified as a product of negative prejudices, stereotypes could be bearing both type of connotations – positive and negative. Prejudices represent “shared beliefs about person attributes, usually personality traits, but often also behaviours, of a group of people”[134], whereas the mechanism of stereotyping is “the process of applying a – stereotypical – judgement such as rendering these individuals interchangeable with other members of the category”[135]. Stereotypes serve as a set of norms within a particular group. The need for stereotypes in the social cognition lies in the necessity for categorizing phenomena in everyday life for the purposes of providing simplicity and easier decision-making. As a consequence, people instinctively look to identify themselves within a social formation after which they seek information about the valid norms within this group and apply these norms to their own behavior[136] [137]. The social perceiver feels a need to share the identity of the group with which they would like to associate and therefore embraces the beliefs and norms of the group itself (the in-group) and about proper reactions regarding out-groups as well. This process is described by

[133] Ibid., 153.

[134] Jacques-Philippe Leyens, Vincent Yzerbyt, and Georges Schadron, *Stereotypes and social cognition* (Thousand Oaks, CA: Sage Publications, Inc, 1994), 11.

[135] Ibid.

[136] John C. Turner, "Towards a cognitive redefinition of the social group," in *Social identity and intergroup relations*, ed. Henri Tajfel (Cambridge: Cambridge University Press, 1982).

[137] "Social categorization and the self-concept: A social cognitive theory of group behavior," in *Advances in group processes*, ed. Edward J. Lawler (Greenwich, CT: JAI Press, 1985).

Hogg and Abrams[138] as an important example of social influence exercised from the group to the individual who desires to be a member.

The aforementioned social approval is particularly impactful since researchers recognize the large role of the social perceiver's need of social approval[139]. A question that immediately surfaces when discussing social influence is the one pertaining to leadership. In a group that consists of equals, there is always someone who stands out with their unique leadership abilities. Interestingly, in a series of studies conducted by Mann[140] it was the intelligence of the leaders who constituted them as such among other group members in addition to the determination of the leader to be perceived as such. Other scholars prefer to focus, however, on more situational characteristics of leader-selection. Leavitt[141] found, for instance, that in network groups established for executing a particular task, the persons who naturally stood out as leaders were the ones who had essential functions on the chain of the communication process. In order to connect the findings from different studies, two central characteristics of leaders emerge[142]. First, the leader in a group setting will be the person who is capable of providing most rewards for the majority of the group members thus ensuring satisfaction while keeping the dissatisfaction of other group members to a minimum. It should be noted here that the more deprived the group members are from particular goods, the more the figure of the leader capable of delivering the goods becomes desired by the deprived. Simultaneously, a leader in a group will most likely become a person who benefits from holding a position of power. The leaders' behavior and their

[138] Michael A. Hogg and Dominic Abrams, *Social identifications: A social psychology of intergroup relations and group processes* (London: Routledge, 1988).
[139] Kenneth J. Gergen, *The psychology of behavior exchange*, ed. Charles A. Kiesler, Topics in Social Psychology (Oxford, England: Addison-Wesley Publishing Company, Inc., 1969).
[140] Richard D. Mann, "A review of the relationships between personality and performance in small groups," *Psychological bulletin* 56, no. 4 (1959).
[141] Harold J. Leavitt, "Some effects of certain communication patterns on group performance," *The Journal of Abnormal and Social Psychology* 46, no. 1 (1951).
[142] Gergen, *The psychology of behavior exchange*.

overall role are considered crucial for the survival of the group members. An example of this dimension is the role of the physician (healers in some cultures) as his function is to ensure preservation and wellbeing of the group[143]. Regardless of these general trends, diverse situational factors could lead to different types of people and qualities to stand out in terms of leadership. The members of a particular social group can have different necessities at a given time which calls for different qualities that they may seek in a leader. This assumption requires a less parsimonious approach in social psychology that could decrease the value of its applicability. To compensate for this, Hollander[144] [145] proposed a useful concept according to which when the leader accumulates enough benefits for the group members over time, they may deviate to some extent from this pattern without to risk losing their leadership position. In spite of this, in the long-run, the leader is still obligated to provide benefits for the group due to their role, otherwise, their influence over the group will reduce gradually.

When discussing leaders and social judgments mechanisms, one impressive phenomenon in social psychology remains to a large extent undisputed over the years – the powerful influence that the obedience to authority produces. In the seminal series of experiments by Stanley Milgram[146], the latter found that positions of authority and positions implying power are capable of exercising a tremendous amount of control over the behavior of people perceiving themselves as inferior in a social situation. In his experiments, the behavior that was required of the participants was in complete opposition to their views, but still, they obeyed the authority and strictly followed the instructions given to them – to allegedly inflict harm to another human being. This study confirmed the relationship between individuals seen as leaders, being in

[143] Ibid.

[144] Edwin Paul Hollander, "Conformity, status, and idiosyncrasy credit," *Psychological Review* 65, no. 2 (1958).

[145] *Leaders, groups, and influence* (New York, NY: Oxford University Press, 1964).

[146] Stanley Milgram, *Obedience to authority an experimental view*, 1st ed. (New York: Harper & Row, 1974).

positions of power, and followers, perceiving themselves as obeying norms, rules, and authority. The controversy surrounding the experiments also deserves some attention so that another important psychological phenomenon is also highlighted. The study resulted in emotional reactions and potential trauma that the participants suffered during the experiments and after them. The reason for this was that their moral perspectives and values were challenged by the need to obey to authority. This contrast between what one's identity consists of and what one feels obligated to do is also known as *cognitive dissonance*. It illustrates the difference between attitudes, understood as judgment patterns, and behaviors, as expressions and extensions to these judgments. When attitudes and behaviors do not overlap and are in conflict, then cognitive dissonance occurs. Two works, by Festinger alone[147] and in collaboration with Carlsmith[148] began exploring the question of how people overcome this cognitive dissonance. They concluded that people convince themselves in the rightfulness of their actions (behaviors) through altering their attitudes (internal evaluating processes) so that they avoid the discomfort of having conflicting thoughts. In Milgram's experiment, this was achieved through the firm belief that the participants were doing what they were ordered to do by the authority, rather than what they decided to do themselves.

Another central question in studying leadership behavior concerns the possible ways in which members of the group get dissatisfied by the status quo[149]. First, the need for novelty in a certain relationship that is constructed by continuously repeating dynamics. In other words, human beings need to *explore* and *discover* thus inviting boredom when these activities are not present in their life. This does not mean, however, that the group does not need consistency. On

[147] Leon Festinger, *A theory of cognitive dissonance*, vol. 2 (Palo Alto, CA: Stanford University Press, 1962).
[148] Leon Festinger and James M. Carlsmith, "Cognitive consequences of forced compliance," *Journal of Abnormal and Social Psychology* 58, no. 2 (1959).
[149] Gergen, *The psychology of behavior exchange*.

the contrary, both tendencies seem to coexist even though the exact extent to which one desires changes in the environment and wants consistency cannot be accurately measured. Second, non-conformity to the existing norms could lead to complete expulsion of the individual from the group which is not so problematic in small groups as it is in large groups. Third, the unequal distribution of goods between members of the groups and leaders, assigned by their social roles. After some time, these inequalities become commonly accepted and blend into the overall pattern of the established relationships within the group. Fourth, when certain norms within a community become stable and fixed, the members will be likely to continue obeying these norms even though the environment may be changing, as this could lead to social irrelevance of the entire group.

David Campbell[150] documents how the conditions of a changing environment, conceptualized as a threat, could act as a catalyzer for consolidating and bolstering the identity of a particular group. Paradoxically, from a social psychological perspective, the refusal to obey to an altered set of social norms that would change one's identity could lead to a marginalization of the group, in case the environment requires a changed mindset that the members of the group are not ready to embrace. A historical example of this tendency would be the emergence of the railroad in the U.S. which some people at the time rejected as potentially being disruptive due to the increased number of newcomers perceived as a threat. As a consequence, many locations were left disconnected from the route of the railroad and thus became marginalized. Moreover, members of a group may have a false perception about the changing surrounding environment due to the tendency of people to connect with like-minded individuals. Newcomb's study[151]

[150] David Campbell, *Writing security: United States foreign policy and the politics of identity* (Minneapolis, MN: University of Minnesota Press, 1992).

[151] Theodore M. Newcomb, *The acquaintance process*, The acquaintance process. (New York, NY: Holt, Rinehart & Winston, 1961), doi:10.1037/13156-000.

connects “interpersonal attraction” to “attitude similarity” between individuals. Furthermore, once a relationship is established, the people in it begin to share the same attitudes. In addition, the social networks of people consist not only of their closest friends but, instead, of a much broader range of acquaintances sharing similar beliefs and values[152].

The dual meaning of perception, emotions and actions in politics

One of the most vivid debates in the field of international studies has always been the place of the individual in the system. Some researchers, primarily realist thinkers, consider that they are merely a pawn in a grand chess game governed by the powers influencing the structure, while other scholars (constructivists, liberalists to some extent, and critical thinkers) maintain that they are more than a pawn and possess the strength to change the system and alleviate the effects of anarchy. Consequently, since the realist paradigms about the IR-world exclude to a large extent the influence of the individual as an agent, their role has not been studied much. Alexander Wendt claims that in most social scientific research there are two relationships between agent and structure that are essential and make them both interdependent: “1) human beings and their organizations are purposeful actors whose actions help reproduce or transform the society in which they live; and 2) society is made up of social relationships, which structure the interactions between these purposeful actors”[153]. Interestingly, even rational choice theorists who focus on the individual and their preferences assume that there is a cost-benefits analysis that is conducted every time a decision has to be made by an individual. Psychological theories

[152] Robert M. Milardo, "Personal Choice and Social Constraint in Close Relationships: Applications of Network Analysis," in *Friendship and Social Interaction*, ed. Valerian J. Derlega and Barbara A. Winstead (New York, NY: Springer, 1986).

[153] Alexander E. Wendt, "The agent-structure problem in international relations theory," *International organization* 41, no. 3 (1987): 337-38.

disagree with this type of modeling, as it was argued earlier. As the role of the individual becomes more and more important in a political environment where beliefs, norms, emotions, and behaviors can provoke regime overthrows, significant changes in the political apparatus and in the institutions themselves, how we study individuals in political science is a topic that enjoys a revived scholarly interest in the post-Cold War era. Jervis argues that in this political climate after the fall of the Berlin Wall, the focus of researchers should again be placed on beliefs, values, and biases that trigger reactions, attitudes and behaviors in individuals[154]. Much of this new wave of political psychology research on individuals was dedicated to leadership, leadership styles, personality traits and disorders[155] [156] [157] [158], and the literature is voluminous. While it is evident that drawing inferences about politics based on one's psychological characteristics is understandably difficult, these scholars prove that it is not impossible. A much more complex research question would be to draw political conclusions based on the individual behaviors, feelings and emotions of many people that do not qualify for the category of group thinking because they are relatively independent in their decision-making process. It is true that individuals differ greatly, but as it was outlined previously in the chapter, there are some general trends that are consistent and can allow for some generalizations. For instance, the field of marketing is quite successfully using psychology for the purposes of the discipline. Therefore, in this study, I will attempt to apply these psychological tools to situations that include groups of people that take decisions relatively independently from each other. I say relatively

[154] Robert Jervis, "Leadership, post-Cold War politics, and psychology," *Political Psychology* 15, no. 4 (1994).

[155] Jerry S. Wiggins and Aaron L. Pincus, "Personality: Structure and assessment," *Annual review of psychology* 43, no. 1 (1992).

[156] Paul T. Costa Jr. and Robert R. McCrae, "Four ways five factors are basic," *Personality and individual differences* 13, no. 6 (1992).

[157] Stephen G. Walker and Lawrence S. Falkowski, "The Operational Codes of U.S. Presidents and Secretaries of State: Motivational Foundations and Behavioral Consequences," *Political Psychology* 5, no. 2 (1984).

[158] Margaret G. Hermann, "Explaining foreign policy behavior using the personal characteristics of political leaders," *International Studies Quarterly* 24, no. 1 (1980).

independently because if individuals are part of the same society, there are some trends (norms and values) that could be influencing their decisions the same way even if the individuals do not know each other and are not in any way in communication with each other.

That said it is important to analyze now how the same type of psychological phenomena can play a dual role in the study of politics, how the individual can contribute to changing the system with their behavior, and how at the same time the individuals are part of a system that controls the maintenance of the status-quo element in their behavior.

First, I will briefly discuss the first scenario or how the system affects the individual. Structural realists argue that the system that is inevitably producing mistrust and uncertainty affects the units in this system (the states) by making them willing to cheat, and not to comply and cooperate with other units because of the anarchy. On the other hand, states consist of individuals that, according to some classical realists[159] [160] [161], possess the same characteristics as the states – the inclination to maximize benefits at the expense of moral principles, egotistic nature, seeking power. At the same time, the system has to govern the individuals and exercise some power over them. Here comes the notion of authority and its expressions in society. One crucial way that authorities can use to control individuals is through depicting the contours of their social environment. Leaving aside merely economic control that authorities have, in the field of IR, other types of control include securitizing areas of public life and altering the otherwise malleable identities of people. I use the word malleable mainly because no matter how strong a particular identity of a group is, it is still vulnerable to mostly negative connotations that power structures can ascribe to it. In this sense, Koschut underlines that "emotional expressions

[159] Thucydides, *The complete writings of Thucydides. The Peloponnesian war*.
[160] Machiavelli, *The prince*.
[161] Thomas Hobbes, *Leviathan* (New York: London & Toronto, J. M. Dent & sons, ltd.
New York, E. P. Dutton & co., 1965).

arguably represent an important link between the discursively constructed identities of subjects, on the one hand, and the power exerted through discourses, on the other hand"[162]. Building on this notion, Solomon adds that "language actively constructs identities, self-perceptions, and social relations"[163]. What makes the power of speech and non-verbal acts particularly important is that it is concealed so well that in most cases its influence is not even recognizable for the recipient of the information.

As for the second type of control that the system has over the individual, securitization is another prerogative that power structures have. Thinkers from the Copenhagen School consider that the way to securitize an issue is for the authorities to assign a place to a problem in the realm of extreme threats that require some extraordinary political measures that can find expression in different domains (military, economic, societal and environmental)[164]. As noted in this section, emotions such as fear, joy, grief, passion, hate, shame, pride, anger, sorrow can contribute both to the securitization of some issues and to the formation and the changing of one's identity. What is fascinating about these emotional states is that they are an inherent mechanism for every individual, and through them, the system affects its human parts through the elites conveying verbal and non-verbal information that will evoke these emotions in the recipients. Simultaneously, this cognitive apparatus of individuals could also be an engine for a change in the system through the opposite process – the individuals reacting to the power structures because of decision-making influenced by emotions. Examples in this regard are not lacking in the history – from emblematic revolutions to regular democratic elections. It should not be

[162] Simon Koschut et al., "Discourse and emotions in international relations," *International Studies Review* 19, no. 3 (2017): 486.
[163] Ibid., 497.
[164] Barry Buzan, Ole Wæver, and Jaap De Wilde, *Security: a new framework for analysis* (Boulder, CO: Lynne Rienner Publishers, 1998).

forgotten, however, that human emotions can also be skillfully used by politicians to achieve or try to achieve the desired outcome with political consequences by persuading social perceivers through presenting to them emotion-inducing information. Consequently, a change in the system can still be achieved by individuals but purposefully manipulated by third parties, a theme that is central in this work. The field of political science and IR pose an emphasis on emotions when it comes to outcomes with political significance. The reason for this is that not only emotions can contribute to decompose the complex process of decision-making, but some scholars[165] [166] argue that "emotion is part of rationality itself, and that the two are intimately intertwined and interconnected processes, psychologically and neurologically"[167]. Emotions help the decision-maker select relevant information for this process and, as Vogel says, appear to be "an essential foundation for at least some kind of reasoning"[168]. That said it is important to focus on how these emotions affect the individual's cognition and shape outcomes in the form of a particular behavior.

The literature focusing on this question, as mentioned previously, mostly belongs to the field of American Politics. It concerns the relationship between emotion and voting, and political behavior, and democratic processes[169]. Based on the contributions made in this area, McDermott[170] proposes ten pillars that have significant implications about the relationship that emotions have with politics. First, emotions trigger a certain reaction regarding an event that either occurred or existed in the individual's imagination in some form. Second, an individual's emotions serve as a compass to the judgments made about the expected utility in decision-

[165] McDermott, "The feeling of rationality: The meaning of neuroscientific advances for political science."
[166] Antonio R. Damasio, *Descartes' error emotion, reason, and the human brain* (New York: G.P. Putnam, 1994).
[167] McDermott, "The feeling of rationality: The meaning of neuroscientific advances for political science," 693.
[168] Gretchen Vogel, "Scientists probe feelings behind decision-making," *Science* 275, no. 5304 (1997): 1269.
[169] McDermott, "The feeling of rationality: The meaning of neuroscientific advances for political science."
[170] Ibid.

making. Third, emotions experienced by the social perceiver can influence a perceived likelihood of positive or negative outcomes. Fourth, certain emotions can make the individual more receptive to some kinds of information, which they will not be otherwise willing to consider. Fifth, mood as a collective state of the body and the mind has an important influence over perception and processing of new information, recollecting old one, and making judgments. Sixth, mood influences the recollection of past events and produce emotions that can affect the creation of new memories. Seventh, different emotions can make the individual either more inclined or more skeptical to undertake risks. Eight, forming emotions from non-verbal information decreases the time necessary for decision-making, as opposed to forming emotions based on verbal information. Ninth, while emotional cues make decision-making faster, extreme emotions can lead to biased thinking. Tenth, emotions and intuition are also related, and the former can shape the contours of the latter thus inviting a biased judgment.

Clausewitz[171] underlines in his view about the political philosophy of war that the balance between the three motivations ("passion, reason and technique"[172]) that the three leading figures in society ("the people, the government, and the military"[173]) have is crucial. It is evident from his definition that he sees people as inevitably driven by emotions. The discussion of the relationship between emotions and politics is particularly importance because, as Neta Crawford says, "institutionalization links the private and individual to the collective and political"[174]. Below, I will provide an overview of the most influential emotions that authors document in the study of politics.

[171] Carl Von Clausewitz, *On War*, trans. Michael Howard and Peter Paret (Princeton, NJ: Princeton University Press, 1976).

[172] Paul D. Williams, *Security Studies: An Introduction* (New York, NY: Routledge, 2012), 189.

[173] Ibid.

[174] Neta C. Crawford, "Institutionalizing passion in world politics: fear and empathy," *International Theory* 6, no. 3 (2014): 535.

Fear is among the emotions with the most notable impact on human cognition regarding decision-making. When a particular stimulus is perceived as a threat, a series of biochemical reactions are triggered that make the perceiver more alert and attentive to the social situation. The increased production of certain hormones, such as adrenaline and cortisol, for instance, helps the brain distinguish between threats and non-threats. After the shocking stimulus ends, the brain goes back to normal and precludes the production of hormones and sends signals to cease the state of extreme alertness. However, when the body and/or the mind are exposed to continuous stress, it becomes very difficult for them to recognize a stressor, and when the stressor is present and when it is gone. This can result in a lengthy process of being overly vigilant and overly responsive to stimuli in the surrounding environment[175]. As a consequence, this "changes what we look for, what we see, and the way we think"[176]. Fear and stress also affect how memories are comprised and recollected. In terms of the former, the way one stores a memory under fear/stress would not necessarily be accurate since the selection of information at the time of the memory production will be highly biased and limited. Moreover, the analysis of the options available and their value cannot be properly assessed under stress. In terms of the way humans recollect events stored in the memory under stress, they will most likely be effortless to retrieve because they are bright and influential for the individual.

Empathy, on the other hand, possesses opposite characteristics of experiencing fear. It is defined as "the cognitive ability to take another person's perspective…[and] to understand how and why others feel and think the way they do and the capacity to see how our behavior might be understood by another"[177]. Studies show that people are more likely to feel empathy toward

[175] Ibid.
[176] Ibid., 540.
[177] Ibid., 541.

individuals with whom they have a significant resemblance, the more similar, the more empathic they are[178]. Based on this principle, the more emphatic people feel, the more they are willing to help[179]. However, when people do not think that they have much in common with another individual, and there is even some feeling of resentment, this could give room for the emergence of another emotion – antipathy. It can even produce positive emotions stemming from someone else's negative emotions (joy from the unhappiness of a person with whom the perceiver does not feel associated). It is also apparent from the studies described above that stressors can reduce the feelings of empathy as they disrupt the normal functioning of the brain, as the empathy becomes an emotion with secondary meaning at the expense of the need to eradicate the stressor (the threat). For a deeper empathy, scholars argue, it is better if the person imagines what the others may feel, as opposed to just witnessing it. Through the mental images, the person empathizing will project their own way of feeling in an unpleasant manner that may or may not be identical with what is actually experienced by the ones in distress. It is still much more accurate and influential experience if the empathizer could vicariously experience the emotions of the ones who provoked the feelings of empathy, even if not utterly accurate[180] [181]. Antipathy and fear, as emotions, are frequently used in military doctrines and could sensibly increase the mistrust and alienation between states thus reinforcing the perception of anarchy. Therefore, it is crucial that individuals make a difference between reasonable fears and unjustified ones relying

[178] William Ickes, "Empathic accuracy," *Journal of personality* 61, no. 4 (1993).

[179] Jean Decety and Claus Lamm, "Empathy versus personal distress: Recent evidence from social neuroscience," in *The social neuroscience of empathy.*, ed. Jean Decety and William Ickes, Social neuroscience. (Cambridge, MA: MIT Press, 2009).

[180] Adam Smith, *The theory of moral sentiments* (New York, NY: Penguin, 2010).

[181] Liesbet Goubert, Kenneth D. Craig, and Ann Buysse, "Perceiving others in pain: Experimental and clinical evidence on the role of empathy," in *The social neuroscience of empathy*, ed. Jean Decety and William Ickes, Social neuroscience. (Cambridge, MA: MIT Press, 2009).

on techniques like empathy that help them identify a real threat, as opposed to one that was depicted to them as such and was most likely already institutionalized[182].

Anger. As opposed to feeling fearful, sense of anger increases the chance of the social perceiver to have positive views about the future. Another effect that anger has on people is that it “can also generate public support for war because anger leads people to be more supportive of punitive and preventive public policy choices”[183]. A group of scholars explores the effect of emotions, anger, anxiety and enthusiasm and political information seeking[184]. The findings from their study are consistent with previous research outlining that anger actually reduces significantly the information-seeking tendencies, as opposed to anxiety that encourages such behavior. According to another study[185], the latter can also downplay the role of habitual voting for a particular political party, and to orient the voter toward looking for new information, while provoking enthusiasm is correlated with party identification and reduced need for new information.

In a more politico-philosophical context, David Ost[186] shares an interesting perspective regarding anger in politics. He argues that it is not only that the power structures in society have to find an outlet for the anger of the masses, but instead, he presents anger as an integral component of power – a tool in the hands of both groups. In fact, politicians and activists “capture and channel”[187] this powerful political energy that anger produces through the figure of the enemy that is portrayed as responsible for certain issues, usually economic. Ost underlines

[182] Crawford, "Institutionalizing passion in world politics: fear and empathy."

[183] McDermott, "The feeling of rationality: The meaning of neuroscientific advances for political science," 697.

[184] Nicholas A. Valentino et al., "Is a Worried Citizen a Good Citizen? Emotions, Political Information Seeking, and Learning via the Internet," *Political Psychology* 29, no. 2 (2008).

[185] George E. Marcus, W. Russell Neuman, and Michael MacKuen, *Affective intelligence and political judgment* (Chicago: University of Chicago Press, 2000).

[186] David Ost, "Politics as the Mobilization of Anger: Emotions in Movements and in Power," *European Journal of Social Theory* 7, no. 2 (2004).

[187] Peter Lyman, "The Domestication of Anger: The Use and Abuse of Anger in Politics," ibid.: 122.

that if the politicians/political activists convincingly introduce the enemy to the public as such, their cause has a significant chance of success, as these dynamics are evident both in democratic and authoritarian societies. Lyman[188] elaborates on this view adding that it is important to look at how the power structures employ anger. In particular, how anger is transformed to support the existing order rather than to alter it. The argument he makes is that “force, moral indignation, care, silence and technique”[189] are four main ways in which anger is subjugated to serve the power structures and the status quo in terms of the order. The first element - anger is dressed by the regime as a force that obeys and complies with the rules established by the hierarchy of command incorporated in a particular structure. The method of transforming anger into force is the training that the military receives, for instance. The second element, *moral indignation* is achieved when the anger alone shifts toward a wave of anger invested into a specific cause or ideology – which is typically the political regime or other institutionalized values cherished by the regime. Third, care, as a transformation of anger should be understood as the need to protect something dear to the individual. An instance in this regard is the feeling of patriotism and duty to loved ones, groups in society and the state itself[190]. Fourth, authority requires that anger provoked by perceived injustice is silenced so that the integrity of the regime is intact. Lyman suggests as an example the denial of injury and the acceptance of unequal treatment as a technique that achieves silence as an extension of anger under the influence of the perceived as a legitimate power in a state or in a structure[191]. The fifth element from the proposed model is the technique. The bureaucratic techniques used to transform anger into non-emotionally charged outcomes through rules and norms is another way of subjugating anger to power – establishing

[188] Ibid.
[189] Ibid., 136.
[190] Ibid.
[191] Ibid., 138.

and reinforcing the existing order. An empirical study by Small and Lerner[192] investigated the relationship between anger and sadness, on the one hand, and welfare policy, on the other. They found that feelings of anger decreased intention of more generous welfare support, as opposed to feelings of sadness that increased the intention for support. The reason for this finding, they argue is that the sadness condition required an increase in "systematic thought"[193] that the anger condition did not require. Another explanation they offer about the results pertains to the stereotyping tendencies that angry people exhibit.

Pain, trauma, and shame. An overview of emotions and how they influence politics requires that another phenomenon is included in this work – trauma. Scholars agree that this is a deeply intimate and private experience that ultimately disturbs fundamental understandings of how the individual sees and perceives the world. Moreover, some scholars stress the inability to link trauma to politics because of the impossible task of expressing the feelings coming from a traumatic experience through language[194]. While these characteristics make the study of this unique phenomenon difficult, its relationship to politics is nevertheless established. One of the mechanisms through which an inherently personal experience like trauma can enter the domain of politics is through representation and transforming the personal into collective. Trauma cannot be described as emotion itself, but rather it represents various emotions that connect the individual to the community through the emotion of solidarity[195]. However, in the process of constituting the individual trauma as a collective one, it is possible that "popular representations

[192] Deborah A. Small and Jennifer S. Lerner, "Emotional Policy: Personal Sadness and Anger Shape Judgments about a Welfare Case," *Political Psychology* 29, no. 2 (2008).

[193] Ibid., 164.

[194] Emma Hutchison, "Trauma and the politics of emotions: constituting identity, security and community after the Bali bombing," *International Relations* 24, no. 1 (2010).

[195] Ibid.

of trauma tend to pave the way for political responses that define security narrowly and create contexts in which antagonistic or belligerent security policies prevail”[196].

Closely related to trauma is pain. It is described either “as a sensation or feeling”[197]. More detailed characteristics of this sensation or feeling are that it is inherently subjective and individual, it reveals more complicated characteristics than other emotions evoked by visually perceived events, it establishes a link “between elements of sensory experience and an aversive feeling state”[198], and lastly, the negative sensations related to pain are constructed through ascribing meaning to what provoked them[199]. An interesting study examining the relationship between pain and information selection found that individuals experiencing chronic pain are oriented to seeking pain-related information[200]. Another research focuses on the information seeking and the fear of pain. It showed that the higher the anxiety provoked by fear of pain, the higher the interest toward pain-related information[201]. While it comes mostly, if not entirely, from the psychological field, research dedicated on the relationship between information and pain (and other emotions) has important implications for the study of politics, especially for the field of security studies.

When discussing pain and traumatic experiences, there is another emotion that also adds value to the efforts to explore emotions’ effect on politics. Shame, as being “crucial to the process of reconciliation or the healing of wounds”[202] serves to acknowledge previous

[196] Ibid., 66.
[197] Joseph L. Cowan, *Pleasure and Pain: A Study in Philosophical Psychology*, vol. 19 (London: Macmillan, 1968).
[198] C. Richard Chapman, "Pain, perception and illusion," in *The psychology of pain*, ed. Richard A. Sternbach (New York: Raven Press, 1986), 153.
[199] Ibid.
[200] Daniel E. Schoth, Vanessa Delgado Nunes, and Christina Liossi, "Attentional bias towards pain-related information in chronic pain; a meta-analysis of visual-probe investigations," *Clinical Psychology Review* 32, no. 1 (2012).
[201] Gordon J. G. Asmundson, Jenora L. Kuperos, and G. Ron Norton, "Do patients with chronic pain selectively attend to pain-related information?: preliminary evidence for the mediating role of fear," *PAIN* 72, no. 1 (1997).
[202] Sara Ahmed, *The cultural politics of emotion* (New York: Routledge, 2004), 101.

wrongdoing. The role that shame has in constructing identity and sense of community between its members is similar to the one that trauma has. Shame is one of the most social emotions since it assumes that someone is “witnessing” the wrongdoing, a conclusion that holds true even if the individual experiencing shame and guilt is alone. An interesting feature of shame - national shame presumes feelings of love. That said, feelings of shame matter when the “witness” of the shame is someone of whom the person experiencing the shame thinks highly[203]. The same goes for national shame where the sense of pride of the citizens was harmed as a consequence of wrongdoing that they would like to compensate for – “witnessing what is shameful about the past, the nation can ‘live up to’ the ideals that secure its identity…”[204]. That said, one of the most influential findings in the literature about trauma and pain is undoubtedly the fact that the discomfort and insecurity that the individual experiences in many ways bolsters their ontological security[205].

Habit. While habits in politics and IR are not emotions, they have an important meaning about political relationships. They represent repetitive acts that include among other things emotions as well. Therefore, they will also be included in this section. Ted Hopf discusses that cognitive neurology discovered that “people regularly perceive, feel, and act before they think”[206], thus casting doubt in the predominant assumption in IR that actors act rationally, deliberately analyzing costs and benefits before making a decision. He maintains that social constructivism exaggerates the unproblematic nature of changes that the individual can bring into the system, ignoring the powerful influence that habits have. Moreover, socialization eventually

[203] Ibid., 105.
[204] Ibid., 109.
[205] Alexandria Innes and Brent Steele, "Memory, trauma and ontological security," in *Memory and Trauma in International Relations: Theories, Cases and Debates*, ed. Erica Resende and Dovile Budryte (New York: Routlege, 2013).
[206] Ted Hopf, "The logic of habit in international relations," *European journal of international relations* 16, no. 4 (2010): 539.

reaches its boundaries and gives room to the creation of habits that serve as an automated behavioral mechanism in which attitude and internal assessment of factors are almost or entirely predetermined by the habitual processes. That could be attributed to the social system that bolsters and encourages the formation and repetition of manifesting habits as they help the individual better adjust to the social environment in an easy, efficient manner. Habits, as "unintentional, unconscious, involuntary, and effortless"[207] processes governing human behavior stand in opposition to emotions that require at least some cognitive function to take place before a reaction is expressed. They are, however, still closely related and comprised of emotions as well as other things as they represent "unreflective reactions we have to the world around us: our perceptions, attitudes, emotions, and practices"[208]. One of the most central questions in the study of habits and political behavior is whether they can be broken and how. To this, Ted Hopf[209] and Wegner and Bargh[210] respond that habits can cease existing over time through a consideration about the relevance of the habit to the surrounding environment, its compliance to the norms and the rules or the lack of such. Conditions favorable for the creation and the practice of habits include situations in which there is little possibility for the social norms to be challenged and thus there is almost no need for consideration and analysis of any factors that determine behavior. Hopf[211] finds the study of habits especially relevant to topics including cooperation, security dilemma, rivalries, and security communities. All of them, according to him, can be easily explained by the existence of the habit as a phenomenon and the security dilemma, in this

[207] Ibid., 541.
[208] Ibid., 544.
[209] Ibid., 543.
[210] Daniel M. Wegner and John A. Bargh, "Control and automaticity in social life," in *The Handbook of Social Psychology, Vols. 1-2, 4th ed.* (New York, NY: McGraw-Hill, 1998).
[211] Hopf, "The logic of habit in international relations."

sense, is not a dilemma at all since the parties either see and treat each other habitually as enemies or as friends.

This chapter highlighted the cognitive construction of individuals. The known mechanisms of human cognition become a vulnerability if they are exploited purposefully for gains of the party seeking to exploit them. The way human cognition is built does not allow for any changes that could be made to prevent its exploitation. However, social cognition, an apparatus that creates and maintains certain predispositions regarding social phenomena, is much more susceptible to influence, including one in a direction to limit manipulations and deceptions. Research shows that among the psycho-emotional areas that are most vulnerable to threats, in particular, are the feelings of anxiety and fear, the sense of identity, control and behavior, and habit, as all of them are more powerful than other experiences, and are thus exploited more. All of them pertain to innate instincts for self-preservation and survival that very often overwhelmingly predict judgments and decision-making. Advances in the field of psychology, social psychology, and political psychology highlighted these patterns through numerous studies over the years and made human cognition a target for different political and corporate interests. As the research produced on this subject matter provided strong evidence for these cognitive tendencies, they began being exploited long before this. The following chapter documents how cognitive vulnerabilities and dispositions were utilized for political purposes over the different historical eras, and how similar or different they are in comparison to contemporary cognitive threats.

CHAPTER 3

HISTORY OF COGNITIVE THREATS

Chronicle of cognitive threats through the ages

The purpose of this chapter is to introduce the reader to the development of cognitive threats throughout the ages and to trace the specific components and conditions that had some meaning for their successful execution. Some tendencies inherent for previous historical epochs are preserved in present times, and others are a new phenomenon for the 21st century, as Chapter 4 will prove. In addition, examining the factors that made them possible would inform and justify a prevention strategy against cognitive threats described in detail in Chapter 5. As this chapter will demonstrate, advances in technological, political, religious and cultural aspects offer insights about the level of applicability of prevention as a strategy, in what situations it presents fruitful opportunities for countering cognitive threats, and when it is severely limited by factors that are difficult to be altered.

As being central pre-condition for knowing and influencing the enemy, very early in the history of humankind, intelligence gathering was recognized as one of the most powerful tools for achieving a military victory. In the fifth century, Sun Tzu underlined that having knowledge about the rival's plans is "the reason the enlightened prince and the wise general conquer the enemy whenever they move"[212]. He also emphasized that gaining leverage against the enemy without fighting requires elaborated skills but is however a priority[213]. The ability to obtain information from political adversaries or even allies has had many names in history: spying,

[212] Allen Dulles, *The craft of intelligence: America's legendary spy master on the fundamentals of intelligence gathering for a free world* (Guilford, CT: The Lyons Press, 2006), 1.
[213] Roger T. Ames, *Sun-Tzu: The Art of Warfare* (New York, NY: The Random House Publishing Group, 1993).

intelligence gathering, diplomacy, etc. One of them that focuses on planting a certain desired perception about reality that is typical for military settings is *reflexive control*. It originated in the 1960s and focused on the attempts of both sides of a conflict to impose reflexive control (cognitive control) over the opponent[214]. While it ultimately pursues the end goals of the aforementioned methods of obtaining information, it is described as being more ambitious in terms of how it will deliver the preferred outcome. Timothy Thomas identifies it as "a means of conveying to a partner or an opponent specially prepared information to incline him to voluntarily make the predetermined decision desired by the initiator of the action"[215]. A central element in this concept and in the others mentioned above is power. The immediate goal of intelligence-gathering and information operations is obtaining a piece of knowledge about a fact or facts and/or to change the rival's behavior. Regardless, the ultimate purpose of this process is to gain power over them. This is frequently achieved by deception and manipulation – a common characteristic in the skillset of spies[216]. Their activities could be motivated by "greed, disappointment, bruised egos, failure in promotion stakes, talents that went unrecognized, disillusionment and a desire for revenge"[217]. Needless to say, while the use of spies in intelligence operations may have decreased in the 21st century, they still exist but are now accompanied by technologies that execute the same functions thus saving money, time and resources. Moreover, the people employing these technologies are motivated very often by the same ambitions as the spies from classical antiquity to post-modern times. Besides, the

[214] Margarita Levin Jaitner and Harry Kantola, "Applying Principles of Reflexive Control in Information and Cyber Operations," *Journal of Information Warfare* 15, no. 4 (2016).

[215] Timothy Thomas, "Russia's reflexive control theory and the military," *Journal of Slavic Military Studies* 17, no. 2 (2004): 237.

[216] Brian T. W. Stewart and Samantha Newbery, *Why Spy? The Art of Intelligence* (London, UK: Hurst & Company, 2015).

[217] Ibid., 69.

technologies used to gather information in the 21st century remarkably resemble cognitive techniques that were inherent for the first spies known to human history.

Classical antiquity. The need for information, as outlined in Chapter 1 has always been among the most fundamental human necessities since it is crucial for survival. In most basic forms, the need for information was met through different types of predictions provided by sorcerers, astrologists, prophets, fortune-tellers, oracles and various rituals supposed to provide signs for the future[218]. In terms of military strategy, the need for information developed from an initial passive stance of obtaining information from prophets to active dissemination of information to the enemy intended to convince them to make a certain type of decision favorable for the former. Deception as a strategy, as opposed to simple information gathering, is a much more complex course of action. It requires a good perception of the enemy's way of thinking so that the deceiving information is processed as being truthful. Therefore, deceit presupposes good knowledge of the opponent's psyche as the latter could be delivered by traditional intelligence gathering. Perhaps one of the most well historically documented manifestations of a cognitive threat is the Trojan Horse. About the same historical period, the ancient Greek historian Xenophon stresses three types of groups that were usually trusted with intelligence gathering – outsiders, neutrals, and insiders[219]. Outsiders were typically fake deserters who infiltrated the enemy's camp, under the false pretense that they deserted, gathered information about military plans and strategy and went back to their original camp to report their findings. Another task that they used to have was disinforming the enemy in a way that the latter would find believable. The idea behind the *fake deserter* role is that the spy would otherwise be denied access to the social

[218] Dulles, *The craft of intelligence: America's legendary spy master on the fundamentals of intelligence gathering for a free world.*
[219] Frank Santi Russell, *Information gathering in classical Greece* (Ann Arbor, MI: University of Michigan Press, 1999).

group. However, through a process of assimilation to the new camp, the spy gains access to information that would be otherwise inaccessible. Similarity between people, as psychological studies show, has always been a powerful bond between members of a group that builds their identity. The assimilation, however, could have been time-consuming and intelligence was sometimes needed urgently. A solution to this problem were the neutrals and the merchants. Neutrals and merchants gained access to the desired location and social and military circles much easier than the infiltrators. The difference is that fake deserters have to be trusted that they actually abandoned their duties and sincerely joined the enemy, while for merchants and neutrals, the skepticism toward their intentions was much less due to their occupations or the lack of military background that can link them to the enemy. Moreover, merchants, in some cases, were warmly welcomed because of the need for the products and the services they were offering. Namely this characteristic was making them suitable spies that would not raise suspicion in the enemy's camp. In ancient Egypt, merchants traveling from Babylonia to Syria, and Palestine were also a very significant source of information[220]. In addition, native people in Egypt served as secret agents delivering intelligence to the pharaoh through the commander of the garrison close to which their villages were.

While Xenophon does not particularly mention the third type of spies – the insiders, it is well known that they have been one of the most valuable sources of information[221]. These so-called *agents in place* were individuals who were already members of the enemy's cohort and were delivering information to their leaders. Since no previous preparation, training or any outstanding skills were needed for this role, insiders, as opposed to outsiders, were just regular

[220] Francis Dvornik, *Origins of Intelligence Services: The Ancient Near East, Persia, Greece, Rome, Byzantium, the Arab Muslim Empires, the Mongol Empire, China, Muscovy* (New Brunswick, NJ: Rutgers University Press, 1974).
[221] Russell, *Information gathering in classical Greece*.

people who did not have to convince anyone that they belong to the social group. In terms of gender, Aristotle makes a very interesting observation. While most historical evidence from this period does not provide any clues that female spies were employed along with their male counterparts, Aristotle explicitly mentions female spies in Syracuse. The lack of sources specifying that women were assigned intelligence gathering missions, as well as men, could be attributed also to the problems related to translating some texts from ancient Greek. For instance, Plutarch uses masculine forms to refer to groups including both men and women[222]. It was mostly women who were engaged with arts, music, and tasks related to entertainment that were recruited as spies because of their access to significant events. However, it was not uncommon for women of noble origin and their servants to also act as spies reporting information about their husbands or their masters. Another kind of intelligence gathering position was the one of envoys that were officially assigned a diplomatic office in a foreign country. Among the benefits of this position was the lack of likelihood of getting exposed and imprisoned since the ambassadors were in the foreign country in an official capacity. There was also a downside to this position – the common knowledge that the attaché is reporting information to their countries made people more hesitant to share and entrust sensitive information. However, it was possible that envoys turned against their sending countries and began delivering information to the rulers of the receiving country.

The matter of who was providing intelligence was also relevant to the quality of the delivered information. First, the agents in ancient Greece reported information that they thought was important as the latter was a purely subjective judgment. Second, it was delivered in a way that represented how the recipient of the information interpreted it and understood it. Third,

[222] Ibid.

many of the spies back then were not explicitly trained to execute these tasks, therefore, “all information gatherers may not be equally capable in differentiating the pertinent from the peripheral”[223]. Soldiers, merchants, and envoys all have different perception about what information is important and how it should be interpreted in a certain context. Ancient Greek rulers and military commanders were aware of the problem and attempted to resolve it in different ways. Aeneas Tacticus suggested that the intelligence gathering should be done by men with a military background who will ensure that the essential information is distinguished from non-relevant facts that can cause confusion[224]. The quality of the delivered information was essential in missions aiming to obscure the enemy’s perception about facts or to provoke “an action beneficial to the deceiver”[225]. Demosthenes underlined the importance of the interests that different sources of information have and how they might affect the delivered information. He assumed that captives’ narratives were trustworthy evidence of the reliability of a fact because they had no longer interest in the outcome of the events[226]. Xenophon and Alexander the Great sought to resolve this issue by obtaining information for the same fact from different sources such as indigenous people, scouts, prisoners, spies, envoys, etc. Regardless of the methods employed by Xenophon, Alexander, and other Greeks at the time, deception by disinformation remained largely successful and thus frequently used as a strategy in military affairs. Another instance of successful disinformation practices in the early ages is given during the battle of Kadesh, in which the Hittite king used deception to mislead the Egyptians led by Ramesses II. Documents reveal that he “sent two Bedouins, posing as deserters, to the Pharaoh’s camp; the two agents played their role so successfully that Ramesses II readily believed their story and

[223] Ibid., 140-41.
[224] Ibid.
[225] Ibid., 216.
[226] Ibid.

pushed forward with but one division to invest Kadesh, his three remaining divisions straggling slowly behind"[227]. As opposed to the very well-developed intelligence-gathering systems in Greece and Egypt, in the early Republican period, Rome mostly relied on information shared by its allies, rather than collecting it on its own[228]. Another instance of the poor level of the Roman intelligence gathering is that in comparison to Romans, "the Persians, or the ancient Egyptians, would hardly have been taken so off guard by the sudden invasion of an enemy as were the Romans when Hannibal invaded Italy proper"[229]. There were some exceptions from this rule, however. Sertorius, a Roman general, from the early years of his early military career recognized the power of good intelligence and the efficiency of deception. As Romans were fighting the Teutons in Gaul, Sertorius, dressed in Celtic clothing, succeeded to present himself as one of the locals, and gathered valuable information for his mission. Despite this ingenious move described by Plutarch, it is also mentioned that it was very rare for Romans to adopt such deception techniques[230]. Another exception from the rule was Caesar in the Gallic campaigns in which he had to turn to some deception techniques to trick the Gauls. Caesar ordered his army to build a small camp that implied a sense of fear than such of courage, and force. The Gauls, thinking that Caesar's army was weakened both physically and mentally, took the bait and attacked only to see that they have been deceived and "fled in disarray"[231]. It is reported that Romans avoided using deception in their military and diplomatic campaigns in the beginning, but by the time of the Republic, for them, this has become a perfectly acceptable and useful tool in warfare.

[227] Dvornik, *Origins of Intelligence Services: The Ancient Near East, Persia, Greece, Rome, Byzantium, the Arab Muslim Empires, the Mongol Empire, China, Muscovy*, 12-13.
[228] Ibid.
[229] Ibid., 61.
[230] Ibid.
[231] Rose Mary Sheldon, *Intelligence Activities in Ancient Rome: Trust in the Gods But Verify* (New York, NY: Frank Cass, 2005), 129.

Accepted as a continuation of the Roman Empire, Byzantium realized that the Roman Empire's intelligence gathering weaknesses should be compensated. Among other measures that were undertaken was the establishment of corps of the agents who were carefully selected by their skills, behavior, social status. They had five years to show evidence of their abilities, and if approved by the *Master of Offices* and the emperor, they were accepted to serve for twenty-five years, after which they would retire[232]. Another tool used to gather information was through the Christian religion of some of the subjects that have fallen under the rule of the Arabs. In addition, Byzantines used natives acting as spies within the Arab territories that were recruited most often through money or other specific interests, religious reasons, or dissatisfaction by the rulers. Complementary to this, information for the people and the lands surrounding the Byzantine Empire was collected by the Office for Barbarian Affairs from merchants, envoys, and soldiers. This structure was functioning from the fifth to approximately the eleventh century[233]. Similar to other political formations at the time, in the Arab Muslim Empires, merchants, travelers, and even elder women were also recruited as spies by different rulers such as Al-Mansur, Harun Al-Rashid, and Al-Mamun. Archives document that Al-Mamun had recruited around 1,700 old women among his spies in Baghdad[234]. In the Mongol Empire, Jenghiz Khan, wanting to obtain intelligence about the Muslims used merchants as sources. He also paid careful consideration to "the enemy lands he wished to subject, trying to obtain any possible information on the military strength of the neighboring nations and on the rivalries among the members of the ruling class, which his diplomacy could exploit to weaken the adversary"[235]. In the Muscovite

[232] Dvornik, *Origins of Intelligence Services: The Ancient Near East, Persia, Greece, Rome, Byzantium, the Arab Muslim Empires, the Mongol Empire, China, Muscovy*.
[233] Ibid.
[234] Ibid.
[235] Ibid., 275.

State, similarly to the Byzantine Empire and the Arabs, Muscovites used foreign envoys as sources of information by spying on them while at the same time aiming to withhold information about their own state from the envoy.

The times of the classical antiquity fascinate with different techniques of information gathering, resembling a lot these in current times. Ancient Greece, Egypt, the Byzantine Empire, the Aram Muslim Empires, the Mongols, and the Muscovites all had some forms of postal services, developed differently. Later, with the technological developments in this regard, manipulations became much more common as the postal services gained a position of higher importance. Thus, in the Renaissance and in the early Modernism, the intelligence gathering was vulnerable to more challenges but at the same time grew into a more sophisticated system. It even developed into an institutionalized structure through the implementation of regular diplomatic missions in countries.

Renaissance and Modernism. In the ages of the Renaissance and Modernism cartography as art evolved sensibly. It became a valuable tool for planning, strategizing and execution of military campaigns. As a consequence, maps started to invite a more significant interest by enemies and their spies. People who have seen certain maps of importance and the plans made from them also attracted much attention as they were perceived as sources of valuable information. This included merchants, envoys, soldiers, their commanders, sailors, and captains of ships. Stealing these maps also became a profitable enterprise. One example is the case with the military engineers Johannes and Cornelis Elandts who threatened to hand the maps of the Dutch East India Company to commercial publishers unless they pay a significant amount of money[236]. It is documented that this was a regular practice among military engineers who had access to the valuable information that maps contained. Their skills were highly appreciated by the royals in Europe. Reports share that Lopo Homem fled Portugal to seek asylum in England where his cartographic skills amazed Queen Mary who ordered him to prepare an atlas with the newest geographical discoveries. King Louis XIV also had an appreciation for one of the most treasured sources of information and continuously sent military engineers to Italy with the mission of obtaining the plans of fortifications in Lombard. One of the most celebrated French cartographers, Nicolas de Nicolay, invited by John Dudley, Viscount Delisle went to England and mapped the location of the English ports with considerable significance. After the death of Dudley, it turned out that Nicolay was working for the French the entire time, a proof of which was the receipt documenting the payments made by the French king. Considering all these circumstances, at the time, "cartographic espionage was perceived of being of greatest practical use"[237]. Although the methods and the people involved in the process have changed, attempts to gain access to the plans illustrating locations of important buildings resemble, to a large extent, a contemporary theft of secrets that, similarly to centuries ago, both private and public parties treasure greatly.

In the Renaissance and the early Modernism, spies increasingly started to be selected based on their relationship with the person of interest, as opposed to choosing a person of skills who was unknown to the target. For instance, in England, circa 1540, among the spies employed to gather intelligence on suspected traitors of the crown were also scholars[238]. During the reign of

[236] Peter Barber, "'Procure as many as you can and send them over': Cartographic Espionage and Cartographic Gifts in International Relations, 1460–1760," in *Diplomacy and Early Modern Culture*, ed. Robyn Adams and Rosanna Cox (New York, NY: Palgrave Macmillan, 2011).

[237] Ibid., 19.

[238] Jason Powell, "Scholars, Servants, Spies: William Weldon and William Swerder in England and Abroad," ibid., ed. Robyn Adams and Rosanna Cox.

Elizabeth, other tactics were also used to manipulate people of interest. Spies delivered gossips and specific information intended to persuade the recipient in a certain cause. Rather than money in this era, spies were also seeking “patronage and preferment”[239] in the context of intelligence gathering as a political activity. An interesting fact for this historical period is that there is no written evidence about the life of popular spies after they ceased their operations. Sporadic are the examples of spies who retired after the end of their employment and historians are speculating that such retirements could have been initiated on behalf of the person who hired them because the agent was exposed[240]. Regarding the women’s role in intelligence gathering during the Renaissance and Modernism, it is well emphasized and acknowledged, as opposed to earlier historical periods, that they were “political intermediaries, brokers of patronage and information”[241]. This was true because of the social networks they have established with family members, relatives, friends, acquaintances and other people who were connected to the same social circles. Since transportation was not very well developed at the time and distances were long and people – frequently traveling, letter-writing has become instrumental to the maintenance of these networks through which women regularly received, disseminated and exchanged news in addition to exercising influence and persuasion.

Especially in England, having a queen, rather than a king made the role of women in court tremendously important, as Elizabeth herself relied heavily on information gathered by appointed female servants and members of the nobility. In addition, it was not only information that was collected by them. They had even more active and responsible roles such as negotiators, intermediaries, and influencers. Women skillfully used personal contacts to convey political

[239] Stephen Alford, "Some Elizabethan Spies in the Office of Sir Francis Walsingham," ibid., 48.
[240] Ibid.
[241] James Daybell, "Gender, Politics and Diplomacy: Women, News and Intelligence Networks in Elizabethan England," ibid., 107.

messages to their addressees and convince them in a particular cause. These dynamics were, however, not exempt from the context of power and hierarchy structures that undoubtedly had an important meaning for the efficiency of the persuasion. The presence of the women in court brought them quick and easy access to both national and international news as well as knowledge of the reactions to them. However, it was not only valuable information from home and abroad that interested women of the English nobility. News about the monarch, court affairs, negotiations, and any changes in the health, the marital status and the wealth of the powerful members of the court was also of particular importance. Women were also instrumental in informing their husbands, fathers, and relatives living away from the court about the latest developments in politics and social life. While earning the Queen's patronage and affection was among the main goals of members of the court at the time, many of the female spies and informants were also acting as such driven by a longing for financial profit. There are multiple examples documented in the history of women exercising influence over family members, including husbands and fathers about important matters for which they were generously compensated[242].

The development of the post office institution in Europe brought new opportunities for an enhanced and speedy correspondence but also made room for covert operations that challenged the integrity of the information enclosed in the mail. Famous at the time were the so-called *black chambers* that "were the hidden offices of secret intelligence units, staffed by an elite group of polymaths and scribed allotted their own compartmentalized task, whether translation, short-had, cryptanalysis, or forging seals, signatures and other marks that authenticated a document"[243].

[242] Ibid.

[243] Nadine Akkerman, "The Postmistress, the Diplomat, and a Black Chamber?: Alexandrine of Taxis, Sir Balthazar Gerbier and the Power of Postal Control," ibid., 172.

These chambers allowed that letters be copied, altered and resealed within a short period of time and the skills of the people employed to accomplish these were proficient enough to convince the recipient of the letter that it was never compromised or even opened. One of the most impressive black chambers was run by the postmistress of Brussels – Alexandrine (1589-1666) who was allegedly working for Ferdinand II and Ferdinand III, or, as suggested by some, for whoever was providing remuneration for her services[244]. As Brussels was a pivotal point for all the correspondence in Europe, possible influence over the information flow was an important acquisition. To alleviate the problem with the monopolization of the mail distribution, the emperor of the Holy Roman Empire was asked by citizens to grant permission for private messengers who would deliver regular mail, supposedly without political significance. While the emperor allowed private messengers, the condition that he set made the delivery difficult, expensive and without any practical use. This way, the family of Alexandrine of Taxis established control over all the correspondence coming out and passing through the empire, which allowed her to exercise power over the political and diplomatic affairs in more than one state.

Deception continued to be a weapon in the hands of the parties in conflict after the end of the Renaissance and the early Modernism. A vivid example from the eighteenth century is the one with the Jacobite rebellion from 1745 against the Hanoverian rule[245]. In this case, both sides skillfully used deception to gain leverage in their battle with the enemy. First, the Jacobite employed strategic tactics to confuse the Hanoverians about the size and the location of their forces. Small numbers of troops were sent to different locations that were inconsistent with where they mapped their routes in reality. This way, the Hanoverians not only made a mistake

[244] Ibid.

[245] Stewart and Newbery, *Why Spy? The Art of Intelligence*.

about the size of the Jacobite army but also got misled about their intentions in terms of locating the troops and the routes they were going to use. However, the Jacobites were outsmarted by the Hanoverians as well. The latter sent a spy to the Jacobite camp who pretended to be a soldier who wanted to join their forces. Warmly welcomed among the Jacobites, the Hanoverian spy provided some false information that was perceived as plausible by Prince Charles.

A later example of the art of deception is the one involving Richard Meinertzhagen, a British Colonel who diligently executed a series of deception operations during World War I[246]. Meinertzhagen prepared a set of British official documents listing their intentions to attack Gaza. The purpose behind this plan was to mislead the Turks about the British military plans. Meinertzhagen hoped that Turkish spies will intercept these letters. Previous attempts to employ such maneuvers, however, appeared to be unsuccessful as the Turks did not seem to get access to the planted false information. Thus, Meinertzhagen utilized a different strategy this time. He made the deception scene much more believable for the Turks, as he fired a few shots in the proximity, leaving some bloodstains on his equipment and his haversack where the letters were left. The operation gained success as the Turks focused on Gaza thus allowing the British to invade Beersheba without resistance.

Post-Modernism. The two world wars brought new aspects to the problem of intelligence gathering. They provoked rapid developments in technology as this changed how it was used to support the collection of information about the enemy. Deception operations were proliferating. An integral part of such operations was the outlet through which the information was disseminated. While in democratic countries the opportunities for purposeful dissemination of particular agenda-oriented content were somewhat limited, in authoritarian countries such

[246] Ibid.

actions were much more easily implemented. The Soviets skillfully played with the tools of deception as they sometimes would "put armaments on display with a certain amount of fanfare in order to draw attention away from other armaments they may have in their arsenal or may plan to have. Sometimes they exhibit mock-ups of planes and other equipment, which may never see the light of day as operational types"[247]. Other outlets of disinformation were also employed. For instance, archives show that Soviet diplomats were instructed to share a specific piece of information with diplomats of a neutral country who also had contact with the enemy countries, relying that the neutral diplomat would share with them this piece of information, as it happened on more than one occasion. Such strategy was frequently put in action by the Soviet Foreign Office[248]. Moreover, there was a special unit within the KGB called the *Disinformation Bureau* whose main purpose was to misinterpret and place in negative context policies, statements, and other official documents of Western governments. In addition to this, this bureau was assigned to forge documents and provoke tension based on religious grounds, such as propagating anti-Semitism. On the other end of the world, the CIA was also busy recruiting different agents to report to them. They were successful in recruiting Soviet agents who, as reported, were disillusioned by the false promises of the Soviet political system or particular issues such as the "KGB's treatment of Russian peasants"[249]. Later, the traitors were captured and executed by the KGB as the CIA had promised them no protections as voluntary agents. However, in cases in which intelligence was needed, and there were no voluntary spies, CIA used deception to make people, unwilling to report to the agency, share information with them through another agent,

[247] Dulles, *The craft of intelligence: America's legendary spy master on the fundamentals of intelligence gathering for a free world*, 149.
[248] Ibid.
[249] David L. Perry, ""Repugnant Philosophy": Ethics, Espionage, and Covert Action," *Journal of Conflict Studies* 15, no. 1 (1995): 4.

typically known to the involuntary informant. For instance, if the unknowing informant harbors resentments toward the U.S., then the person interacting with them would present themselves as non-U.S. citizens, typically citizens of a neutral country. Another way of obtaining information from people unwilling to share it with the CIA was through coercion. The CIA agent would exercise pressure over the informant through some sensitive, humiliating or incriminating information and thus ensure the informant's cooperation[250].

After the end of the Cold War, the espionage declined in intensity. Later, with the emergence of the Internet, almost everything changed, including the ways espionage was conducted. Interestingly, many of the deception and manipulation techniques remained the same, but they were executed differently. With astonishing ease, a sentence could travel to the other end of the world, reaching millions of people, in a split second. In 1993, alarming articles warning people of the beginning of a *cyberwar* started appearing. Two political scientists – John Arquilla and David Ronfeldt added that people should prepare for a *netwar* which includes actions to "disrupt, damage, or modify what a target population 'knows' or thinks it known about itself and the world around it"[251]. They also mentioned that such manipulation could take place in many domains (psychological, political, cultural) and take many forms (altering public opinion or the opinion of the people with power in society). The most important conclusion that they reached was that such type of deception was going to change both politics and warfare.

In 2003, a policy document from China confirmed the predictions of Arquilla and Ronfeldt. The Chinese military declared that their strategy is built on three pillars – warfare understood as a psychological influence, manipulations of legal aspects of international

[250] Ibid.

[251] P. W. Singer and Emerson T. Brooking, *LikeWar: The Weaponization of Social Media* (New York, NY: Eamon Dolan Books, 2018), 183.

agreements, and influence over public opinion[252]. Fully realizing the growing threat, NATO created the Strategic Communications Centre of Excellence, intended to counter disinformation and propaganda campaigns on social media. Very soon, the Internet became an arena for battles of regular people, politicians, celebrities, armies, terrorists, criminals and even entire governments. The technological advances gave birth to bots and trolls who severely disrupt the perception of public dialogue, of public opinion. The consequences of their actions went far beyond a simple disruption, however. Slowly, the disruption started to change the dialogue itself and to reach matters of highest importance – the U.S. presidential election in 2016. At his point, it has become clear how seriously the information warfare affects every sphere of the public and private life of people. As many things changed from the classical antiquity period, other integral elements of deception remained unchanged – the power of "narrative, emotions, authenticity, community, and inundation"[253]. Bots and *trolls* mastered the art of disinformation and misinformation as they changed the public dialogue in the desired way allegedly establishing *social consensus* on popular topics among the users online.

Advancements in information science were welcomed in authoritarian countries as just another way of imposing control over the citizens by monopolizing the public dialogue. Some states went even further than this. China, for instance, introduced its *social credit system* in 2015, according to which the citizens will be assigned a specific score based on their activities thus assessing their loyalty to the state[254]. Establishing control over WeChat – the Chinese version of an expanded, multi-functional Facebook would feed the authorities with useful information about the citizen's daily activities, thoughts, judgments, and general attitude. Interestingly, a study by

[252] Ibid.
[253] Ibid., 21.
[254] Ibid.

Pan, King, and Roberts (2017) found out that in addition to the propaganda efforts of the Chinese government executed by people called the *50-Cent Army* (based on the payment they receive for one social media post), Beijing also relies on methods of distraction rather than just disinformation[255]. Converting the attention from popular public topics to other topics that do not attract attention is a strategy that is among the weapons of domestic psychological warfare. Russians, however, openly employ disinformation techniques, adopted by government agencies, both toward their own people and abroad. One of Russia's generals, Valery Gerasimov, emphasizes the increasing role of non-military methods of influence, simultaneously viewing Russia's efforts as a *defensive* campaign that is merely a response to information cyber-attacks by the West[256]. Some non-cognitive cyber-attacks (such in which a device has been compromised directly, without manipulating an individual) are prevented successfully by the computer engineering industry through anti-virus programs, passwords, encryptions, and cyber security tools. This does not mean that cyber-attacks are not getting more sophisticated and ceased to cause problems online. In comparison to cognitive cyber-attacks, however, non-cognitive ones are much more easily identifiable and are therefore much easier to be prevented. An instance for this is Mark Jakob who, using access from his former employer – Internet Wire, issued a fake press release concerning the resignation of Paul Folino, a CEO of Emulex (server and storage provider), accompanied by news that "the company was under SEC investigation"[257]. As a result, stock prices dropped and ultimately led to Mark Jakob profiting from rates that were lowered artificially after the press release. It was Jakob's access to Internet Wire – the company

[255] Gary King, Jennifer Pan, and Margaret E. Roberts, "How the Chinese government fabricates social media posts for strategic distraction, not engaged argument," *American Political Science Review* 111, no. 3 (2017).
[256] Singer and Brooking, *LikeWar: The Weaponization of Social Media*.
[257] George Cybenko, Annarita Giani, and Paul Thompson, "Cognitive Hacking: A Battle for the Mind," *Computer* 35, no. 8 (2002): 50.

producing press releases, rather than any technical skills that helped him achieve his goal. The same rule applies to theft-of-secrets cases in which an employee in a company from the defense industry is misled to release confidential information, thinking that the person requesting it is entitled to know it. Rather than old-fashioned hacking and unauthorized access to computers, the problem here is the human cognition rather than the level of security of a device.

Evolution of cognitive threats: from the Trojan Horse to Facebook

Development of cognitive threats in the classical antiquity. The technological, societal, and cultural developments in the classical antiquity may look much slower and much less progressive when compared to further historical periods, but they are nevertheless still significant. They set the foundations of many components of today's life, including some social consensus about reality and truth, and identifying deviations from these, such as deception. In the 21st century, the problem of *truth* is very complex. For the people in the classical antiquity, the dimensions of this notion were much clearer. There were figures within the society, outlining the aspects of what *truth* is who were trusted and who were enjoying respect and obedience. Truth was very closely related to the idea of culture. People responsible for cultural norms, usually men in this era, were individuals "who do their work of cultivation within specific institutional contexts for specific social groups with a vested interest in sustaining their activities"[258]. Different examples of such people were priests, monks, rabbis, scholars, librarians, educators, etc. Even as early as in the classical antiquity era, educational materials, such as the Latin classics, served a powerful political purpose – to unify people, to impose ideas both by religious and secular authorities. Simultaneously with this, access to knowledge was severely limited and

[258] Michael S. Silk, Ingo Gildenhard, and Rosemary Barrow, "The Classical Tradition: Art, Literature, Thought," (Hoboken, NJ: John Wiley & Sons, Incorporated, 2013), 33.

considered a privilege. Books were copied by hand and copies were disseminated by missionaries and pedagogues, traveling to distant locations, teaching pupils reading and writing in Greek. Literacy was a skill for the elite, not for the masses. Incapable of reading from the source of information, people were vulnerable to misinterpretations, intentional or not. Controlling literacy meant control over the *truth.* Control over the truth meant control over the population's minds. The agreement with authorities was the prevalent spirit in which most works were written until the 18th century when authors started disobeying the accepted norms for writing[259]. This does not mean that attempts were not made to refute the *truths* established by the authorities, but they were quickly destroyed, and their authors sued for treason and either imprisoned or murdered. Because of this long-lasting tradition of works, embedding moral norms, political and social attitude, desired by the authorities, later works in 18th century denying these principles, became especially appealing to the masses – a tendency that continues even in the 21st century.

It was also in the classical antiquity when the first archetypes were created – a notion of which is still present into the contemporary literature and from there – to the everyday life. The stereotype of the hero, representing "the admiration for the man of action"[260] embraces different features, both physical and moral that created standards for generations of people from ancient Rome to present days. The male hero, muscular and physically attractive shows his strength and courage mostly in times of war, as the latter started to get perceived as a desirable opportunity for the hero to demonstrate his exceptional qualities[261]. Violence was depicted as acceptable, as it

[259] Ibid.
[260] Ibid., 264.
[261] Akkerman, "The Postmistress, the Diplomat, and a Black Chamber?: Alexandrine of Taxis, Sir Balthazar Gerbier and the Power of Postal Control."

served to portray the domination of the hero against the villain, the win of the good against the bad.

Seen as an ultimate opportunity for bravery and exceptionalism, wars were presenting a chance for demonstrating personal qualities and superior military thought that was becoming more and more technological in nature. The invention of the catapult as a powerful tool in sieges and attacks of fortifications brought an undisputable advantage to one of the sides of the conflict. As a response to this new weapon, further advancements in weaponry also emerged. For instance, during the siege of Perinthus in 341 BC, the Macedonian king used archers with arrows positioned in higher than the catapults towers[262]. Later, soldiers throwing stones were also included in the campaigns during sieges. With these technological innovations, sieges have become complicated, costly and lengthy operations. While it was obvious that both sides of a conflict will compete about whose weapons are more effective and have higher destruction capability, it was in many times wit and resourcefulness that won battles, rather than the technology itself, even in these early centuries of traditional warfare. Among many others, one example of human wisdom defeating military technology is the one with Diognetus – the military engineer of Rhodes. He stopped Demetrius Poliorcetes's siege of Rhodes not with a more powerful machine, as one of his competitors - Callias offered, but with wit. It is reported that "Diognetus stops the siege engine in its tracks by diverting an enormous amount of water, mud and refuse out of the city; the machine is caught in the mire"[263].

In conclusion, most ancient societies skillfully employed deception techniques, espionage and counterespionage as conventional weapons in war. Slowly with time, even Romans started to

[262] Serafina Cuomo, *Technology and culture in Greek and Roman antiquity* (New York, NY: Cambridge University Press, 2007), 49.
[263] Marden Fitzpatrick Nichols, *Author and Audience in Vitruvius' De Architectura* (Washington, DC: Cambridge University Press, 2017), 27.

use deception in their battles as wars became more complicated and the competition between new technology, advanced strategic planning and cartography became fierce. Manipulation and coercion manifested themselves as standard practice in later periods. Moreover, the historical figures who used them actively in their political careers were among the most successful leaders, using their intellect to gain and retain power quickly and efficiently.

Development of cognitive threats in the Middle Centuries and in the two World Wars. One of the most significant changes in terms of military planning was that modern intelligence institutions have emerged in this period, as one of the first official heads of such office was Queen Elizabeth's Secretary of State – Sir Francis Walsingham[264]. Some authors share that it is even possible that the famous Cardinal Richelieu learned a lot from his predecessor about deception, political maneuvers, and intelligence[265]. There was a notable proliferation of Black Chambers across the European states as the need of intelligence, espionage and counterespionage grew exponentially. However, durable institutions engaged with collecting information over time both in war and in peace were absent. When the need arose, different political figures were tasked with intelligence gathering through their networks of spies, including diplomats, who had their own channels of information[266]. Diplomacy, at the time, did not have the dimensions it has nowadays, as ambassadors were acting merely as official spies rather than having a more independent role than this. Industrial changes brought new opportunities and challenges in military campaigns for which armies should have prepared - the need for timely and quality intelligence mainly regarding maps and railways. The first permanent intelligence structures were established in Britain and in America in the 1870s and 1880s, followed by the British

[264] Michael Herman, "Diplomacy and intelligence," *Diplomacy and statecraft* 9, no. 2 (1998).

[265] International Spy Museum with Denis Collins, *Spying the secret history of history* (New York, NY: Black Dog & Leventhal, 2004).

[266] Herman, "Diplomacy and intelligence."

Secret Service Bureau conducting operations of espionage and counterespionage in 1909[267]. Among other technological innovations, the radio changed not only the everyday life of citizens but also military planning and the campaigns themselves. Radio channels also provided ways of intelligence gathering and deception at the same time. For instance, a captured soldier may have been kept alive if he had a radio station ensuring direct communication with the enemy through which deceiving information could be conveyed[268]. Aerial photography, and later satellite surveillance also quickly altered the dimensions of traditional warfare. If this innovation was used by one side in a conflict, then automatically, ways of deceiving the enemy through this technology were emerging. An instance of this is the British deception of Nazi bombers during World War II. The former hid their airfields, masking them as farms[269]. A similar strategy was also used for other targets of significance. It is not clear if technological development in these decades was driven by military needs only or the military needs changed as a consequence of the rapid technological developments. Therefore, it could be concluded that they were intertwined in a way that made a clear statement – technology changes intelligence, its sources, its goals and the how counterintelligence was conducted. In this case, would it be enough to gather information only by using the latest innovations in the world of technology? Machines were replacing agents and other personnel, doing their job faster and without the worries of possible errors. Why did then the traditional intelligence gathering kept relying on methods different than machines? James Schlesinger, who became a director of the Central Intelligence in 1973, said: "[y]ou cannot photograph an intention"[270], implying that human intelligence and technical intelligence

[267] Ibid.

[268] Dulles, *The craft of intelligence: America's legendary spy master on the fundamentals of intelligence gathering for a free world.*

[269] Ibid.

[270] Stewart and Newbery, *Why Spy? The Art of Intelligence*, 77.

could only be successful as long as they are complementary and not used independently. This became even more evident in World War II as the notion of *total war* “needed total intelligence, not restricted to military matters, on the adversary as a whole and all his national capabilities”[271].

While significant, changes in the way military campaigns were conducted was not the only way in which cognitive threats evolved. Religion and culture were just as important as technological developments in these periods. The rapid technological developments, along with changes in how political power was distributed brought disruption in people’s sense of identity. European countries that were behind others or felt like they were soon going to be behind felt insecure and started questioning their belonging to a particular social entity. As this was compensated with an attempt by politicians to bolster this sense of identity and unity, some states started to feel like they were not getting the necessary respect that its citizens thought they deserved. The most vivid example in this regard was Germany, but similar moods were also present in Slavic countries, Finns, and Magyars[272]. The industrial revolution was understood differently by people. The first notable crises in religion were in the sixteenth century, as it was starting to fail to respond to some questions that were gaining popularity among people[273]. The role of religion, at the time and further until the Industrial Revolution, was still sensible but slowly declining, giving room to blossoming ideologies in the 19th century that were more suited to explain the changes that were happening during this time. Lindemann[274] outlines a few questions that were taking central place in public debates in Modern Europe. These questions demanded more specific answers than what religion was capable of providing. Thus, these

[271] Herman, "Diplomacy and intelligence," 3.
[272] Albert S. Lindemann, *A history of modern Europe from 1815 to the present* (Malden, MA: John Wiley & Sons, 2013).
[273] Cathal J. Nolan, *The Age of Wars of Religion, 1000-1650: An Encyclopedia of Global Warfare and Civilization*, vol. 2 (Westport, CT: Greenwood Publishing Group, 2006).
[274] Lindemann, *A history of modern Europe from 1815 to the present*.

questions were the generator of the proliferation of ideologies: “the Social Question (touching on such new ideologies as socialism and capitalism), the Woman Question (feminism, the changing status of women), the Irish Question (nationalism, racism, imperialism), the Jewish Question (antisemitism, Zionism), the German Question (nationalism, racism), and the Eastern Question (having to do with the fate of the Ottoman Empire, especially in the Balkans and the Middle East)”[275]. It is argued that in times of uncertainty, people look to attach themselves to a collective entity that ensures proper confirmation of one’s identity. An amalgamation between religion and nationalist ideology is found to be particularly successful in reaffirming identities and providing ontological security in times of intensively changing environment[276]. As leaders found that ideology could be a mighty weapon in mobilizing people to do one thing or another, they started shaping ideologies as antidotes of other ideologies (e.g. communism as an antidote to capitalism). Part of this discourse were propaganda campaigns with the aim to convince people in the rightfulness of a particular ideology. In some cases, however, the propaganda went further than this and employed disinformation to a goal different than just attracting people to an idea. There are some examples of cognitive threats that aimed to convince people in the superiority of a particular ideology, but they needed more than just this. They wanted particular actions from the recipients of the disseminated messages – for instance overthrowing capitalist governments (communism) or provoking oppression or aggression to minority ethnic groups (nationalism).

Development of cognitive threats in the 21st century. The beginning of post-Modernism brought tremendous changes in the way people understand warfare. While cultural, religious and

[275] Ibid., 56.

[276] Catarina Kinnvall, "Globalization and religious nationalism: Self, identity, and the search for ontological security," *Political psychology* 25, no. 5 (2004).

social changes are still very important in this time period, the progress in technology was the most remarkable component in studying the evolution of cognitive threats in warfare.

Social media made a big step toward changing traditional perceptions about communication, interaction, and even politics and diplomacy. The high number of significant events whose beginning can be traced to a conversation or an initiative in social media is an example of how successful they were in connecting and uniting people, easily, quickly and effortlessly. The figure of the individual in political science and international studies gained new meaning as humans, and their collective actions in social media attracted the interest of many scholars. It was not only the participants' strong will to change regimes, policies and to voice concerns of social significance that brought them to social media. It was simply the addictiveness of the social media platforms that not only attracted but kept and gained even more users worldwide. The idea behind social networks was to create an interaction that resembles the features of a real face-to-face interaction – through emojis, likes, shares, tweets, and other reactions. Lured into this easy way of compensating for distance and lack of actual communication with friends, people started to share details of their lives with individuals with whom they would not even think about sharing in person. Users have known and still know very little about the huge amount of data that was gathered from them but not for them. Tired of lengthy legal notices online, users eagerly click *agree* to anything that could be on these forms. As a consequence of this and the fact that very little has been shared about what has been done with the collected information, users consent to participate in a game for which they do not know much. This could not be labeled literally as deception since the legal notices notified users for various things. Companies are aware that the vast amount of the users will not read what they agree to or will not understand the language and the implications of the content. Relying on these instinctive human reactions to avoid reading pages of information that they find hard to understand, companies skillfully gained a legal way of profiting from their users' information. As opposed to this, some actions of social networks were violating rules and laws, as it was in the case with Cambridge Analytica, which will be explored in detail in Chapter 3.

The new social setting gave birth also to new conflicts and diplomacy-making. While both could come from public figures, most voices in these conversations were anonymous which made traditional understanding of warfare and negotiations disrupted and unclear. In the era of Modernism, diplomacy was a more secretive enterprise involving meetings at undisclosed publicly locations between representatives of different governments. Social media changed all this, as the entire process became "less private and policy-oriented and more public and performative"[277]. In practice, it was the loudest voice that mattered, rather than the voice stating the more solid argument. Quantity replaced quality in the online conversations whose main value was the attraction of attention rather than statements supported by proven facts. One of the mechanisms for spreading a message was through like-minded people who, due to their confirmation biases, agreed and shared rapidly the content online very often without even questioning the source or the truthfulness of the message. In the classical antiquity, Renaissance and early Modernism, the personality behind the message mattered, as reliability was mostly determined by the status of the person delivering the information. Commanders, rulers. and people of power shared information that was rarely doubted. However, even in these periods, with the creation of deception and disinformation as a military strategy tool, it became evident that a story that is confirmed by various sources should be accepted as true. As the power dynamics shifted and the world transitioned into democratic forms of government, the voice of

[277] Singer and Brooking, *LikeWar: The Weaponization of Social Media*, 15.

the citizens started to matter more. With social networks, the personality of the messenger became even more loosely associated with the reliability of the message, also because in many cases there was very little known about the author. Moreover, many people who use social networks for entertainment and communication are still not fully aware that unknowingly and inevitably they are part of a much bigger picture – of conflicts, of corporate interests, money, and power.

One of the most remarkable advancements in technology that reflected directly on many areas of human life are the neural networks. Simply put, they represent a different kind of computers that do not rely on a simple mathematical rule to make deductions but use complex systems of information that build connections between each other and are based on recognition rather than on a specific command. In many ways, these neural networks are supposed to imitate a human brain, as it was claimed years ago that machines would never be able to think on their own unless they start learning. That possibility is no longer theoretical as neural networks keep evolving in ways that are closer and closer to how human brains function. Among the numerous applications of neural networks that are beneficial to society (e.g., in medicine, predicting the weather and financial trends), neural networks started to get utilized in many other ways that are nowadays considered, controversial, the least.

Interestingly, as social networks took a central place in social life and modern warfare, the role of the users in these networks also changed dramatically. They intended to contribute content, exchange thoughts, and other information have transformed partially into observers of interactions between trolls, bots, chat-bots and other advanced algorithms meant to simulate human online activity[278]. These neural networks' main task is to make predictions. While their

[278] Ibid.

application was oriented to helping people, the users turned out to be the study subjects of neural networks and AI technologies. This, by itself, does not necessarily entail adverse consequences. However, in the post-modern era in which corporations with practically unlimited capabilities were proliferating, money and power have become even more central. The means of obtaining them in a time period in which democracies are accepted as the predominant political model in the world is to simply control the *demos* (the population). Admitting to openly controlling a population would contradict the principles of freedom of thought and speech in democracies. Regardless, machine learning and AI made it possible that people give in the control over their own cognition to others, unknowingly sharing information about every corner of their minds. What is more problematic is that social media is just one part of the problem. It is also the easy access to tracking the digital moves of people, that helps corporations and governments collect so much data. Moreover, technological developments have a very important quality – they are irreversible. Once they emerge and begin being used, there is no way of forgetting about them. Even with nuclear weapons and years of international treaties and negotiations, they still exist, and their creation cannot be undone. The possibility that they are used will always be there.

Another technological development threatening to bring new meaning to warfare is the so-called *deepfake* software. What this software does is manipulating video and audio content. Thus, the face and the voice of a celebrity or a public figure can be adjusted in a way in which actions, statements, and expressions appear to come from them. An old predecessor of the *deepfake* content was the Photoshop software, which started being used to manipulate pictures to deceive people and institutions to which they were presented. The more advanced the technologies become, the more real their products look like. Furthermore, while such manipulations still require skills and access to software that is typically controlled by organizations, governments, or super-empowered individuals, specialists predict that these techniques will rapidly become more accessible to different actors with various goals, some of which harmful to society[279]. Strategic analyses outline trends that could create favorable conditions for the implementation and the intensive use of AI and cognitive threats – a fact that makes it an even more serious threat to society in the future[280]. First, in the political realm, changes are expected in terms of the increasing role of non-state actors, power-politics, and distribution of power in the international system. Among the most important elements of some cognitive threats is also the increasing public discontent with how power is distributed and is being exercised. As for changes expected with human capital, growing urbanization, the polarization of societies, and human networking will also create an environment for cognitive threats. In the area of economics and innovations, the dependence on technology and the expanding inequality (including gender inequality) is likely to make populations vulnerable to tools of psychological warfare and manipulations.

All of these conclusions led to several points of consideration. Singer and Brooking[281] underline that now that internet has conquered a place in people's everyday life, it will continue to be present and will even expand its meaning further. Next, they confirm that the cyberspace is an arena for battles, information is a weapon and should be carefully thought about in such way. Participants in these battles are users of technologies, regardless if they consider themselves as participants or have unknowingly become such. That said, governments should urgently adopt new approaches to fight any harmful practices employed in the cyberspace. Thus, it is crucial that users have literacy and are educated about the multitude of ways their information can be

[279] Marc Jonathan Blitz, "Lies, Line Drawing, and (Deep) Fake News," *Oklahoma Law Review* 71, no. 1 (2018).
[280] NATO, "Strategic Foresight Analysis," (Norfolk, VA 2017).
[281] Singer and Brooking, *LikeWar: The Weaponization of Social Media*.

used, and the purpose and the meaning of this use. It should be recognized that efforts at the governmental level are not going to be sufficient to combat the problem. Technological giants in the industry should assume responsibility for their actions since most of people's everyday life is linked to the use of the internet and technology in general. Presented as sources of entertainment, communication channels, and a non-political space, owners of social network companies can no longer pretend that their products do not have other applicability and goals. Before all, these companies are established to make profits, and such are provided through a variety of ways that obscure the idea of their neutral nature. Bots taking over Twitter, examples of hate speech remaining unpunished on Facebook are just a few examples of why cognitive threats have become so prevalent. Bots create conversations and provoke people to be more active online which increases the popularity and the attention to Twitter. At the same time, Facebook was incapable of imposing rules condoning hate speech and offensive behavior online. The number and the popularity of some of the users were just as valuable as money for the company since the former, in no small part, ensures the influx of financial profits. As any other entity that has influence over a large number of people, social media quickly became a means to achieving certain political goals by actors. They used this space to quickly and effectively disseminate disinformation or to impose targeted political advertisements, both of which for the purpose of tailoring public opinion in a way favorable to the perpetrators, thus violating the democratic process.

The fight against cognitive threats

Cognitive threats are a very specific category of military and political challenges that differ from other types of threats. What distinguishes them from traditional threats is that they are not material, in the first place. Thus, it is difficult to know exactly when they reach the victims and the extent to which they will be harmed. In many cases, it is also unclear how the damage will be manifested and when. Some of these questions are relevant to other, traditional, material types of threats, for instance, a nuclear threat but science has good answers about the predicted effect of these threats. However, similar to them, cognitive threats do not have a history of being successfully fought once the attack is launched. Regardless, there were many attempts over the years to combat cognitive threats, even nowadays. These attempts are mostly two main types – directly fighting cognitive threats that transformed into successful attacks, as the process of conveying the manipulative information is accomplished already, and prevention and deterrence – seeking to convince the party responsible for the cognitive threat that the costs of launching it outweigh the benefits. Psychological mechanisms, increasing the number of personnel and their preparation, educating users, implementing new secure devices, new software and policies were implemented to counter the detrimental impact of cognitive threats. In order to answer the question to what extent these measures were and are currently successful, in the following sections I will provide an overview of the tools used to counter four of the most common types of cognitive threats that I previously mentioned: 1) traditional intelligence gathering and persuasion through deception, 2) disinformation, 3) recruitment practices through cognitive manipulations, and 4) collection and exploitation of information for political gains by companies and even governments (e.g., China).

Traditional intelligence gathering and deception is probably the oldest type of cognitive threats in human history. As mentioned previously, some societies were reluctant to use them in warfare initially, such as the Romans, but later this changed as this turned out to be a war tool that is cheap, fast and effective. Examples show that they sometimes outweighed the benefits of expensive and complicated machines which could be destroyed with a simple trick of the mind. The most common scenario in which cognitive threats were present in the classical antiquity is the one related to fake deserters who gathered information and then reported back to their command. At the time, the mechanisms that were used to prevent the flow of information to the enemy's camp were mainly the experience with previously known cases of fake deserters and the awareness this brought to future cases. Commanders, politicians, military strategists started becoming more suspicious of newcomers and strangers and the information they were sharing. However, the complete isolation from contacts with newcomers or outsiders was impossible for many reasons including the need for merchandise, especially in wartime. Thus, the previous experience with deceptive practices, the awareness that it may happen in the future and the lessons that were learned were the primary weapons against such threats. This, however, was not in any way a guarantee that they will not happen again. Furthermore, if the very same deception that was used before in similar circumstances occurred again, there was no guarantee that it would have been caught even though leaders were aware of similar cases in the past. Captured spies, especially such from a perceived as friendly, state, were punished severely and the relationship between the former allies quickly became strenuous. Knowing the possible consequences of spies being caught, states were sometimes reluctant to proceed with their actions, especially if there was a risk of starting a war for which they were not prepared or an end of a diplomatic relationship that was otherwise beneficial in economic and political regard. In a very elementary form, deterrence against deception emerged as countries were sometimes not ready to pay the high price of a captured spy or an exposed deception that could be linked to them thus possibly causing a war.

Further, in the Renaissance and in the early Modernism, the art of torturing and questioning, especially in the era of powerful monarchies was proliferating. A wide range of methods of obtaining information was used. Despite the elaborate mechanisms of making people report information of interest, in many cases, physical tortures made the prisoners more likely to deliver information that the torturers wanted to hear, rather than the truth. Torturing also became a powerful method for political retaliation thus information gathering did not always deliver the expected results. Monarchical societies after the end of the classical antiquities were more structured– farm workers had their own social circles, royals, and people of noble origin who were typically present in the court and had their own community. The lower class had no access to the elite, as the only exception were the merchants depending on their status. The wealthier and more prestigious merchants had access to court, and the poorer ones were selling their products and services to the lower class outside of the court. Even with these social divisions, however, it was difficult to know every single person who resided in the court since the servants taking care of the nobles were changing frequently. The sanctions for treason and espionage was, similar to the previous era – death. Even with the prospect of such punishment, a large number of people were ready to use deception and manipulation to obtain information for the highest bidder who will ensure money, power or both. Hence, the increased level of security and the relative isolation from other circles of the society were not sufficient. Without any doubt, such measures were contributing to some extent to prevent cognitive threats, but at the same time, they just made manipulations and deceptions more elaborate and thus frequently successful.

In the era of the Renaissance and the Modernism, the possibility of war and an end to diplomatic relationships with countries whose spies were caught, and their plans exposed also served as deterrent to cognitive threats. In this time period, even more than in the classical antiquity, economic dependence was present and was a powerful reason not to risk war or sanctions with a friendly or even an antagonistic country. The fear of lengthy and extremely painful tortures in cases of exposure of the agent was also a significant deterrent for the lack of involvement in such missions. It has to be mentioned that religion was still very important component in these societies. The loyalty to the monarch, whose figure was directly connected to the idea of God's representative on Earth, was also motivation for abstaining from spying and deception against the crown. Loyalty, patriotism, and religious piety, at least partially, served as a barrier to actions involving cognitive threats. Interestingly, sometimes the same political and religious reasons served to encourage deceptive actions in support of the monarch. For others, however, money and power were a much more important priority, which is also the most important reason why even considering these deterrents, cognitive threats were still very common and once triggered were difficult to be prevented, and their effect reversed. That said the fight against cognitive threats was not delivering the expected results unless it was caught in time before it triggers a particular behavior from the recipient. Once the behavior, goal of the cognitive threat, was present, its mission was accomplished, and it could no longer be prevented. A very bright example in this regard is Lord Walsingham and his intention to do everything possible to protect the reign of Elizabeth I from her cousin Mary Queen of Scotts. Walsingham tricked the Catholic queen in exile to get involved in an assassination plot against Elizabeth. At the time, even though Mary was a threat to her throne and her lands, Elizabeth I was reluctant to sentence her cousin to death. Aware of these sentiments, Walsingham deceived Mary to consent to an assassination plot against Elizabeth. The proof of her involvement was still not enough for Elizabeth to confirm the death sentence and Walsingham fabricated a few other plots for her assassination with the idea to make her afraid for her life and reign[282]. After Walsingham's skillful portrayal of Elizabeth being surrounded by Catholic enemies and traitors, she finally consented to Mary's execution[283].

Further, during the Cold War concerns about breaking diplomatic ties was not an issue since the world was bipolar at the time and the connections between the two camps were already broken. Economic dependency was only present in countries who were satellites either of the West or the Communist bloc, and they were reliant mostly on their patrons. Security measures were increased, espionage and counterespionage, deception techniques and intelligence gathering were proliferating. At the same time, connections of people from either the West or the Communist bloc with individuals from the opposite side was considered ideological betrayal and was thus severely repressed. It is paradoxical how in such isolation between the two camps, so much traditional espionage and deception was still taking place despite the highly limited interaction between people supporting different ideologies. The political conditions created a favorable environment for cognitive threats. Severe punishments including death were not enough to prevent agents from executing cognitive operations against their own countries. As opposed to nuclear threats whose detrimental effect both sides realized, cognitive threats were perceived as quite common weapon in warfare at the time. Moreover, since diplomatic relations were not a concern, states invested large amount of resources in expanding the espionage and counterespionage units. Deception gained new dimensions, and such operations became much more elaborate than in previous years. In fact, the ideological competition at the time was so

[282] Robert Hutchinson, *Elizabeth's spymaster: Francis Walsingham and the secret war that saved England* (London, UK: Weidenfeld & Nicolson, 2006).

[283] Neil Younger, "Robert Peake (c1551—1619) and the Babington Plot," *The British Art Journal* 14, no. 2 (2013).

intense that many argue that the Cold War was more a battle for people's minds than anything else[284] [285].

The end of the Cold War and the new technological society in the 21st century marked a new chapter in the history of cognitive threats. Much has changed since previous historical periods. First, most of the states are now democratic rather than autocratic even though some examples with authoritarian countries show how cognitive threats thrive there as well. Second, diplomatic and economic connections have uttermost importance in a globalized world in which war is a costly endeavor that the liberal world seeks to avoid at all cost. Third, globalization in its social, technological and educational aspects brought people closer than ever, even if only to be able to argue with each other. Fourth, except for a few instances with increased border control and immigration opposition, in comparison to previous eras, isolation of societies from *outsiders* was not so inherent for the 21st century. Instead, the liberal order seeks to remove borders, create a sense of common identity and bolster equality between people. Wars are far from being an extinct phenomenon, however. They just gained different dimensions in terms of the actors involved in them and the entities between which they are led. In this post-modern background, traditional human espionage through deception has a decreased role. In spite of this, it is still present. Mainly its underestimated role in a world governed by technologies brings back some of the simple deception techniques of the past – the figure of the spy deceiving an individual to obtain information about the enemy, both in the physical and in the cyberspace. Countries still maintain their intelligence gathering units and are aware of possible deception operations. Regardless, they know that they are rare because the price if a spy gets caught is higher than ever

[284] Tony Shaw and Denise Jeanne Youngblood, *Cinematic Cold War: The American and Soviet struggle for hearts and minds* (University Press of Kansas Lawrence, 2010).
[285] David Caute, *The dancer defects: the struggle for cultural supremacy during the Cold War* (Oxford, UK: Oxford University Press, 2003).

nowadays. Instead, security measures in terms of training of personnel are adopted in addition to efficient cybersecurity practices. Such mechanisms are not preventing cognitive threats altogether but just increasing the costs of an eventual attack by enemies in terms of time, strategy and resources. Furthermore, if exposed, the identity of an agent in the physical space could quickly be linked to working for their country of origin as this could create a series of diplomatic problems. Thus, a preferred way for conducting cognitive warfare is in the cyberspace where the identity of the perpetrator could remain unknown. Among other strategies for deterrence, adopting general international agreements and regulations decreases the chance of cognitive threats since they imply free will and voluntary binding. Moreover, the idea of international society where negotiations and persuasion will occur openly and in a direct manner makes deceptive operations without much meaning. The world in the 21st century, while resembling some features of international society, still has a long way to go to fully implement the ideals proclaimed by the liberal order. Thus, traditional wars still exist but so do unorthodox ones. Democracies are the prevalent form of governance, but autocracies still exist as well. In this sense, a transition to *the end of history*[286] but not an arrival to this state still grants many opportunities for non-traditional warfare, and cognitive campaigns as being the most successful of them.

Disinformation. Although the importance of disinformation was recognized early in the classical antiquity period, it went through a fascinating transformation over the ages, mostly driven by the political, technological and social conditions. Feeding the enemy with disinformation was established as a very successful strategy in the early centuries. It was not unproblematic as it seems at first glance. In order to be believable, the person conveying the

[286] Francis Fukuyama, *The end of history and the last man* (New York, NY: Simon and Schuster, 2006).

information has to be trusted or at least not distrusted. Second, the information should be tailored in a way that would be believed by the recipient. Along with these complications, the fear of exposure, the punishment and the consequences of a revealed disinformation plan also made disinformation in the early centuries a useful practice but not ideal as its cost was too high sometimes. There were some measures that ancient leaders were using to identify disinformation, such as checking the information provided by one source and comparing it to other accounts of the same event. While practical, this strategy does not come without some limitations. To attempt to verify a piece of information, first, there should be a suspicion that it could be possibly untrue. Second, there should be more than just one source available to verify the original story. Third, there should be enough time for this investigation to be conducted and such time was rarely available in wartime periods. Directly fighting disinformation was not always possible because of the reasons I outlined, and deterrence had a relatively limited effect because of two main reasons. First, war was accepted as a common phenomenon and moreover, one that was inherent and even a desired option rather than a last resort. Second, there was a lack of strong diplomatic and economic ties between the entities at the time.

In the Renaissance and the early Modernism, disinformation was also present but again – with limited use in an era with strong monarchies linked to the powerful role of religion. The application of disinformation was present mostly in military campaigns and political maneuvering. While for agents without established links to the crown, exposed disinformation was not necessarily destined to begin a war, for such who were spies of the crown or people in official positions serving the crown, war was a possible option. However, in comparison to the previous era, diplomacy was more common through marriages, the role of ambassadors and other economic arrangements. While wars were definitely not out of the question, frequently countries had other concerns that were consuming significant resources and were thus trying to avoid wars and retaliated similarly – with covert actions seeking to destabilize the enemy. It is important to be noted that disinformation used not against a foreign country but against a country's people was not common – monarchs had on their side religion and tremendous power concentrated in their hands and did not find disinformation of significance in domestic affairs.

The World Wars changed the role of disinformation as it gained a central place in espionage. Public opinion started to matter more than in previous centuries, and wars had to be justified in order to prevent rebellions and other disruptions in the regime as a consequence of the decision to go to war. One of the most efficient ways of convincing people of the need for war and other extreme measures became propaganda and in some cases disinformation. As previously described, the Cold War was the era with blossoming techniques of deception and disinformation as diplomatic relations carried little significance to the two blocs. Even relationships between allies in the West were sometimes full of suspicion and mistrust. The central priority of the time – avoidance of nuclear war and winning the ideological battle made disinformation an acceptable tactic that was not threatening to escalate the tension created by the fierce competition.

In the 21st century, disinformation became a regular practice and was thus recognized as a serious problem that has to be addressed. In comparison to other cognitive threats, disinformation is the most frequently used, because of the little resources (time and human capital) that are invested in producing the intended results. Much has been written on the mechanisms that disinformation uses to persuade its addressees. Less in number are the works dedicated to battling it. That could be attributed to the quick and easy ways of adjusting disinformation campaigns to overcome obstacles. For instance, if one website distributing fake news is shut down, it could be replaced within minutes with dozens of new websites that have the same mission.

Efforts are made to combat disinformation operations, but so far there is no ultimate solution to the issue. Some of the tactics recommended for dealing with this threat include the role of the military, education practices, and legislation. Among the strongest arguments for the active role of the military are the ones that underline that information operations typically come from military units and should be combatted with such, in response[287]. For instance, one successful anti-disinformation campaign was led by the Active Measures Working Group of the 1980s[288]. Another measure that could be employed in the fight with disinformation is education. Literature shows that social networks are an excellent example of *echo chambers* in which various like-minded users seemingly agree with each other, but in fact, they only confirm their own opinion on a particular question. As users do this, they reaffirm their own stance and avoid information that contradicts their convictions – a psychological mechanism that is well described in the literature. It is argued that in the digital era, education about information, computers, and the Internet is what literacy meant for society in previous time periods[289]. Oliver Batchelor[290] suggests that librarians and fact-checking services online are crucial in fighting disinformation. However, there are various problems with fact-checking as a useful strategy in this regard – one study of Twitter conversations showed that it "lags behind misinformation both in terms of

[287] Timothy P. McGeehan, "Countering Russian Disinformation," *Parameters* 48, no. 1 (2018).
[288] Ibid.
[289] Singer and Brooking, *LikeWar: The Weaponization of Social Media*.
[290] Oliver Batchelor, "Getting out the truth: the role of libraries in the fight against fake news." *Reference services review* 45, no. 2 (2017).

overall reach and of sheer response time—there is a delay of approximately 13h between the consumption of fake news stories and that of its verifications"[291].

Some computer and social scientists devote their attention to solutions to the problem that are more technical. A research team developed an algorithm for detecting hoaxes on Facebook based on the people who like the posts[292]. While such detection mechanism is undoubtedly valuable, even if Facebook has information about accounts disseminating disinformation, the administrators may still not delete them because of two main reasons – corporate interests and the right of free speech both in the physical and in the online space. As for the first, some authors write that social media companies should be regulated and held accountable as traditional media companies[293]. In terms of the second consideration, most democratic countries treasure the right of free speech as essential, and any restrictions to it should be justified. For instance, in the U.S., the First Amendment could be suppressed in light of some cases involving defamation. In addition, in speech acts that involve threats of violence or represent hate speech, the right of free speech could also reach its boundaries. Even if successful in the long run, such lawsuits could be not only expensive but also very time-consuming. As a consequence, the recipients of the false information may have already manifested some behavior that was intended by the entity spreading the false statements – a fact that no sentence can repair. Such considerations, however, deserve to be discussed seriously with another purpose – future deterrence - since disinformation harms the very idea of the First Amendment which is the autonomy of thoughts, attitude, and behavior. Marc Jonathan Blitz supports this notion underlining that "when the listener is

[291] Giovanni Luca Ciampaglia, "Fighting fake news: a role for computational social science in the fight against digital misinformation," *Journal of Computational Social Science* 1, no. 1 (2018): 149.
[292] Eugenio Tacchini et al., "Some like it Hoax: Automated fake news detection in social networks" (paper presented at the 2nd Workshop on Data Science for Social Good, SoGood 2017, 2017).
[293] Konrad Niklewicz, "Weeding Out Fake News: An Approach to Social Media Regulation," *European View* 16, no. 2 (2017).

deceived by false speech, she is doing something that autonomous and rational people never want to do: build their actions upon confidence in false factual premises. Moreover, where these false factual premises are fed to her by a speaker who uses them to steer her in ways she would never move herself, her autonomy is not only left unsupported, it is undermined, making the listener a tool of the speaker rather than an agent forming and acting on her own rational decisions"[294].

Recruitment practices through cognitive manipulations. One of the most dangerous cognitive threats is the one used to recruit people for certain political movements through appealing to their ideals. While not all recruitments for organizations and movements are defined as threats, the ones who recruit people to use them for political causes that involve violence, or prohibited coercion of any kind could be definitely labeled as a threat. The mere fact that the recruiter knows that the recruited will be used as pawns to achieve the goal of the recruiter is sufficient such practices to be defined as threats – for the recruited person and for the entity to which harm will be inflicted. In the early centuries, the discontent of the people was skillfully used as a mobilizing method of the masses. Discontent alone was not enough, however, if there was no ideal for whose name the future actions will be initiated. In this kind of cognitive threat, the personalities of the target group members and of the person, who is doing the persuasion mattered and still matter a lot – from the early centuries to nowadays. In all cases, for a successful persuasion campaign, there should be an echo-chamber with like-minded individuals who are dissatisfied by an existing fact that they want to change, and they share the same ideals that will be represented in a new status-quo after the previous one ceases to exist. The campaign will not succeed without a motivated and gifted messenger who motivates the target audience to

[294] Blitz, "Lies, Line Drawing, and (Deep) Fake News," 92.

undertake a certain behavior. In the early centuries, in order to fight such recruitment practices, it was sufficient that the leader of the movement seeking participants, gets discredited. This was not problematic considering that much of the power was concentrated in the hands of the rulers and they could incriminate anyone who is trying to dismantle the regime, as long as they have knowledge of the movement planning a rebellion. The channels of disseminating a message to potential participants in the movement were also very limited. They included mostly physical presence at the time of the speech. Such gatherings of people, however, were closely monitored by authorities and their leader usually imprisoned, if caught.

In the Renaissance and in the Modernism, the powerful meaning of ideals and identity became even more important. The channels for disseminating messages for recruitment increased in number. One of the weapons for fighting such practices was again the elimination of the leader. In addition to this, the Black Chambers added new nuances in the fight against cognitive threats in terms of recruiting. Messages were caught, rewritten, resealed and resend back to the recipients. Black Chambers caught conspiracies and exposed plots against regimes. Some monarchs and nobles used fabricated evidence of allegiance to rebel movements to eliminate political adversaries, as was the case with Mary Queen of Scotts and her perceived involvement in the Babington Plot.

In the era of democratic regimes, cognitive threats for recruiting participants in radical movements gained new meaning. While old radical formations aiming to achieve state independence and/or recognition were still present, religion and ideologies gave rise to new movements, new goals and new type of recruitment strategies with the emergence of social networks. The most vivid example of such recruiting practices is the Islamic State of Iraq and Syria (ISIS) as they not only considered the Internet as a supplemental source of conveying their message but instead, they used it as a central arena for conducting their information operations. Numerous studies explored the reasons why ISIS was so successful in recruiting new members. Among the most important ones are economic reasons, including unemployment, discrimination, a perceived violation of rights, including religious customs and traditions, adventure seeking, fame, depression, emotional isolation, confusion, loneliness, and others[295] [296] [297] [298] [299]. In most, if not all cases, multiple factors were present in a decision to join ISIS. As some of them are micro-level and other macro-level components, they are difficult to be addressed comprehensively. Societal phenomena such as racial discrimination and government policies prohibiting displays of religious symbols were also not helping in the fight with cognitive threats of this kind. It is true that traditional intelligence gathering was successful in terminating some efforts for online recruitment, but in general, the anonymity, the easy access and the speed of exchanging information were defeating the intelligence gathering agencies in their attempt to prevent recruitment. Detection of all online communication, while practiced in some cases, is still not accepted as a lawful measure against possible recruitment. In fact, as in the case with disinformation, any restrictions imposed on the right of free speech (and by extension the free communication), unless specifically proclaimed as illegal, would be a violation of the First Amendment.

Collection and dissemination of information by companies and governments. Back in the early centuries, information had a tremendous value that was recognized. The information

[295] Efraim Benmelech and Esteban F. Klor, "What Explains the Flow of Foreign Fighters to ISIS?," *Terrorism and Political Violence* (2018).
[296] Tim Slack and Leif Jensen, "Underemployment across immigrant generations," *Social Science Research* 36, no. 4 (2007).
[297] Anne Speckhard, "ISIS and the Rise of Homegrown Terrorism in the West," *Security Solutions Magazine* 24 (2015).
[298] Imran Awan, "Cyber-extremism: Isis and the power of social media," *Society* 54, no. 2 (2017).
[299] Tamar Mitts, "From isolation to radicalization: anti-Muslim hostility and support for ISIS in the West," *American Political Science Review* 113, no. 1 (2019).

about people of interest was also important. Information about regular people was not so valued, however, because they had little power to endanger the status-quo. They were the ruler's subjects, and their voice did not matter as much as in the following historical periods. In the Renaissance and in the Modernism, the collective opinion of the regular people still did not matter as much as it does in the democratic era. It could be said that the collection and dissemination of information by companies and governments is a phenomenon of the Post-Modernism. The Internet and social media along with the growing need to have an accurate perception of the political and cultural views of different social groups led to this new type of cognitive threat. Despite the fact that in the 21st century most political regimes are democratic, some remain authoritarian. Even in authoritarian countries nowadays, the collection of information plays a tremendous role – not for purposes of altering the status-quo, but for maintaining it. For instance, the Chinese government collects information from its citizens to construct profiles for them in an attempt to measure their loyalty to the regime. Based on their individual score, they obtain some privileges or lose them. The construction of the profiles happens through the collection of information from the Chinese social media monopolist – WeChat. Since it combines a multitude of functions available to its users, it also offers the government quick and easy access to numerous spheres of the private life of its citizens. Unlike the goals pursued by companies and governments in democracies, the target of the Chinese government is to retain control over its population, preserve the status-quo, and motivate its citizens to be obedient to the regime's values and priorities.

In democratic countries, the goal of collecting information from the users is a more complex phenomenon. First, very often the users do not know that they are being surveilled and profiled. Second, the desired objective in collection-of-information campaigns through social platforms and Internet of Things (IoT) devices is to sell the information to interested parties that will then convey messages to targeted groups. The aim of the delivered message is to manipulate people to undertake certain actions or abstain from such. The mechanisms through which the manipulation is executed is psychological in nature – through the exploitation of cognitive vulnerabilities of the human mind. In authoritarian countries, the regime does not hide the close observance of its people and their private information because they have little power to protest this action. Contrary to this practice, in democracies, companies, politicians and organizations, while having enormous power concentrated in their hands, are still liable to lawsuits, protests, or missing election or re-election opportunities. Thus, the collection and dissemination of personal information of users is a covert operation that in many cases is either on the borderline of being illegal or is simply illegal. Interestingly, even if users are presented with a statement announcing how their information will be used, they never have the option to continue using the social platform without having to authorize their information to be used in the way described in the statement. Consequently, the addictive nature of social media including peer pressure and suppressing concerns about privacy make users more inclined to share their personal information. One study found that if it "is generously provided, limiting privacy preferences are hardly used; only a small number of members change the default privacy preferences, which are set to maximize the visibility of users profiles"[300]. In addition to this, the literature on privacy in social media confirms that "social engineering is a well-known practice in computer security to obtain confidential information by manipulating legitimate users"[301].

[300] Ralph Gross and Alessandro Acquisti, "Information revelation and privacy in online social networks" (paper presented at the Proceedings of the 2005 ACM workshop on Privacy in the electronic society, 2005), 79.
[301] Ibid.

Similar to disinformation, this type of cognitive threat is also combatted through three different methods – educational, technical and legal[302]. The first one is intended to limit the amount of information that users share voluntarily on social media, the second seeks to encourage social media themselves to give their users more control over their own information online, and the third mechanism pertains to legislative solutions to the subject matter. The first two are in direct conflict with the need of individuals to share information and the need to make it visible. The third mechanism is in nature deterring than confronting an already emerged problem. While education and technical solutions are helpful, if the entire issue of stealing personal information is not addressed, social media will keep collecting and selling data to interested parties as long as users post it. Moreover, educating users about the risks of sharing personal information cannot guarantee sharing will not occur since it is, after all, a personal choice. As for companies forced to provide more freedom to users to control their accounts and the access to them there are two relevant factors. On the one hand, companies are not interested in doing so because if the sharing goes down so will their profits, and on the other, even if users are given more freedom to control how their information is seen and used, this does not mean that they will exercise their newly gained rights. The latter is confirmed by a study on Facebook users' use of privacy settings[303] that showed that 80% of the participants know that they could use privacy setting and gain better control over the information and yet only 40% of them decided to take advantage of this feature. As similar results were demonstrated by other studies,

[302] Susan B. Barnes, "A privacy paradox: Social networking in the United States," *First Monday* 11, no. 9 (2006).
[303] Tabreez Govani and Harriet Pashley, "Student awareness of the privacy implications when using Facebook," *Carnegie Mellon University* (2005).

researchers concluded that “the gratifications of using Facebook tend to outweigh the perceived threats to privacy”[304].

This chapter outlined various mechanisms for intelligence-gathering, deception and persuasion. All of them continued their existence in later historical periods, but within different conditions, some of which facilitated the proliferation of cognitive threats even more. Deception by infiltrating a particular group through a shared identity, known in the early ages through the cases of fake deserters, still exist nowadays in the form of traditional espionage and even through social media posts that are not shared by an individual but an entity with political interests, disguised as a person. As an antidote to disinformation, much like in the antiquity, fact-checking is still an available tool to people but difficult to be used – in the past, because of the lack of sources, and in present days, because of the presence of too many sources. The medieval informants offering their persuasion and intelligence-gathering skills for remuneration and power resemble closely the companies hired by politicians to collect intelligence to profile and then influence voters. The role of women also grew gradually through the ages as it is preserved nowadays through the presence of many female spies, and many female recruiters and influencers. Once difficult, falsification of official documents and correspondence became easy with the creation of *black chambers* and even easier with the digitalization and transparency of information in democratic countries. The digital information was manipulated and distributed even faster than in the *black chambers* due to technological innovations and democratization. In the post-modernism, the distribution of power was increasingly in the hands of the individuals, part of a democratic political entity. The lack of established diplomatic relations between countries, laws and regulations governing those between state and non-state entities and

[304] Bernhard Debatin et al., "Facebook and online privacy: Attitudes, behaviors, and unintended consequences," *Journal of computer-mediated communication* 15, no. 1 (2009): 103.

individuals made deterrence tactics weaker in previous historical periods but a stronger opportunity in present days. Innovations were growing in number but so are threats as well. The high cost of wars made entities reluctant to pursue this option and turned to something that remained mostly unregulated by states as a battlefield – the human mind. The only possible way for cognitive threats to fail was for the perpetrator to discontinue pursuing them, or the victim, being aware of the threat, to catch them in time, before any harmful consequences appear. Is this possible to be achieved? In the next chapter, I explore four case studies with cognitive threats in an effort to outline the reasons for their success. Then, in Chapter 5, I propose strategies to neutralize these conditions and prevent the cognitive attack through deterrence and prevention tactics.

CHAPTER 4

THE FOUR HORSEMEN OF THE COGNITIVE APOCALYPSE

Stories about cognitive threats

In this section, I will present four case studies that will help tailor a strategy for countering cognitive threats in the 21st century. The selection of these cases was made on the principle of their notoriety in media and in the scholarship, and their recognition by both fields as a serious problem that has to be addressed. In addition, newer cases were preferred over older ones, as brief overviews of the latter are an integral part of the context of the former. I chose four case studies from the past ten years (2009-2019) that all share the main characteristics of cognitive threats and yet, they are different because they were executed in variety of ways. Their divergent characteristics will be elucidated through the case studies as this will contribute to a more detailed strategy that covers more than just one type of cognitive threats. All case studies represent attacks against individuals primarily. On a broader level, through such persuasion tactics used against individuals, these attacks aim to disrupt state and non-state entities as targets as well. The case studies do not focus only on one country but strive to exemplify the diversity of affected parties. The only exception is the traditional espionage case that was solely directed toward the U.S. and other U.S. non-state actors. This case was nevertheless chosen despite the fact that represents a threat against only one state and its non-state actors because the nature of this kind of espionage imposes a limit of the potential actors against which it could be exercised. Regardless, it is an important cognitive threat that has to be analyzed as it is also one of the oldest types that are recorded in the history of humanity.

In the literature, the type of cognitive threats that enjoys most of the scholarly attention is disinformation and the recruitment of people for radical organizations. However, as described previously, the deterrence techniques aimed to eliminate these threats are so far with limited success. While disinformation is an important cognitive threat, it is not the only one. Much less attention is paid to the oldest type of cognitive threats – the one involving espionage, conspiracies, and manipulations, as well as to the newest cognitive threat – stealing personal information and treating it as a tradable product. A product used as a weapon for persuasion.

In Chapter 3, I present the cases of Maria Butina, Russian disinformation, ISIS recruitment, and Cambridge Analytica as they were described by the media, state agencies, and the scholarship. This I do to introduce the cluster of facts that comprise them and to explore their impact on what happened. I begin every case study with background information that will place a particular case in a context hence connecting it to other similar cases and underlining the continuity in the history of cognitive threats. Further, I make an overview of the case as it was reported by a number of resources, both private and state ones. Next, I track what measures were undertaken against this threat and how the cases developed further after the damages were inflicted.

The case with Maria Butina

Background. On July 15, 2018, Maria Butina was arrested in Washington, DC on allegations of being a Russian spy. In December 2018, she pleaded guilty on charges of conspiracy to act as an agent of the Russian Federation without prior notification to the Attorney General[305]. She admitted she conspired together with Alexander Torshin, her political mentor,

[305] Department of Justice, "Russian National Charged in Conspiracy to Act as an Agent of the Russian Federation Within the United States,", 2018.

and her boyfriend Paul Erickson, a gun activist with close ties to National Rifle Association (NRA). Butina's alleged handler in Russia – Alexander Torshin, who was not named in most of the court documents on Butina's case became a person of interest of the U.S. Department of the Treasury even before her arrest. On April 6, 2018, the U.S. Department of Treasury's Office of Foreign Assets Control (OFAC) designated Torshin as one of the Russian government officials against whom the U.S. adopted sanctions through the Countering America's Adversaries Through Sanctions Act (CAATSA)[306]. On February 7, 2019, Paul Erickson was indicted by a federal grand jury for money laundering and wire fraud[307]. While these charges were not directly related to Butina's conspiracy case, it was evident that she had some role in his allegations as well as he had in hers.

While this case may seem shocking for the 21st century where everything is digital, anonymous and the attribution dilemma makes it easy for attackers to hide their actions, it was not even the first case of this kind in the past 20 years. In fact, in 2010, an operation called the "Illegals Program" concluded with the arrest of ten individuals accused of being unregistered agents of the Russian Federation[308]. These Russian undercover operatives called *illegals* "spent time—sometimes for an extended period—living in the target environment and becoming accustomed to their new surroundings, testing their new identities, and perfecting cover stories. This time helped them melt into the background and ensure that they could perform their intelligence mission without raising suspicion. They further 'legalized' themselves by receiving local identification documents, obtaining local employment, and stabilizing their living

[306] U.S. Department of the Treasury, "Treasury Designates Russian Oligarchs, Officials, and Entities in Response to Worldwide Malign Activity ", 2018.

[307] Department of Justice, "Sioux Falls Man Charged with Wire Fraud and Money Laundering,", 2019.

[308] "Ten Alleged Secret Agents Arrested in the United States,", 2010.

situation"[309]. Then the actual collection of intelligence began, as they regularly conveyed it to their Russian handlers through "wireless hotspots to pair directly with another laptop and communicate information point-to-point" and "steganography to hide sensitive data inconspicuously in digital images"[310]. Among the intelligence gathering tasks, other missions assigned by the Russian officials also included sabotage operations as well[311].

One of these ten Russian *illegals* was Anna Chapman – a Russian agent whose story became especially popular in the U.S. media. Married to the U.K. citizen Alex Chapman, Anna Chapman is a Russian national, born in Stalingrad (nowadays Volgograd) in the family of the former KGB agent (later a diplomat in Kenya) Vasily Kushchenko. After her marriage, she also received a British passport, which citizenship is later revoked by the U.K. after she got exposed and deported to Russia. Alex Chapman later confirmed that at the time at which they were still living in London, Anna began meeting with Russians and became very private with her affairs. It is reported that after a trip back to Russia, and despite her previously stated dislike for Americans, she suddenly expressed her wish to move to the U.S. where after a few financially difficult years with her new business, the latter started to flourish, and her living standard changed sensibly[312]. During her time in New York, she was caught communicating with her Russian handler. The FBI suspected that she was supposed to infiltrate the political circles in the U.S. Soon after that, Russia and the U.S. made a deal to mutually exchange intelligence operatives in 2010 and among other Russian agents, Anna was also on her way to Russia. Warmly welcomed by President Putin, Anna was offered a position as the leader of the youth

[309] Kevin Riehle and Michael May, "Human-cyber Nexus: the parallels between 'illegal'intelligence operations and advanced persistent threats," *Intelligence and National Security* 34, no. 2 (2019): 7.
[310] Ibid., 8.
[311] Ibid.
[312] Stephen Adams, Andy Bloxham, and Gordon Rayner, "Anna Chapman: profile of a 'Russian spy'," *The Telegraph* 2010.

wing of Putin's political party[313]. When asked about her time in the U.S., however, she remains silent stating that she is not allowed to discuss it, allegedly told so by her handlers in Russia[314].

While the aforementioned cases only outline the features of Russia as a political competitor sending undercover agents in the U.S., the Kremlin is not the only government doing so. Other states that are America's political and/or economic rivals have been continuously using foreign students as intelligence-gatherers. Joseph Augustyn, a former director of the CIA's Defector Operations Center, asserts that "Chinese security officials meet with many of their students before they go abroad to study, and in certain cases debrief them on return"[315]. Foreign students are not the only ones who act as spies for their countries of origin, however. A substantial amount of the individuals who are accused of theft of secrets in relation to their employment is from China - 84% of the foreign perpetrators of theft of secrets are Chinese citizens, according to a study that incorporated data from Department of Justice between 2009 and 2017[316]. However, espionage, defined as "the unauthorized international collection of information by states"[317] in the case of Maria Butina, differs quite significantly from the corporate espionage inherent for Chinese citizens working for the Chinese government. Legally, even corporate espionage is not as easy to be proven because there has to be a link to the government that allegedly ordered the illicit activity. However, in the case of corporate espionage, there is a second option for the offenders to be brought to justice – the theft of secrets in which the only element that has to be beyond doubt is the unpermitted possession of certain information, it, being either a physical or digital copy. That said the case of Maria Butina

[313] Marc Bennetts, "Anna Chapman: Agent provocateur " *The Guardian* 2011.
[314] Christopher Sultan, "Russian Spy Anna Chapman Finds Celebrity at Home," *Spiegel* 2010.
[315] Joseph Augustyn, "Maria Butina Is Not Unique," *The Atlantic* 2019.
[316] Lora Hadzhidimova and Brian K. Payne, "The profile of the international cyber offender in the US," *International Journal of Cybersecurity Intelligence & Cybercrime* 2, no. 1 (2019).
[317] Darien Pun, "Rethinking espionage in the modern era," *Chi. J. Int'l L.* 18 (2017).

presents a lot more complexity and vagueness because at first glance she did everything, according to the laws. She entered the U.S. with a valid visa, attended meetings and conventions organized by an organization of which she is a member, then she became a foreign student in a prestigious university from which she later successfully obtained a degree. The harmful effect, in this case, is the influence that she wanted to exercise but also another component – the fact that she was able to exercise it due to her connections. Mainly this influence is what distinguishes cognitive threats of this kind from other types of espionage and makes it a century-long political practice with notable consequences.

The thin line between legal and illegal influence in the context of espionage is demonstrated once again in a more recent case in which there is only the suspicion for possible espionage but no concrete proof for anything further. The daughter of Putin's spokesman Dmitry Peskov – Elizaveta Peskova began in November 2018 her internship in the European Parliament with the French right-wing member Aymeric Chauprade[318]. It is claimed that Elizaveta, a law student in Paris, does not have access to any confidential information but only to publicly accessible one. Regardless, as a former adviser of Marine Le Pen, Chauprade is a vivid supporter of the Russian annexation of Crimea. Furthermore, he is currently serving as a member of the EU Parliament's Security and Defense subcommittee and in this capacity he has access to very important documents that could be classified on different levels of security. Unlike the North Atlantic Treaty Organization (NATO), the European Union does not screen interns and does not require them to obtain a security clearance before beginning the internship. Regarding Peskova's internship, there was an expressed concern that the European Parliament elections in May 2019 may be compromised by Russia[319].

[318] "Putin spokesman Peskov's daughter working as E.U. intern," *BBC* 2019.
[319] Ibid.

From the reports compiled during the years about Russian access-agents and spies, it becomes evident that they sometimes act as *sleeping cells* but get active when a specific task had to be accomplished. For years, Maria Butina's case was allegedly building the foundations of a more significant project that aimed to establish communication between certain circles of American political life and Moscow. However, while not charged directly with interference in the U.S. Presidential Elections in 2016, it was established in court that she was receiving orders from her handler Torshin in Russia even on the election night[320]. In her plea agreement, there are no details about her possible mission to influence the elections, but another case in which 12 Russians were accused of hacking accounts of Democratic Party members brings some context to her case as well. While there was a lot of tension surrounding the U.S. Presidential Elections in 2016, for some amount of time, concrete accusations were not made until on July 13, 2018, the U.S. Department of Justice (DOJ) officially announced charges pressed against 12 Russians accused of hacking members of the Democratic Party[321]. These 12 Russian individuals were agents working for the intelligence unit of the Russian military division. The indictment released against them states that they acquired usernames and passwords of various representatives affiliated with the Democratic Party, hacked their accounts and obtained information that was later posted on personal blogs and websites that supposedly belonged to "American hacktivists"[322]. All of those acts were committed with the intention of interfering with the Presidential Elections, according to the DOJ press release. Days after the indictment, Maria

[320] Kara Scannell, Sara Murray, and Mary Ilyushina, "The Russian accused of using sex, lies and guns to infiltrate U.S. politics," *CNN* 2018.

[321] "Russian woman charged with spying in the U.S.," *BBC* 2018.

[322] Department of Justice, "Grand Jury Indicts 12 Russian Intelligence Officers for Hacking Offenses Related to the 2016 Election,", 2018.

Butina gets arrested for her role in a conspiracy to act as an agent of the Russian Federation within the United States without prior notification to the Attorney General.

Overview. Born in 1988 in Siberia, Russia, Maria Butina becomes one of the most controversial figures of contemporary espionage. At an early age, she was introduced to guns, claiming later for an interview in 2015: "For such places like Siberia or forests of Russia, this is question of survival. Everyone has a gun"[323]. Her early interest in guns evolves into a passion that will affiliate her with many powerful circles both in Russia and in the U.S. In Altai State University, she studied political science and education and joined Vladimir Putin's party – United Russia. Later, she obtained a master's degree as well. She also established an organization called *The Right to Bear Arms* that "called for the sale of short-barrelled firearms to civilians to be made legal"[324]. Despite some resistance by the opposition in Russia, this movement quickly developed and added new members, one of which was Alexander Torshin – a high-ranked official in the Russian Central Bank and a member of the Russian Council Federation. Mainly this relationship will later be one of the most significant reasons for the charges pressed against both. It is reported that Alexander Torshin became a mentor for Maria Butina, encouraging and supporting her political career and sharing her passion for guns. Butina expressed in an interview for a Russian website that she dreams "to live in a prosperous, highly developed country, leading in the world, and without immigration"[325]. She appreciates Torshin's advocacy for her cause that is to "advance Moscow's long-term strategic objectives"[326]. Torshin is also a lifetime member of the NRA, as well as Maria Butina who joined in 2012. Interestingly, before 2013, Butina was refused a visa to go to the annual NRA meetings multiple times,

[323] Scannell, Murray, and Ilyushina, "The Russian accused of using sex, lies and guns to infiltrate U.S. politics."
[324] "Maria Butina: Russian gun activist in U.S. conspiracy case," *BBC* 2018.
[325] Ibid.
[326] Jake Rudnitsky and Evgenia Pismennaya, "NRA-Linked Russia Central Banker Retires," *Bloomberg* 2018.

according to CNN[327]. After joining NRA in a member capacity, she began traveling to the U.S. Prosecutors in her case claim that a Russian oligarch who paid for one of her visits after obtaining a visa told her: “I want you to go work with the US, not go on a tourist trip”[328].

In 2018, it is documented that Butina and Torshin organized a delegation to the National Prayer Breakfast in Washington, DC where Torshin requested a meeting with President Trump which did not take place after all. However, Torshin previously admitted that he had met President Trump in the past at annual meetings of the NRA. At the same time, Butina was also active in her intentions to establish connections with U.S. governmental officials. In 2015, at an event held by Donald Trump in Las Vegas, she inquired about his stance on the financial sanctions imposed on Russia[329]. Her next step, with the help of Torshin, was to organize a delegation from NRA representatives to travel to Russia for a meeting with influential members of the Russian political elite. While there is some controversy surrounding the attendance of the then-NRA president, Alan Cors, to the meeting, he decided not to go so that this is not viewed as an official NRA meeting with Russian government officials. Even without his presence in Moscow, the meeting took place. This made various Democrats hesitant about the NRA’s relationship with Russia. When the former asked the NRA if they have used any funds by foreign governments to support Trump’s presidential campaign, the association said it did not[330]. Regardless, they admitted that they receive money from foreign donors, thus suggesting that NRA may have been sponsored by Russian oligarchs or directly by the Kremlin itself through intermediaries.

[327] Scannell, Murray, and Ilyushina, "The Russian accused of using sex, lies and guns to infiltrate U.S. politics."

[328] Ibid.

[329] "Maria Butina: Russian gun activist in U.S. conspiracy case."

[330] Clare Foran, Sara Murray, and Jessica Schneider, "Democratic lawmakers ask NRA for answers over 2015 Moscow trip and alleged Russian ties," *CNN* 2019.

Not long after the Moscow meeting, Butina traveled to the U.S. to pursue a master’s degree in the American University in Washington, DC. Her presence in the U.S. also allowed her to be closer to her boyfriend - Paul Erickson – a 56-year-old supporter of the Republican Party and NRA - with whom, supposedly, she was preparing to move in South Dakota before her and Erickson’s arrests. The couple met in Moscow in 2013, as Erickson and the president of NRA at the time David Keene traveled there to meet with Butina - the young activist behind *The Right To Bear Arms*. After officially becoming a couple, Butina frequently traveled to the U.S. to see Erickson, where she was introduced by him to powerful members of the gun-lobby at conferences and other events[331]. At the time, Erickson, in his role of an NRA supporter, volunteered on multiple occasions, according to reports, to establish connections between Trump’s campaign managers and members of the Russian government[332]. There was a note, found in Erickson’s home that was asking the question “How to respond to FSB offer of employment?”, suggesting that FSB either made or may have made a possible offer to Erickson to work for them in some capacity. During Butina’s trial, it was argued that her relationship with Erickson was merely a means to achieving Butina’s and Torshin’s goals of obtaining access to conservative politicians and activists in the U.S. – something that both have sought to accomplish during the years of their acquaintance. In the allegedly unrelated charges of wire fraud and money laundering pressed against Erickson, there were a few transactions in which Butina’s name was involved. Court documents show that he made a payment to the American University, supposedly for Butina’s tuition and another transaction of $9000 to a person with

[331] Pete Madden, Matthew Mosk, and Kyra Phillips, "Lover or cover? Maria Butina and the romance at the heart of an alleged Russian influence operation," *ABC News* 2018.

[332] Carrie Johnson, "Paul Erickson, Boyfriend Of Russian Agent Maria Butina, Charged In Fraud Scheme," *NPR* 2019.

initials *M.B.*[333]. While being in the U.S., Butina did not cease her communications with Moscow. One message via Twitter revealed that the Russian government official with whom Butina was in touch assured her of her talent and skills: "Your political star has risen in the sky. Now it is important to rise to the zenith and not burn out (fall) prematurely"[334]. In addition, she allegedly shared with an American politician/activist that she had Moscow's approval to organize dinners at which conservative members of the gun lobby will be invited, thus underlining the official support for this "communication channel"[335]. In 2018, this task was becoming harder and harder as her name appeared in media, connecting her to American politicians and NRA lobbyists, attracting suspicion and mistrust to her intentions. She started expressing concerns about returning to Russia, stating that she may not be safe there anymore[336]. Regarding Butina's unusually good ties to Capitol Hill, her mentor, and alleged handler, Torshin noted that she had "upstaged Anna Chapman"[337].

Applied measures against this threat. Maria Butina was arrested in April 2018 and moved to an adult detention facility in Alexandria, VA. She spent most of her time in Washington, DC and in Alexandria, VA in solitary confinement for a total of 67 days. On December 6, 2018, Butina and her lawyers were presented with a plea offer according to which she will admit she was involved in a conspiracy as a foreign agent without the proper registration with the U.S. Such crime carries a maximum of five years imprisonment and a fine of $250,000, and a supervised release up to three years. In exchange for the guilty plea, the prosecution on the case will not further prosecute the case. The recommended sentence in the plea deal is 0-6

[333] Kate Sullivan and Sara Murray, "Political operative who was dating alleged Russian spy Maria Butina indicted," *CNN* 2019.
[334] "Russian woman charged with spying in the U.S.,"
[335] Scannell, Murray, and Ilyushina, "The Russian accused of using sex, lies and guns to infiltrate U.S. politics."
[336] Ibid.
[337] Ibid.

months of imprisonment (which Butina had almost already spent in detention facilities) and a fine ranging from $500 to $9,500 considering that she does not have any prior offenses[338]. Following these guidelines, and as a non-U.S. citizen Butina, agreeing to plead guilty becomes a subject of removal proceedings and deportation. On December 8, 2018, Butina and her lawyers accepted the deal offered by the prosecution that confirms multiple examples of her communication of Alexander Torshin, who remained unnamed but described in a way that leaves no doubt that he is the man in question. The communication, mostly in the form of text messages shows that Butina was indeed intending to not only influence NRA (named simply *Gun Rights Organization* in the plea offer[339]) but to later benefit from establishing a channel of communication with Russia. In addition to any other details specified by the plea agreement, Butina also agreed to cooperate with authorities requesting her assistance. She was questioned by the special counsel investigating the interference in the 2016 U.S. Presidential Elections. However, Butina's cooperation was predominantly focused on the case that the U.S. Attorney's office is preparing for her boyfriend – Paul Erickson[340]. Because of Butina's requested assistance on other cases, her sentencing has been delayed – a fact that will make her sentenced to time served most likely if the judge agrees and confirms the sentence recommended by the prosecution.

As for Paul Erickson, while his name does not appear concretely on the plea agreement as an accomplice in the conspiracy, it is apparent that the prosecution envisions him in particular when documenting Butina's actions in the U.S. However, he has not been accused of any other crimes different than wire fraud and money laundering so far. In the meantime, Alexander

[338] United States Attorney Jessie K. Liu, "United States v. Mariia Butina," ed. U.S. Department of Justice (Washington, DC 2018).
[339] Ibid.
[340] Sara Murray, "Special counsel briefly interviewed Maria Butina, sources say," *CNN* 2019.

Torshin, the other unnamed individual that appears by description in Butina's plea agreement only suffered financial sanctions from the U.S. but has not been so far accused of any crimes regarding Butina's case.

The measures that the U.S. has undertaken so far are mostly legal in nature. Even these measures were first challenging to be applied because influence is a psychological category rather than a material one and as such it could not be easily identified. Maria Butina was accused of operating as an unregistered foreign agent mainly because there were no other legal grounds to charge her with any other crime – she was traveling to the U.S. with a valid tourist visa to gun-lobby conferences, after which she obtained a student visa for an education that she in fact finished. Contemporary law is not evolved enough to encompass modern threats to liberal societies such as persuasion. It is very difficult to draw a line between legal persuasion that the law allows, and illegal persuasion that constitutes a crime. Especially in the legislature about espionage, such offenses are political and as such are described more vaguely than others. They could include many different behaviors when placed in different contexts. As for the implications of using legal deterrence against espionage, after the swap of agents between the U.S. and the Russian Federation in Vienna, one of the returned captives – Anna Chapman was welcomed as a hero in her home country. After her arrival, she was offered a job and enjoyed status of a celebrity. That said, if Maria Butina returns to Russia which is more than likely since she will get deported after she serves her sentence, she may share a similar destiny as her intelligence-gathering predecessor Anna Chapman. The deterrence effect that legal measures have in her case is limited. The sentences themselves are typically very short if there are no prior offenses and upon return to Russia, the former agents enjoy Putin's recognition and support in their future endeavors. As for the preventative role that a guilty plea has in the context of politics, it also does not have a significant role since the agents may be linked to Russian politicians, oligarchs, and even government officials but it could not be proven legally that there is an intentional state-supported espionage campaign against the U.S. Furthermore, even if the captured Russian agents give away the names of other operatives, there will be just more sent to replace the ones whose real intentions and missions were exposed.

The case with Russian Disinformation

Background. In an essay about the Russian (Soviet) disinformation, Herbert Romerstein[341] writes that as early as in 1972, archives show, that there was a special KGB handbook that contained instructions for disinformation campaigns aiming to produce certain impressions about reality, in the enemy's mind, in order to provoke them to derive favorable to the Russian goals, conclusions about facts. Evidence also testifies that within these campaigns, there were not only guidelines to disseminate disinformation to vilify and discredit the adversary but also to exercise influence over them in any other possible way.

In order to explain how Russian disinformation works, first, a proper definition for it has to be introduced. To begin with, disinformation should be distinguished from another phenomenon - misinformation. Misinformation is defined in the literature as an unintentional presentation of wrongful information, according to an agreed-upon perception of truth. Contrary to this, disinformation stems from incorrectly stated source or from an unreliable one and affects the legitimacy of the information in a purposeful and anticipated manner. Disinformation practices aim to manipulate the recipient of the message, to provoke them to change their attitude

[341] Herbert Romerstein, "Disinformation as a KGB Weapon in the Cold War," *Journal of Intelligence History* 1, no. 1 (2001).

in a certain way[342]. From a social psychological standpoint, disinformation and any type of propaganda represent “techniques which induce the individual to follow non-rational emotional drives”[343]. They include, first, outreach to the collective and individual entities, second, an appeal for identification with the group identity that resists an alleged enemy, and third, they seek to conceal the sender of the message as much as possible. That said, only disinformation could pursue political gains since misinformation is not a deliberate but rather unintentional misrepresentation of information. It is a non-purposeful, erroneous portrayal of facts. While difficult to prove, the intent to mislead, in the case of disinformation, could be reasonably traced, through three mechanisms: the authenticity of the presented facts, the level of impartiality of the reporting style, and the legitimacy of the sources of the reported information[344].

According to its purpose, the disinformation could be divided into two types: *agitative*, that evokes active behavior and *integrative*, inviting the addressee to get a passive stance about an issue[345]. The former aspect finds expression frequently in the form of an appeal to public opinion which causes political tensions leading to the allegedly logical solution to just follow the leaders[346]. The integrative propaganda, on the other hand, seeks “bringing the scattered members or parts of a particular thing (being) into a harmonious whole”[347]. Further juxtapositions could be made based on the content and the source of the disinformation that identify white, black and grey propaganda[348]. The white propaganda reveals an accurate disclosure of the source of

[342] Miroslav Tudjman and Nives Mikelic, "Information science: Science about information, misinformation and disinformation," *Proceedings of Informing Science+ Information Technology Education* (2003).
[343] William W. Biddle, "A psychological definition of propaganda," *The Journal of Abnormal and Social Psychology* 26, no. 3 (1931): 294.
[344] Ben Nimmo, "Identifying disinformation: an ABC. Policy Brief Issue 2016/01-February 2016," in *Archives of European Integration (AEI)*, ed. Institute for European Studies (IES) (2016).
[345] Garth S. Jowett and Victoria O'Donnell, *Propaganda & persuasion* (Sage Publications, 2014).
[346] Jacques Ellul, *False presence of the kingdom* (Seabury Press, 1972).
[347] Geoffrey O. Ozumba, "National consciousness, value reorientation and identity: An Integrative Humanist Approach," *Journal of Integrative Humanism* 3, no. 2 (2014): 152.
[348] Jowett and O'Donnell, *Propaganda & persuasion*.

otherwise reliable information, but the content is still subjectively represented in a way to convince the addressee of a particular idea. A relevant example in this regard is the propaganda shaped by the use of patriotic statements. Black propaganda is described as a type of information “concealed or credited to a false authority and spread lies, fabrications and deceptions”[349]. As opposed to this, the grey propaganda does not have a clearly identified source which makes room for doubts about the authenticity of the reported information[350].

One of the most vivid examples of a disinformation campaign is undoubtedly the period of the Cold War. Regardless of its end, however, such practices are still actively employed by Russia in the post-Cold War era even more with the presence of digital technologies that could easily disperse the propaganda message to broader audiences. In the years after 1989, Russia aimed to maximize its soft-power through defensive strategies and the power of persuasion about the positive sides of Russian culture. In 2009, a new mechanism pursuing offensive rather than defensive soft-power was enabled by the Russian TV-station Russia Today (RT)[351]. Along with this focal point, the Russian cyber-propaganda became a very active weapon in the hybrid war against the West and some former Soviet countries that lean toward the Western cultural and economic model[352]. The 21st-century Russian disinformation could be perceived as a continuation of the Soviet media’s propaganda but adapted to the new information age in a *neo-Soviet* manner[353]. These modifications include a heavy reliance on *active measures* such as

[349] Ibid., 17.
[350] Dave Gelders and Øyvind Ihlen, "Government communication about potential policies: Public relations, propaganda or both?," *Public Relations Review* 36, no. 1 (2010).
[351] Marcel H. Van Herpen, *Putin's Propaganda Machine: Soft Power and Russian Foreign Policy* (Rowman & Littlefield, 2015).
[352] Sascha Dov Bachmann and Hakan Gunneriusson, "Hybrid Wars: The 21st-Century’s New Threats to Global Peace and Security," *Scientia Militaria, South African Journal of Military Studies* 43, no. 1 (2015).
[353] Sarah Oates, "The neo-Soviet model of the media," *Europe-Asia Studies* 59, no. 8 (2007).

intentional placement of strategic content, disinformation, and exercising tactics of influence by public figures enjoying popularity and trust[354].

Considering this historical context, the main mission of contemporary Russian disinformation is to undermine Western ideology and to strengthen Russia's positions as a cultural, religious and political hegemon through the tools of offensive soft-power. More concretely, the Russia-supported project, *Eurasianism*, as opposed to *Westernization*, has a few distinctive features, according to Aleksandr Dugin, the creator of this strategic vision[355]. First, Eastern civilization does not recognize the liberal values as its intrinsic mindset. Second, the state's goals should be located above liberal values in the hierarchy of social interests. Third, Russia is a defender of traditional values that are in dissonance with many of the new, Western liberal principles. Fourth, the U.S. is the enemy that stays in the way of the Eurasian project. Fifth, the Eurasian project should be embracing the former Soviet states along with states that reach Central and West Asian territories. In that sense, what would be the strategic mechanisms for fulfilling this agenda and why have they been successful? Van Herpen[356] claims that among the instruments of Russian influence are: direct and indirect distribution of state propaganda to the West; change of ownership of Western media companies in favor of Russian businessmen; establishing new social networks and websites that spread messages favorable to the Kremlin; intensive posting in blogs and forums as well as *trolling* content undermining Russia or its interests; subsidizing political parties and political figures; re-installing espionage practices; and assigning the Russian Orthodox Church a vital role as a promoter of soft-power.

[354] Steve Abrams, "Beyond propaganda: Soviet active measures in Putin's Russia," *Connections: The Quarterly Journal* 15, no. 1 (2016).
[355] John Lough et al., "Russian influence abroad: Non-state actors and propaganda," *Chatham House* 24 (2014).
[356] Van Herpen, *Putin's Propaganda Machine: Soft Power and Russian Foreign Policy*.

As for the success of the tools used to disseminate propaganda, Bjola and Pamment[357] explain why such campaigns enjoy fruitful results in many countries. The authors stress three main strategies used to accomplish this goal: 1) “the efforts to exploit differences between EU media systems (strategic asymmetry)”[358], 2) “the targeting of disenfranchised or vulnerable audiences (tactical flexibility)”[359], and 3) “the ability to mask the sources of disinformation (plausible deniability)”[360]. In addition, some authors[361] point to the high number of sources that distribute particular news containing disinformation, the alleged diversity of the sources and the repetitiveness of the message itself, as well as the community of people that have similar beliefs to the author of the propaganda message which helps spread the news even further. As for the perceptual mechanisms that increase the trustworthiness of the disinformation message, it is the familiar appeal of the message and not the reliability of the information that attracts the audience. Furthermore, readers look for evidence supporting the presented information and evaluate it as being true if they find any, even if the evidence is fraudulent.

Another element contributing to the triumph of disinformation in the digital age is the presence of online trolls. Their primary function is “twisting and manipulating the public debate”[362] and engaging in harassment of users that express anti-Russian standpoints. The *Kremlin School of Bloggers* was, in fact, a project intended to undermine critics of the Kremlin, oppose anti-Russian content online and post messages and videos supporting Russian policies and interests. The Kremlin trolls are supposedly contributing on average “50 news articles daily

[357] Corneliu Bjola and James Pamment, "Digital containment: Revisiting containment strategy in the digital age," *Global Affairs* 2, no. 2 (2016).
[358] Ibid., 131.
[359] Ibid.
[360] Ibid.
[361] Christopher Paul and Miriam Matthews, "The Russian “firehose of falsehood” propaganda model," *Rand Corporation* (2016).
[362] Jessikka Aro, "The cyberspace war: propaganda and trolling as warfare tools," *European View* 15, no. 1 (2016): 121.

and maintain six Facebook and ten Twitter accounts, with 50 tweets per day"[363]. In a broader context, in the hybrid war against the West, there is a central place assigned to information as a weapon. However, as opposed to the Cold War type of propaganda that the Soviet Union used, in the 21st century, this propaganda is transformed into information warfare that seeks to achieve goals beyond those of propaganda. These goals assume the use of *spetspropaganda* (special propaganda), a tool that embeds "computer network operations, electronic warfare, psychological operations, and information operations"[364]. As opposed to the old goals of propaganda that aimed to attract social perceivers to the Soviet ideology, the ultimate goal of the new Russian strategy after the fall of the Soviet Union is instead, to "plant seeds of doubt and distrust; to confuse, distract, polarize and demoralize"[365].

Overview. While some of the Russian disinformation is focused mostly on particular populations, their campaigns are widely spread even beyond the borders of the European Union, beyond the U.S., beyond continents, cultures, and values. The European External Action Service (EEAS) created a resource called EU vs. Disinformation that tracks disinformation articles, identifies the target audience and provides facts that disprove the misleading information in the original pieces. Archives on this website show that the disinformation wave reached even countries such as Armenia, Azerbaijan, Finland, Moldova, and Serbia. However, the Top 3 countries affected by disinformation campaigns were namely the U.S., Ukraine and the European Union countries[366]. Interestingly, a poll in Russia showed that respondents consider these three countries/entities as its biggest enemies[367]. For the purposes of this overview, in the following

[363] Van Herpen, *Putin's Propaganda Machine: Soft Power and Russian Foreign Policy*, 279.
[364] Michael Connell and Sarah Vogler, "Russia's Approach to Cyber Warfare," ed. Center for Naval Analysis (2017), 3.
[365] Sophia Porotsky, "Social media and the access it provides to voter data give Russian active measures the ability to influence the outcome of an election," *Global Security Review* 2018, The Security Gap, par. 1.
[366] Disinformation Review, "Top 3 targets of disinformation," *EU vs. Disinformation* 2018.
[367] ЛЕВАДА-ЦЕНТР, "Враги России," (2018).

sections, I will only describe the disinformation practices in the three regions where Russian disinformation is most prevalent – the U.S., Ukraine and EU-member states. Though not exhaustive, it will give a representation of the political, psychological and social context of disinformation threats.

Some of the disinformation campaigns could be easily traced back to Russia but others cannot. In fact, some of the disinformation, especially in social networks, is disseminated by users that do not even know that are contributing to someone's political agenda. That is namely what makes disinformation so dangerously powerful and the cognitive threat it represents - so detrimental.

Many were skeptical that the Russian disinformation practices of coercive influence could be successful in the U.S. – there is not any particularly large ethnic or religious minority that Russia can easily appeal to, nor is there any close relationship that could justify potential benevolence of a large amount of U.S. people to Russia. On the contrary, both countries have portrayed each other as *villains* for decades. Yet estimates show that this influence-campaign reached approximately 126 million users[368]. Considering this historical background, it was indeed shocking for many to find out that Russian disinformation had entered the U.S. borders. This campaign overwhelmed the online space with fake news and ads on Facebook "to create chaos, inflame emotions, and polarize a divided public…to discredit Hillary Clinton, whom President Vladimir Putin expected to win the Oval Office"[369]. The various advertisements that Russians bought include pictures promoting anti-Clinton, anti-immigration, anti-Muslim messages and such that directly try to provoke a clash on topics on which public opinion is

[368] Benjamin Jensen, Brandon Valeriano, and Ryan Maness, "Fancy bears and digital trolls: Cyber strategy with a Russian twist," *Journal of Strategic Studies* 42, no. 2 (2019).

[369] James P. Farwell, "Countering Russian Meddling in US Political Processes," *Parameters* 48, no. 1 (2018): 37.

strongly divided (e.g., Confederate flags, police brutality, and the Black Lives Matter movement)[370]. The disinformation was in these cases mixed with strong messages seeking to influence the social perceivers in a certain way. Among all online media, Facebook and Twitter appeared to be a central arena for the disinformation campaigns in the 2016 U.S. Presidential Elections. The majority of websites reporting false information was housed by Facebook and used as a *political clickbait*[371]. Facebook was also the generator of more partisan propaganda and disinformation than Twitter and other websites. The highly partisan-charged content is also described as “the principal incubator and disseminator of disinformation – and Facebook-empowered hyperpartisan political clickbait sites played a much greater role on the right than on the left”[372]. That said it was established that both sides of the political spectrum were using such strategies to engage their already committed voters and gain new ones.

Through circles of allegedly different networks, the same political narrative was distributed, confirmed and validated to feed into the agenda of either the left or the right. As Facebook contributed significantly to the success of the disinformation spread, Twitter was also an accomplice but with a different role. Facebook was a fruitful domain for a variety of external websites, but Twitter was a welcoming host to further discussions on political matters presented by Facebook. Twitter enjoyed the attention of a variety of users ranging from the far-left to the far-right. They were not the only ones commenting on popular topics, however. The Kremlin employed numerous trolls and bots who not only increased the popularity and supposedly the attention to a particular issue but also disseminated false information and ungrounded accusations. If the dimensions of the disinformation attacks against the U.S. were only outlined

[370] Scott Shane, "These Are the Ads Russia Bought on Facebook in 2016," *The New York Times* 2017.
[371] Robert Faris et al., "Partisanship, propaganda, and disinformation: Online media and the 2016 US presidential election," ed. Berkman Klein Center for Internet & Society at Harvard University (2017).
[372] Ibid., 19.

by the increasingly populist media and their profiting from sensational headlines, an eventual solution to the problem would have been much easier. However, domestic political trends, values, and interests of various actors in the U.S. matched the Russian ones. And as Moscow's attitude proved on multiple occasions: *The enemy of my enemy is my friend* – a phrase that finds applicability in Russia's support for nationalist and extremist parties whose views contradict those of the traditional political parties. This complicated scenario identifies a few actors and relationships that contribute to disinformation campaigns - first, online media. Second, the catalysts that make online media accessible and even imposed on users (e.g., Facebook, Twitter, Reddit, and Google) and their interest in profiting through their existence. Third, the reputation and the accessibility of established news outlets to readers of all economic backgrounds. Fourth, political actors whose interests match those of Russia in one or more than one area. Fifth, the readers and viewers of information distributed through traditional and online media that increasingly need content clearly defining "winners and losers"[373] and thus validating choices that users make, typically in an effort to reaffirm their identities.

Another political adversary of Russia, and thus a target of fake news and attempts to exercise coercive influence, is Ukraine. The history of Russian disinformation in Ukraine after its independence is most intriguing in the period of the Orange Revolution (2004-2005) during the disturbances surrounding the election of the pro-Russian candidate Viktor Yanukovych, whose victory was claimed to be fraudulent. This particular event marked the beginning of an intensive post-Soviet Union disinformation campaign that coincided with an increase of Internet users particularly of those using social media. At the same time, re-oriented toward a pro-EU

[373] Sarah Oates, "When Media Worlds Collide: Using Media Model Theory to Understand How Russia Spreads Disinformation in the United States," in *American Political Science Association 2018 Annual Meeting, Boston MA* (Boston, MA2018).

path, Ukraine was still struggling with some domestic problems. One of them was the high number of oligarch-owned media. Shortly before the Orange Revolution, a new outlet gained popularity – Channel 5 and rapidly became one of the most reputable sources of information. It is claimed that this channel had an essential role in constructing the narrative that helped Viktor Yushchenko defeat Viktor Yanukovych in the third stage of voting that took place[374]. The medium is currently owned by Petro Poroshenko – Ukraine's president since 2014. This tendency is not rare in post-communist countries, however, and its influence is proven by studies to be decreasing the level of freedom of speech.

In this political climate and skepticism toward the mainstream media, the digital ones emerged as an alternative to the politically tailored by media *truth*. Somewhat instinctively, the people turned eyes toward the digital media as it implied some more objectivity due to the lack of control over the distributed content. During the Orange Revolution in Ukraine, the new online newspaper *Ukrayinska Pravda* accumulated nearly 700,000 new visitors[375] [376]. While true, such digital outlets also have owners and invested interests in the particular representation of facts. Moreover, the effortless dissemination of digital information and the numerous potential addressees of this information made the solution of the old problem – a new problem. In times of societal anxiety caused by popular events, disinformation is used as a weapon mostly because the targets are very vulnerable in their thirst for information. Disinformation is not a new phenomenon, but the digital media with all of their positive sides turned "regular citizens into propaganda machines capable of spreading disinformation, paranoia and hatred"[377]. Moreover,

[374] Ulises A. Mejias and Nikolai E. Vokuev, "Disinformation and the media: the case of Russia and Ukraine," *Media, Culture & Society* 39, no. 7 (2017).
[375] Ibid.
[376] Sergii Leshchenko, "The Media's Role," *Journal of Democracy* 25, no. 3 (2014).
[377] Mejias and Vokuev, "Disinformation and the media: the case of Russia and Ukraine," 1032.

there was another political detail that contributed to the intensified disinformation campaigns. After Yanukovych fled the country, the interim government decided to change the law guaranteeing the Russian language a status of a *regional language*, a law adopted in 2012[378]. This way the Russian-speaking population in Eastern Ukraine was left dissatisfied not only by the turn of events in terms of the president they elected but also in terms of their own language. In this polarized environment in Ukraine, social platforms and online media became outlets for the concerns of a very politically divided population. This politically-divided population believed and was telling different narratives about the events on *Maidan Nezalezhnosti* and what followed after[379]. These narratives were not monochromic though but had many shades as the people supporting them were influenced by different factors – some of them they perceived as true and others as lies – regardless of what was actually accurate and what was a fabrication of the media and the powers behind them.

In the light of these events, the attention to online media did not eliminate the influence of traditional media and the disinformation that it produced. Instead, the disinformation became even stronger as traditional media started referencing and thus confirming false facts from online media and vice versa[380]. This was true for both Russian and Western media. Referring to the quickly escalating situation in Crimea, Western media "claimed that an imminent or actual invasion was under way – 26 completely separate occasion from 2 March to 12 November"[381]. The political environment was so heated at the time that reporting of false news by the West contributed to the spreading cracks of the very fragile peace in the region. Russian

[378] Joseph Laurence Black, "Setting the tone: Misinformation and disinformation from Kyiv, Moscow, Washington and Brussels in 2014," in *The return of the cold war: Ukraine, the west and Russia*, ed. Joseph Laurence Black and Michael Johns (Routledge, 2016).

[379] Ivan Kurilla, "Shaping new narratives: How new histories are created," ibid.

[380] Mejias and Vokuev, "Disinformation and the media: the case of Russia and Ukraine."

[381] Black, "Setting the tone: Misinformation and disinformation from Kyiv, Moscow, Washington and Brussels in 2014," 178.

disinformation campaigns were not lacking either. For this pattern testifies the following case from 2014. The Russian Channel One reported a story of a woman from Slovyansk who was grieving her 3-year-old child who was allegedly killed and “nailed…to a board ‘like Jesus’”[382] by Ukrainian soldiers in order to keep the local population in fear. The authenticity of the story was never confirmed, and no evidence proved that the story was real. However, it first appeared in a blog post of Alexandr Dugin, the ideologue behind the *Eurasianism* project and a vivid supporter of Kremlin’s policies.

In addition to these practices, another tool in the arsenal of disinformation is the intentional misplacing of content. For instance, a picture of a young Syrian boy with an open wound was presented as a boy from the Slovyansk region, allegedly wounded by Ukrainian troops[383]. It was later confirmed that the picture originally appeared in an article about the war in Syria.

Another problem regarding the false information distributed through traditional and digital media are the paid trolls that generate thousands of comments with explicit content – typically confirming the authenticity of an article and expressing outrage or refuting some content that is supportive of ideas and values unfavorable to Russia’s policy. As outlined previously, evidence shows that the *troll factories* not only exist, but verify various speculations surrounding their functions, funding, and overall mission. Infiltrating a troll factory in Russia hidden under the name *Internet Research Agency*, Lyudmila Savchuk admitted that she and her co-workers were supposed to follow guidelines in their postings defaming Ukraine’s pro-

[382] Maria Danilova, "Truth and the Russian media," *Columbia Journalism Review* 2014, par. 2.
[383] Mejias and Vokuev, "Disinformation and the media: the case of Russia and Ukraine."

Western government and condemning the violence that Ukrainian soldiers were allegedly exercising over the population in Eastern Ukraine[384].

Among other reasons, the annexation of Crimea was a result of Moscow's intention to protect its Russian-speaking population, living outside of the Russian Federation's borders. Russia was never hiding its ambition to serve as a leading nation uniting the Slavic countries under its wing. Therefore, similarly to the Russian-speaking population in Crimea, other regions are also hot points of the Russian geopolitical interests. Some of these countries are now part of the EU, others are not. While the EU-alliance has always been seen as a competitor by Russia, the treatment of the countries that sustain it is different. It is evident that while the former Soviet countries that are now part of the EU, and the Western states are all targets of the disinformation campaigns, they are executed very differently due to the way Moscow sees them. The Baltic countries, similarly to the Crimean population have a high number of Russian-speaking population. It is no surprise that the disinformation campaigns there are particularly intensified. In Estonia and Latvia, for instance, they compound more than 25% of the population[385]. The Northeastern region of Estonia with the largest amount of Russian-speaking population is also "significantly less integrated to Estonian society and it is also economically in a poorer state than the Estonian average"[386]. However, if compared to the economic conditions that the same population will be having if potentially this territory becomes Russian, it will turn out that they would be worse off than in the conditions they are living under currently. Despite these reasons, Russia still appeals to the Russian-speaking population in Estonia in numerous ways. As for the

[384] Neil MacFarquhar, "Russian Trolls Were Sloppy, but Indictment Still 'Points at the Kremlin'," *The New York Times* 2018.
[385] Henrik Praks, "Hybrid Or Not: Deterring and Defeating Russia's Ways of Warfare in the Baltics: the Case of Estonia," (2015).
[386] Ibid., 4.

politicians and the people opposing the Russian politics, the Kremlin pressures them with a powerful argument – their gas dependence. The unrests related to the Bronze Statue in Estonia in 2007 and the followed after Russian cyber-attacks also showed that every action that is undertaken, consciously or not, against Russian interests will be punished in one way or another. In its disinformation campaigns, Moscow seeks to underline the oppression by the Estonian government to Russian-speaking population and the attempt to destroy and diminish the legacy of Russia in the country. Another focal point in the narrative distributed in Estonia pertains to the alleged degradation of society's morale and the failure of the state to provide acceptable welfare conditions to its citizens. The goal of the disinformation is to cast doubt in the Estonian government's ability to ensure both the moral and the material wellbeing to the Estonian people[387].

Somewhat resembling the Russian view of Estonia is the one that it has of other former Soviet countries that are EU-members currently. Among the most serious vulnerabilities to disinformation in Bulgaria, the Czech Republic, Hungary, Slovakia, and Poland is the education system. Researchers focusing on this issue point out that the education systems in these countries are based almost entirely on memorizing facts rather than interpreting them through a critical lens. Moreover, the history books themselves do not contain moments from the world history whose importance is widely recognized (e.g., the Cold War)[388]. Through online media and other sources, Russia seeks to convince Eastern- and Central European countries that "the history of Slavs was different from that officially presented by historians"[389]. The rationale behind this was to emphasize Russia's role in both the religious, cultural and statehood history of these countries.

[387] Ibid.

[388] Tomáš Čižik, "Information Warfare–Europe's New Security Threat," *CENAA Policy Papers* 3 (2016).

[389] "Russian Information Warfare in Central Europe," *Information Warfare–New Security Challenge for Europe. Bratislava: Centre for European and North Atlantic Affairs* (2017): 20.

Additionally, the success of disinformation is bolstered by factors such as weak civic society, ethnic and linguistic ties of Russia with some of the population in former Soviet countries[390]. Moreover, Russia has local military dominance over these countries that cannot engage in any campaign against it without a NATO intervention and such is hard to trigger because of the unidentified legal status of cognitive threats, understood as warfare.

Another element that carries meaning in the context of disinformation in Central and Eastern European EU-states is the non-decisive standpoint of politicians. While some of them show a friendly attitude toward Russia, others are very reluctant in labeling Russia as an aggressor and the mastermind behind the disinformation campaigns[391]. This is especially true since there is a confirmed pattern of Russian financing for right-wing parties, radical parties expressing supremacist, Nazi, anti-globalization, anti-multiculturalism anti-immigrants, anti-EU, anti-NATO and anti-U.S. beliefs[392]. Consequentially, Russian trolls support the agenda of such parties that in return support the Russian political goals[393].

Due to the lack of common religious and ethnic background that Russia shares with the Eastern European states, the features of the disinformation campaigns in Western Europe are different than in the countries with Russian-speaking or strongly pro-Russian population. While propaganda and disinformation operations are not missing in other times, they are manifesting themselves mostly before important elections in Western Europe. Considered as the heart of the European Union, Germany's domestic political life falls under the Russian disinformation attacks. In terms of propaganda, the three central news outlets in German are RT Deutsch,

[390] Alexander Lanoszka, "Russian hybrid warfare and extended deterrence in eastern Europe," *International affairs* 92, no. 1 (2016).
[391] Čižik, "Russian Information Warfare in Central Europe."
[392] Alina Polyakova, "Putinism and the European Far Right," *Institute of Modern Russia* 19 (2016).
[393] Čižik, "Russian Information Warfare in Central Europe."

Sputnik Deutsch, and NewsFront Deutsch, as the first two are state-owned and the third one is allegedly independent, but with suspected strong ties to the Russian Secret Services[394]. While sensibly less than in the Baltic countries, the population of Russian descent in Germany is approximately 2.5 million people and is among the main targets of cognitive threats[395]. Other German citizens, who are affiliated or share the ideas of Germany's far-right party – Alternative for Germany – also become victims of both propaganda and disinformation due to their predisposition to anti-immigrant and anti-globalization rhetoric. Among the disinformation cases that gained the most popularity in the media is *Our Lisa* – a story about a German girl of Russian origin who was allegedly abducted and raped by men of Middle-Eastern origin. The news provoked protests in different cities in Germany in a time in which the question about refugees was severely dividing the German public opinion. In 2017, news about German soldiers raping a girl in Lithuania, as "part of a NATO reassurance mission" appeared in media[396]. Two other stories that gained popularity were that "700,000 Germans had left the country because of Merkel's refugee policy" and that "refugees had destroyed the oldest church in Germany"[397].

An intensified disinformation campaign was triggered also in France before the Presidential Elections in 2017. A study confirmed the presence of bots that were employed in the U.S. Presidential Elections in 2016 and then re-used in the French ones. In addition, it provided a potential answer to the question of why the disinformation campaign against Emmanuel Macron failed. The results of the project showed that most of the audience for Twitter content with the hashtag #MacronLeaks "was the English-speaking American alt-right community, rather than

[394] Constanze Stelzenmüller, "The impact of Russian interference on Germany's 2017 elections," *Testimony before the US Senate Select Committee on Intelligence June* 28 (2017); ibid.
[395] Ibid.
[396] Ibid., 6.
[397] Ibid.

French users"[398] – a pattern that was in opposition to the general political discussion in which mostly French voters were involved and were supportive of Macron's candidacy.

Russian disinformation spread even to Sweden – a country that has not been in the eyesight of the Kremlin as an important target in the post-Cold War period or at least not until 2014, as some authors argue[399]. With increased attention toward the Baltic region, Sweden became a zone of deployed active measures by Russia. Similar to other countries where disinformation is spread, in Sweden, "the openly pro-Kremlin elements in the Swedish far right include the fascist organisation Nordic Resistance (Nordiska motståndsrörelsen). Nordic Resistance has cooperated with two Russian organisations, the Rodina party and the Russian Imperial Movement; their international network is the World National-Conservative Movement, which has also donated an unspecified sum of money to Nordic Resistance"[400].

Official Swedish documents are also a subject of manipulations by the Russians. Online media report the existence of certain documents supposedly prepared and signed by Swedish politicians. Such forgeries often include even a letterhead that gives the document authenticity. While they circulate mostly in less-known websites in Russian or Swedish, research shows that at least on one occasion a forgery reached the traditional media that reported it[401]. In the case of Sweden, since there is no ethnic and religious background through which Russia can appeal to a large number of Russian-speaking population, the target becomes the Swedish public opinion and the decision-makers, mainly regarding the country's relationship with NATO. An instance of this is a host agreement from 2016 for easier access of NATO forces to Swedish territories

[398] Emilio Ferrara, "Disinformation and social bot operations in the run up to the 2017 French presidential election," *First Monday* 22, no. 8 (2017): Discussion and Conclusions, par. 3.
[399] Martin Kragh and Sebastian Åsberg, "Russia's strategy for influence through public diplomacy and active measures: the Swedish case," *Journal of Strategic Studies* 40, no. 6 (2017).
[400] Ibid., 30.
[401] Ibid.

including times of training and crises. Attempting to prevent the ratification, an anti-NATO narrative started dominating the disinformation campaigns. It was depicted in the news announcing “NATO submarines violating Sweden’s territorial waters”[402] and some legal concerns surrounding the ratification, such as that NATO “will be allowed to place nuclear weapons on Swedish military bases, use Swedish territory to launch a first-strike attack on Russia and enjoy legal immunity for crimes committed by NATO troops on Swedish territory”[403].

Applied measures against this threat. Beginning to realize the seriousness of the problem with Russian disinformation, states affected by these campaigns launched a series of measures – some to deter future threats, others to combat their consequences. These measures could be conceptually divided into four groups: legal measures, the establishment of new agencies and units, creation of new media channels to prevent disinformation, and drawing awareness to the issue.

The legal measures that are undertaken are dependent upon multiple conditions since disinformation is not a crime, and, in the online space, the attribution dilemma makes it very hard to establish a connection between content and a user, especially if the user is acting on behalf of the government. That said legal measures against disinformation are only possible when they are combined with another act that actually constitutes a crime – for instance, hacking and posting false statements on social media, as it was in the charges pressed against twelve GRU officers[404]. Even if the offenders are indicted, the chance of bringing them to justice is minimal because, if they reside in Russia, they will not be extradited to the U.S. Some of the

[402] Ibid., 36.

[403] Ibid., 26.

[404] Department of Justice, "Grand Jury Indicts 12 Russian Intelligence Officers for Hacking Offenses Related to the 2016 Election."

tactics used in such cases are that the defendants are manipulated to visit a third country with which the U.S. has an extradition treaty. Once they visit, they can be captured and extradited. However, such scenario would be highly unlikely. As evident, legal measures are severely limited to a narrow circle of cases, and even they have a very low likelihood of concluding with a sentence because disinformation, by itself, does not entail legal liability unless it pertains to cases of defamation.

Other measures used in the fight against disinformation include the establishment of new units and agencies intended to control the spread of fake news and propaganda (e.g., the European External Action Service East Stratcom Task Force). In Central Europe, the Czech Ministry of Interior presented a new unit that will handle the cases of disinformation and will train professionals to combat such threats. A year later in 2017, Slovakian Ministry of Interior announced that online media and their content would be monitored by twelve newly added officers employed in the Computer Crime unit. Similar statements came also from Hungary and Poland. Other government efforts include the Inter-departmental task force at the Ministry of Foreign Affairs in the Netherlands, that was launched in November 2015[405]. While this is a step forward toward recognizing the magnitude of the problem, such measures and their effectiveness remain out of the sphere of competence of the law enforcement. There are no laws against disinformation and taking down websites containing such may clash with laws protecting the freedom of speech and the right of information (even if it represents disinformation rather than information). In May 2008, NATO created the Cooperative Cyber Defence Centre of Excellence in Tallinn, Estonia. It was created shortly after the Russian cyber-attacks in Estonia that followed

[405] Kremlin Watch, "The Prague Manual: How to Tailor National Strategy Using Lessons Learned from Countering Kremlin's Hostile Subversive Operations in Central and Eastern Europe," in *European Values Protecting Freedom* (2018).

after the Bronze Statue demolition in 2007. The center "is responsible for identifying and coordinating education and training solutions in cyber defence for all NATO bodies across the Alliance"[406]. Some NGO efforts to combat the problem are also documented. In Armenia, Azerbaijan, Georgia, the Netherlands, Hungary, Poland, Moldova, Slovakia, and Ukraine NGOs use as weapons against disinformation fact-checking websites and resources, and identification of tools used by Moscow as disinformation tactics[407].

Potentially much more purposeful and productive is the measure that Estonia adopted to deter disinformation. Recognizing the similarities between Estonia and Ukraine in terms of the pro-Russian population that resides within the borders of the country, Tallinn decided to deal with disinformation not by taking something away, but by offering something new. In September 2015, "the local public broadcasting has opened a new, Russian-language TV-channel called ETV+…to keep the Russian-speaking minority in Estonia informed about local and international issues (two one-hour programs per day and regular daily news in Russian) and to provide the audience with entertainment (such as shows and film purchased by ETV+, such as the TV and web programs of Deutsche Welle in Russian)"[408].

The third measure used against disinformation is the awareness of the problem. A study of EU-countries exploring three variables - political acknowledgment of the threat, government counter-activities and counter-intelligence activities - identifies the level of awareness of the disinformation threat and how much is currently being done to counter it[409]. Its results show that most awareness and efforts dedicated to the problem are made in Lithuania, Latvia, Estonia,

[406] NATO, "Cooperative Cyber Defence Centre of Excellence - About us."

[407] Kremlin Watch, "The Prague Manual: How to Tailor National Strategy Using Lessons Learned from Countering Kremlin's Hostile Subversive Operations in Central and Eastern Europe."

[408] Viljar Veebel, "Russian propaganda, disinformation, and Estonia's experience," ed. Foreign Policy Research Institute (2015).

[409] Kremlin Watch, "The Prague Manual: How to Tailor National Strategy Using Lessons Learned from Countering Kremlin's Hostile Subversive Operations in Central and Eastern Europe."

Sweden and the U.K. Some but less awareness and efforts are registered in Poland, Denmark, the Czech Republic, Finland, Germany, Romania, France, the Netherlands, and Spain. Hesitant to recognize disinformation officially as a problem and therefore to combat it actively are Belgium, Slovakia, Bulgaria, Ireland, and Croatia. Among the countries with least awareness and adopted measures against it are Italy, Slovenia, Portugal, Malta, Luxembourg, Austria, Hungary, Greece, and Cyprus, as the last two's coefficient is zero, implying that no political acknowledgments of the threat are made, and no measures are undertaken to combat it.

The case with ISIS recruitment

Background. One of the most popular examples of cognitive threats is the one with radical organizations' member recruitment. While the Islamic State of Iraq and Syria does not exist anymore, at least not territorially, such organizations existed long before its emergence (e.g., Al-Qaeda) and will surely continue to exist in one form or another. In this section, I outline the background of the problem with recruitment in terms of its targets and the factors that facilitate this process.

Among the main targets of the ISIS recruitment were men, predominantly foreign-born such as Saudi Arabian students, Tunisian workers, and European adolescents who have quit attending school[410]. Most of those people did not have military expertise but some recruits such as "battle-tested Chechens and Uzbeks"[411] were compensating for the others' lack of skills in combat. In 2014, Abu Bakr Al-Baghdadi appealed to men and women, of all background to travel to ISIS and help develop the newly declared caliphate[412]. Especially valued were

[410] Mia Bloom, "Constructing expertise: Terrorist recruitment and "talent spotting" in the PIRA, Al Qaeda, and ISIS," *Studies in Conflict & Terrorism* 40, no. 7 (2017).
[411] Christopher Reuter, "The Terror Strategist: Secret Files Reveal the Structure of Islamic State," *Der Spiegel* 2015.
[412] Bloom, "Constructing expertise: Terrorist recruitment and "talent spotting" in the PIRA, Al Qaeda, and ISIS."

preachers, doctors, engineers, and of course, soldiers. Children and adolescents were also viable targets since their psyche was still vulnerable to ideological influence. The main part of the young recruits was "children living in single family households…who have less adult supervision or neglectful parents… who experience domestic abuse, etc."[413]. Moreover, they were valuable recruits, treasured for the long-term plans of the caliphate. The steps of the child recruitment process were first, earning the child's trust, then acting as a mentor figure to them, while at the same time "showering the potential recruit with attention, gifts, food, and money"[414]. Another example of this tendency is that at the end of 2014 and the beginning of 2015, six Spanish girls of Moroccan origin and between the age of 14 and 19 were arrested for attempting to join ISIS[415]. European teenage girls and young women from other countries are also among the ones who wished to join ISIS after they radicalized – they typically come from the United Kingdom, Germany, Austria, and Belgium[416]. However, not small is also the number of women who with their children, left for Iraq and Syria to join their ISIS-husbands.

Among the main factors that contribute to radicalization and recruitment is the marginalization and the isolation of many immigrants, or citizens whose parents were foreign-born or they were foreign-born themselves. Some were citizens of the country against which the acts of violence were committed and were representing the concept of *homegrown terrorism*. The latter envisions the residents of a certain country who get radicalized and recruited while being in their home or host-country just to return and commit acts of terrorism against this very

[413] Asaad Almohammad, "ISIS Child Soldiers in Syria: The Structural and Predatory Recruitment, Enlistment, Pre-Training Indoctrination, Training, and Deployment," ed. The International Centre for Counter-Terrorism –The Hague (2018), 6.
[414] Ibid.
[415] Moha Ennaji, "Recruitment of foreign male and female fighters to Jihad: Morocco's multifaceted counter-terror strategy," *International Review of Sociology* 26, no. 3 (2016): 9.
[416] Anita Peresin and Alberto Cervone, "The western muhajirat of ISIS," *Studies in Conflict & Terrorism* 38, no. 7 (2015).

same country later. It is possible that the notions of immigration and homegrown terrorism overlap since many of the citizens of a country, if foreign-born or born by parents who are or were non-citizens, are perceived as they do not belong to the community and are therefore rejected and marginalized politically, economically, culturally and socially. The rejection turns into alienation, alienation into a vulnerability that gets skillfully exploited by radical organizations.

In a social context, the process of acceptance of an immigrant to society goes through an assimilation period in which immigrants have to prove that they belong by giving up their *otherness* and by embracing the qualities prescribed by the society as signifiers for *sameness*. However, some authors argue that for effective integration in the era of transnationalism, it is no longer mandatory for immigrants to abandon their previous identities and cultural beliefs and to replace them with the ones in the receiving country[417]. Instead, they could preserve their self-identity and embrace the shared values of their new home country.

Regardless of the approach to the issue, the premise of geopolitical and mental migration of people assigns a pivotal role of the media, the education system, and the state itself to create a framework of openness and inclusiveness to the newcomers [418] [419] [420]. However, societies are reluctant to welcome foreigners[421]. Their fear of a particular problem becomes highly generalized when it flows into the mainstream narrative opposing immigration altogether – a factor that reflects on children's school experiences as well. Even generations after relocating, an

[417] Francis Fukuyama, "Immigrants and family values," *Commentary* 95, no. 5 (1993).

[418] Jan Michael Kotowski, "Narratives of Immigration and National Identity: Findings from a Discourse Analysis of German and US Social Studies Textbooks," *Studies in Ethnicity and Nationalism* 13, no. 3 (2013).

[419] Etienne Balibar, "The nation form: history and ideology," *Review (Fernand Braudel Center)* 13, no. 3 (1990).

[420] Pierre Bourdieu and Samar Farage, "Rethinking the state: Genesis and structure of the bureaucratic field," *Sociological theory* 12, no. 1 (1994).

[421] Caitlin Cahill, "'Why do they hate us?'Reframing immigration through participatory action research," *Area* 42, no. 2 (2010).

immigrant's identity and culture continue to be perceived by some as *external* to the identity that the citizens of the home-country aim to maintain. The multitude of terrorist attacks committed by ISIS in 2014-2016 raised attention to immigrants and entailed a rapid securitization of immigration, even though some of the perpetrators were *born-and-raised* citizens[422]. This resulted in suspicion, mistrust, and skepticism to the mobility of people across borders that in some cases was even equalized to *invasion*[423]. As a consequence of the increasing politicization of the debate some anti-globalization parties and organizations advocated vigorously for the threat that immigrants, in general, are posing to be eliminated through closed borders policies. While proponents of free migration strongly condemn terrorist attacks and designate such violence to belong in the realm of securitized problems, they still maintain that immigration, as a category not equal to terrorism, has to remain in the non-securitized realm.

The contrast of identities of individuals that belong to the community, and others, who are perceived as external and delegitimized, has transformed into a battle for electoral votes on the political scene. These so-called *policy narratives* succeed to gain followers due to three main criteria: plausibility, appealing to the audience tone, accordance with perceived national interests[424]. Accordingly, the narratives for immigration distributed by nationalist, far right-wing and populist parties consist of similar elements of emotionally appealing binaries that only increase their impact through continuous repetition in the media. Regardless of their patriotically-charged tone and their attempts to create a connection between economic instability and increased crime rates, these *grand narratives* are doomed to fail eventually, according to

[422] Ariane Chebel d'Appollonia, *Frontiers of Fear: Immigration and Insecurity in the United States* (Ithaca, NY: Cornell University Press, 2012).
[423] Virginie Mamadouh, "The scaling of the 'Invasion': A geopolitics of immigration narratives in France and The Netherlands," *Geopolitics* 17, no. 2 (2012).
[424] Christina Boswell, Andrew Geddes, and Peter Scholten, "The role of narratives in migration policy-making: A research framework," *The British Journal of Politics and International Relations* 13, no. 1 (2011).

some authors, due to inability to rationalize the fear from the assumption that everyone different is a threat[425].

By securitizing immigration, far-right parties not only create a sense of fear through speech acts and the power of language but also support discrimination on a racial principle in their attempt to mask their unease of the fact that they could not combat terrorism when it comes from within the state[426]. Therefore, voices in these political circles do not only reject the notion of belonging to the community of racially-diverse immigrants but also reject children of immigrants that were citizens since their birth. Only *exclusive* citizenship that originated generations ago is perceived as a sign of acceptable relationship to the state, and only a shared identity in terms of race, culture, language, and ethnicity could entitle the newcomers to truly fit into the nation[427]. Consequently, many of these patterns could be found in speeches and proclamations of nationalist leaders, thus making the immigrants feeling marginalized. The former endeavor to conceptualize the threat as a more simplified category that could be easily eliminated by creating stereotypes for the immigrants and thus delegitimizing them, instead of recognizing the complexity of the issue. Although the populist movements are not only strong but also represented almost everywhere in the world, some countries remain much more willing to accept immigrants than others. Therefore, nationalist moods in their political climate are either not significant or almost missing. However, the ones with a visible presence of nationalist/far-right party/parties create a dominant narrative in terms of the immigrants, despite the fact that they do not even hold majorities in the national parliaments. The member-states that do not

[425] Miguel de Oliver, "Nativism and the obsolescence of grand narrative: Comprehending the quandary of anti-immigration groups in the neoliberal era," *Journal of Ethnic and Migration Studies* 37, no. 7 (2011).
[426] Didier Bigo, "Security and immigration: Toward a critique of the governmentality of unease," *Alternatives: Global, Local, Political* 27, no. 1 (2002).
[427] Nancy Foner and Patrick Simon, Fear, anxiety, and national identity: Immigration and belonging in North America and Western Europe, (Russell Sage Foundation, 2015).

perceive themselves as *countries of immigration* see immigrants as *foreigners*, and even after they enter the borders of the state, they remain assessed mainly through their *otherness*[428]. According to such narratives, immigrants are perceived simultaneously as a threat to the state's physical and economic security thus justifying discriminatory policies and oppressive behavior towards them[429].

After leaving their country of origin and settling into the host-state, many families are struggling to find employment and means to support themselves. Experiences of ethnically different (than the majority) groups in the workplace frequently entail suppression, unemployment and underemployment practices that inevitably result in discrimination in terms of the economic opportunities for them[430]. Monetary rewards and other financial benefits for joining ISIS were pointed in studies as important reasons mentioned in recruitment and its success – the remuneration of an ISIS fighter is approximately $1400. Moreover, fighters are predominantly from low-income families, typically earning not more than $200 a month, and non-college educated[431]. Paradoxically, economic privilege understood as affluence, access to good education, and technology could also be among the reasons for radicalization, especially of young women as they "become subsumed by the religious, social, and political forces and overtake their identity. They focus less on themselves, and more on the external environment"[432]. Mainly young women are among the recruitment targets to whom financial rewards appeal the

[428] Gisela Brinker-Gabler and Sidonie Smith, *Writing new identities: gender, nation, and immigration in contemporary Europe* (MInneapolis, MN: University of Minnesota Press, 1997).
[429] Alexandria J. Innes, "When the threatened become the threat: The construction of asylum seekers in British media narratives," *International Relations* 24, no. 4 (2010).
[430] Slack and Jensen, "Underemployment across immigrant generations."
[431] Ennaji, "Recruitment of foreign male and female fighters to Jihad: Morocco's multifaceted counter-terror strategy."
[432] Leah Windsor, "The Language of Radicalization: Female Internet Recruitment to Participation in ISIS Activities," *Terrorism and Political Violence* (2018): 6.

least. Many of them are from wealthy families, living in the West, well-educated and having a promising future[433].

The component of acute sensitivity, and longing for adrenaline and adventures, especially of adolescents, also facilitates the radicalization and recruitment of ISIS members. Vulnerabilities in "a small number of Muslims who can't find their way to belong to society, feel rejected or lack purpose in their lives, who want adventure or to bolster their sense of manhood or womanhood, or who are angered by geopolitics and insults to their religion"[434] are crucial to understanding why ISIS's ideology becomes such an attraction to young people. Among the appealing reasons to join ISIS is also boredom that is eliminated by subscribing to the exciting alternative that the life as a member of the radical organization presents to the recruit. In addition, some women left their countries with intentions to contribute to a humanitarian mission. Frequently, such women did not plan to participate in battles[435]. Others were interested in helping the wounded but did not mind being included in combats as well.

Another important reason for radicalization is the exploitation of religious grounds for achieving ISIS's political goals. Radical Islamism has been the engine of the terrorist attacks committed by members of ISIS both inside and outside of Europe. While the implementation of ideas of the Salafism has been different across the various terrorist groups, its main goals have not changed since Sayyid Qutb, Sayyid Abud A'la Mawdudi and other jihadist ideologues developed them. The end-goal of jihadism is the establishment of an Islamic order that should replace the existing Western civilization that is perceived as impure, corrupt, and decadent[436].

[433] Peresin and Cervone, "The western muhajirat of ISIS."
[434] Speckhard, "ISIS and the Rise of Homegrown Terrorism in the West," par. 17.
[435] Peresin and Cervone, "The western muhajirat of ISIS."
[436] Mary R. Habeck, *Knowing the enemy: Jihadist ideology and the war on terror* (New Haven, CT: Yale University Press, 2007).

The original objective was to create a new Islamic regime after the fall of the Ottoman Empire in 1924, the Western order had to be destroyed first. ISIS declared the establishment of the Islamic State before completing the mission of taking down the existing Western culture as their former leader Abu Musab al-Zarqawi planned, unlike Al-Qaeda members who preferred to follow the original order of tasks, prescribed by the jihadist literature[437]. Regardless of the particular sequence of executing the different parts of their strategy, the continuing attacks of ISIS show support for the fact that they still adhere to the two central tenets of the jihadist school – eliminate the old order and establish the Islamic one. In order to execute its main goals, ISIS recruited members through, among other things, the religious appeal of the utopian narrative that jihad offers[438]. Interestingly, when it comes to women who radicalize, typically they "do not come from particularly religious families, but are students who want to go to Syria to marry a devout Muslim or provide humanitarian aid. As a rule, young women are radicalized outside the home, due to peer group influence, a preacher in a mosque (masjid) or through religious schools (madrasas)"[439]. Moreover, the jihadist ideology is appealing to women, especially to the ones experiencing insecurity, because of the following reasons - first, the communal conditions offered by ISIS. Second, the chance to contribute to broader goals, such as working to create an Islamic caliphate. Third, the predictable nature of the patriarchal order, that even if entailing the loss of some freedom, would be preferred than the uncertainty of life outside of a strong community united by shared goals and identity[440].

[437] Erin Marie Saltman and Charlie Winter, "Islamic state: The changing face of modern jihadism," *London: Quilliam Foundation* (2014).

[438] Bloom, "Constructing expertise: Terrorist recruitment and "talent spotting" in the PIRA, Al Qaeda, and ISIS."

[439] Ennaji, "Recruitment of foreign male and female fighters to Jihad: Morocco's multifaceted counter-terror strategy," 551.

[440] Ibid.

The religious component in radical organizations' recruitment strategies was always present, but online space made them much more impactful – they became more appealing, and their message was reaching much more recipients than before. ISIS's presence on social media was evident in Facebook, Twitter, YouTube, Instagram, Tumblr as well as in communication channels that included Telegram, Signal, WhatsApp and others[441]. The essence of ISIS's propaganda is in the dualistic nature of the content they distribute. On the one hand, it is violent, brutal, merciless, and unapologetic, appealing mostly to people who crave excitement. On the other, appealing to a different kind of audience, mostly professionally-oriented, it is also depicting "altruism and good deeds, with positive messages, soft lighting, and smiling children"[442]. Propaganda videos were typically representing the Islamic caliphate as a heavenly place to live - a myth to which the lack of actual information reported by alternative sources, contribute significantly. In fact, "on Facebook, Twitter, and other social media sites, young Muslim women, who already live on the territory occupied by ISIS, portray their lives as a sort of 'Disneyland for Muslims' by posting pictures and writing blogs of daily life activities and offering help and support"[443] to anyone who is interested in joining the caliphate. It was not only what content they were using and through what channels but also how they were reaching such a broad audience. The media strategy on Twitter included following every day's top hashtags that were generating a large number of retweets. Once they got the attention of the Twitter audience, they were free to incorporate their own message in the tweets. An example of the skills with which they were operating in social media is the case with World Cup 2014, in which hashtags

[441] Ahmad Shehabat and Teodor Mitew, "Black-boxing the black flag: anonymous sharing platforms and ISIS content distribution tactics," *Perspectives on Terrorism* 12, no. 1 (2018).
[442] Bloom, "Constructing expertise: Terrorist recruitment and "talent spotting" in the PIRA, Al Qaeda, and ISIS," 606.
[443] Anita Peresin and Alberto Cervone, "The western muhajirat of ISIS," ibid.38 (2015): 504.

#Brazil2014, #ENG, #France and #WC2014 were used "to gain access to millions of World Cup Twitter searches, in the hope that users would follow links to the group's propaganda video"[444].

Overview. The following case study was selected to represent ISIS recruitment because of its unique characteristics. First, the targets were women, instead of men, as the latter are more likely to be recruited and join the organization. Second, the recruits were not the stereotypical *vulnerable targets*, according to most risk factors such as isolation, low performance at school, lack of social contacts, lack of prospects for better life and poverty.

The story I am using for this case study describes the path of the then 16-year-old Khadiza Sultana and her two school friends – Shamima Begum and Amira Abase who traveled from their homes in London to Syria to join ISIS. Described as "joyful, sociable, funny and kind"[445] Khadiza Sultana pretended to go to school one day and got on a flight to Turkey from where the girls took a bus to Syria. When she did not come home after the end of the school-day, her relatives started worrying about her. Not suspecting any reasons why Khadiza would like to become a member of ISIS, her mother and sister found out that she was reportedly in Turkey, with her two friends – a fact of which both women were made aware by the Metropolitan Police unit that deals with terrorism. Khadiza's father had passed away, but unlike other cases with personal tragedies, the girl was not introverted and isolated from the world. Khadiza was described as very intelligent, very gifted girl who was not only exceeding the expectations of her teachers but was also tutoring students having troubles with their school preparation. Another evidence for her social environment is that she was having a sleepover with her niece and a friend at her house, right before she departed for Syria. The latter could not have been attributed to some whim, however, but to a carefully executed plan for which the following facts testify.

[444] James P. Farwell, "The media strategy of ISIS," *Survival* 56, no. 6 (2014): 51.
[445] Katrin Bennhold, "Jihad and Girl Power: How ISIS Lured 3 London Girls," *The New York Times* 2015, par. 3.

First, Khadiza did not take all of her clothes, but most of them, leaving some, as to look like she has not left at all. Moreover, she used tote bags instead of suitcases to gather her belongings in order to avoid suspicion. Second, she told her relatives she was going to school, as she usually does. Third, when she left, allegedly for school, she only took a small backpack with her, as she would have if she had actually gone to school. The overall purpose of the trip was to join ISIS, but it is not entirely clear what particular goals she had in mind for her life in ISIS. Some of the girls who left for Syria state that they were looking to join a cause, to discover meaning in life and to reconnect with religion and spirituality. As women are generally not allowed in battles, they assume the roles of "wives, mothers, recruiters and sometimes online cheerleaders of violence"[446]. If there is any stereotype surrounding the male supporters of ISIS, indicating a low educational level, this is certainly untrue for the women who join the organization. They are typically much more educated than men, much more goal-oriented, as this is found to be true for various women who traveled to Syria across economic class, ethnicity, and nationality. Khadiza's friend Amira was also an example of these characteristics – she was very intelligent, an advocate for Muslim women, a gifted athlete and public speaker with a vivid interest to reading. She mentioned before her departure that she feels like she does not belong in the conditions that the West offers. The decision to abandon their life in the West and join the caliphate is perceived typically as an example of a rebellion, engendered by teenage impulsivity and immaturity, a result of oppression of Muslims, anxiety about arranged marriages from a young age, such as the one of Khadiza's sisters when they were as old as Khadiza was when she left.

[446] Ibid., par. 14.

Despite the girls' allegiance to ISIS as a potential form of protest against social conditions and cultural norms, there was also another factor that probably contributed to the young women' departure. Khadiza's close friend, Sharmeena, then 16-years-old, also left for ISIS after experiencing a personal tragedy – the loss of her mother from cancer. She radicalized in her views as she was growing more and more religious after her death. Sharmeena's father remarried after the death of her mother and she then began to visit the mosque regularly and to defend ISIS in class, sometimes passionately and relentlessly. A change in Khadiza's behavior also was noticed before she left for Syria. She began covering her hair, sometimes at school but also at home. Her brother remembers a conversation with her about Syria in which his younger sister asked him about the political situation there. His response was that it seemed that most people were against Bashar Assad's regime. Sharmeena's departure for Syria influenced Khadiza and the other girls to do the same, even though, officially the girls did not disclose anything about Sharmeena's location and new life and pretended they had no knowledge of reasons for her disappearance. The original plan was that Khadiza and three more girls, not two, travel to the caliphate. Allegedly, the fourth girl decided to stay because her father had a stroke. Soon after the police discovered the note suggesting the planned trip of the four girls along with a few items they wanted to bring along and their cost, a judge confiscated the fourth girl's passport. In the meantime, between Sharmeena's disappearance, and the time the other girls left for Syria, their school work became delayed and worsened – a sign that both parents and school staff missed. After the girls' departure, evidence of Amira's father being present at Islamic rallies at which the American flag was burnt, surfaced. Amira was sometimes accompanying him at these rallies, organized by Anjem Choudary, a British Islamist, known for his hate-speech and his allegiance to ISIS.

Perhaps among the most important questions in this case is whether the girls received some help in fleeing the U.K. The fact that the plane tickets themselves, along with the other expenses that had to be made for the trip were beyond what the girls could have saved or obtained, makes it very likely for them to have been recruited and even sponsored financially for the trip. Khadiza, allegedly, had not have taken the necessary money from her family as she only took some jewelry that was not of high value. As for Sharmeena, she had received an inheritance after her mother's death, possibly enabling her to be able to travel to Syria. Another fact suggesting the girls had an inside help was that a Turkish network reported that a man was waiting for them by the Syrian border and giving them passports. The footage showed him unloading the content of his car's trunk and saying something to the girls. Even before they reached Turkey, their lawyer suggested that they may have been a target of a recruitment network that operates in their London neighborhood – a conservative Muslim community – which is why the network potentially enjoys the protection of some of the locals.

Shortly after their arrival in Syria, allegedly in Raqqa, Khadiza got in touch with her sister to tell her she is safe, they are eating pizza, French fries and fried chicken and are staying at a place that had chandeliers, supposedly a hostel for single women in Raqqa. While not explicitly stating her intention to get married, Khadiza shared with her sister that she considers doing so. She also indicated that further communication should be initiated by her, a detail, suggesting that her external communications may have been controlled. After some time passed from the girls' first outreach to their relatives, they got married to Western men and have moved out of the hostel to begin living with their husbands. One of them, Amira, became allegedly, a recruiter as well. An undercover journalist posed as a potentially interested in joining ISIS girl. Amira recommended that the girl should tell her parents that she will attend school activities in the day in which she plans to flee, and then fly to Turkey from where she should be smuggled to Syria. There was also mentioning of a person who would help her start her journey in London, residing at a close distance from Amira's former school – the Bethnal Green Academy. As for the third girl who traveled with Khadiza and Amira – Shamima, she married a Dutch citizen, Yago Riedijk, shortly after the girls arrived in Raqqa[447]. Allegedly, she requested an English-speaking husband between the ages of 20 and 25. The couple has three children, two of whom, died. The third one was born in a refugee camp in northern Syria after she left ISIS. Shamima's British citizenship was revoked, as government officials in the U.K. stated that she would not be stateless as her mother is Bangladeshi and she is entitled to citizenship in this country, a possibility that was later denied by the Bangladesh's Foreign Ministry. While Shamima's husband is still technically allowed to return to the Netherlands, he may face a long sentence for his involvement in ISIS. Moreover, the Netherlands already revoked the citizenship of a person who was an ISIS member. Considering these circumstances, it is unclear where Shamima, Yago and their newborn baby would live and whose citizens they would be.

Applied measures against this threat. Politicians, practitioners and law-enforcement officers from all over the world are puzzled by how to successfully counter recruitment for radical organizations. Since such organizations are a threat themselves, the easiest solution to the problem would be to destroy the organizations. However, especially, with the case of ISIS, radical groups merge, split, join efforts or differentiate from each other but they never disappear entirely because their ideology is still alive, as well as their ideas and goals. The defeat of Al-Qaeda did not prevent the emergence of ISIS, nor the end of ISIS will probably eliminate chances of another radical organization's rise. Realizing this, Western governments developed

[447] Iliana Magra, "Dutch ISIS Fighter, Husband of Shamima Begum, Wants to Return Home With Family," ibid. 2019.

measures to combat *the war for minds*. Overall, they could be divided into three different groups: disruption, diversion, and counter-messaging strategies[448]. The first set of methods include cyber-operations that seek to take down accounts of ISIS-member that contain propaganda. In 2013, Facebook, YouTube, and Twitter started deleting and blocking such accounts[449]. Regardless, the nature of social media allows for a quick generation of multiple websites, multiple accounts, hashtags, posts and tweets for every single one that has been deleted. Moreover, the use of bots that could further facilitate the spread of a message leave efforts to disrupt ISIS online agenda without the anticipated results. Some scholars even argue that such strategies could push the ISIS digital recruitment and propaganda to the darknet – which will make disruption of such communications even harder as "the choice of whom to monitor, and under what conditions, remains murky and potentially full of legal potholes"[450].

Another campaign aims to redirect potential ISIS-recruits to other community-significant tasks to divert them from the appeal that the broader goals of ISIS pursue. In 2012, the State Department launched such program intended to prevent young people in Southeast Asia from radicalizing[451]. Similar efforts were devoted to the American youth but in the physical, rather than in the online space.

A third measure to combat and deter the aggressive persuasion tactics of ISIS is countering their messages through counter-narratives that are mainly two types. The first sends a message through Imams and other scholars interpreting Islamic religion properly, highlighting that "killing and suicide missions and brutality are anathema to traditional Islam"[452]. One

[448] Karen J. Greenberg, "Counter-radicalization via the internet," *The ANNALS of the American Academy of Political and Social Science* 668, no. 1 (2016).
[449] Ahmet S. Yayla and Anne Speckhard, "Telegram: The mighty application that ISIS loves," ed. International Center for the Study of Violent Extremism (2017).
[450] Greenberg, "Counter-radicalization via the internet," 269.
[451] Ibid.
[452] Ibid., 172.

downside of this approach is that many ISIS recruits do not interact with Imams, they do not go to mosques, and may not be religious at all. The second narrative distributed as a counter-measure to ISIS propaganda is debunking the myth that life in ISIS equals life in paradise, as its supporters promise. Instead, through videos depicting the violence, the brutality and the bloodsheds of the terrorist organization, the social perceiver should get convinced that the life described by ISIS members is an illusion. As this could potentially serve as a strong deterrent to ISIS recruits, a notable issue in such campaigns is that the number of Muslims involved in these efforts are not high. In addition to this, the anti-Muslim environment in some Western countries could devalue the message of inclusion and support for diversity that is in the core of the counter-narrative strategy[453]. In this regard, Aistrope notes that the "credibility deficit opened up by the tension between rhetoric and practice in the US War of Ideas should serve as a cautionary example for Western governments seeking to address ISIS social media recruitment of their domestic populations"[454].

In terms of military measures, it is evident that physically defeating the radical organization is a step forward toward future deterrence. Punishing its members too. However, the legal measures aimed at deterring future threats are minimal. The numerous ISIS soldiers, who are detained in Iraq, are a subject of vigorous international negotiations. The question that is in the center of these negotiations is what to do with the prisoners. Iraqi prisons are claimed to be full[455], and other countries are reluctant to take the prisoners for their due process. That said, concrete legal measures undertaken to deter this threat in the future, are subject to disagreement

[453] Ibid.

[454] Tim Aistrope, "Social media and counterterrorism strategy," *Australian Journal of International Affairs* 70, no. 2 (2016): 134-35.

[455] Richard Hall, "What happens to ISIS fighters when they are captured," *Public Radio International (PRI)* 2016.

between the different stakeholders in this issue. Therefore, implications for deterrence are with limited potential.

Another suggested measure of punishment and future deterrence for being associated with a terrorist organization is the stripping of citizenship that some countries, such as the U.K. have already enforced. Other countries, such as Sweden, have discussed the measure at a government level but it was concluded that the cumbersome legislative process of implementing this measure would take years and is therefore considered to be inapplicable[456]. Germany is also planning to introduce measures for stripping ISIS fighters of their citizenship in case they possess dual citizenship[457]. This consideration is engendered by the principles of the international law according to which people cannot be deprived of citizenship in case they will remain without one and will become stateless. Therefore, stripping of citizenship would only be legally supported if the individual is a citizen of more than one country. The American President Donald Trump, for instance, declared that he will oppose the return of people who have been involved with ISIS, and will revoke their citizenships of naturalized Americans, even if they resided in the country their entire life before they pledged allegiance to ISIS[458].

When it comes to child-soldiers and children of ISIS-members who started returning from Iraq and Syria, there is not a large number of measures that are supposed to reintegrate them into society. Moreover, placement in a Western-system that is foreign to them after years in the ISIS-environment proved itself to be even counterproductive. The characteristics of the ISIS's educational system would make their adjustment to a secular, Western environment particularly difficult and traumatic. This experience could potentially result in depression,

[456] "Sweden Democrats call on government to strip Isis fighters of citizenship," *The Local* 2019.

[457] Harvey Gavin, "Germany 'to strip ISIS fighters of citizenship' with new law," *Express* 2019.

[458] Ibid.

isolation, and even more radicalization. The following sections identify why and provide an example of the consequences that the lack of awareness of the problem brings.

In 2014, Abu Bakr al-Baghdadi established a new order in the ISIS schools that underlines three tendencies. First, the female students and teachers were divided from the male ones as the former were obligated to wear a mandatory niqab. Second, classes in arts, social sciences, music, philosophy, and philosophy were eradicated from the curriculum[459]. Third, new classes such as *Islamic jurisprudence* and *Biography of the prophet* have been implemented[460]. Sources report that "ISIS changed the internationally acknowledged mathematical symbol for adding (+), replacing it with a new symbol represented by the letter (z). The Islamic State's reasoning for these actions was that the (+) sign indicates the cross, which is used worldwide as a symbol for Christians: using a plus sign would be imitating infidels, and was thus forbidden[461].

In addition, these new subjects and the alterations of the commonly accepted scientific language along with the overall atmosphere in the schools of the Islamic State resulted in parents' refusal to send their children to school. They were trying to protect them from the strong propaganda disseminated there as this could easily lead their children to become fighters in the ISIS's army. Regardless, many children were still sent to school and were therefore raised in traditions of hatred and aggression. Outside of the school doors, public executions were a common practice that children observed as well. After the age of nine, boys had to start military training and girls were considered old enough to marry.

Considering this background, placement in a completely different school environment than the one that students used to have in ISIS, could be confusing, frustrating and full of

[459] Eline Gordts, "This Is What Education Under ISIS In Raqqa Will Look Like " *The Huffington Post* 2014.
[460] Caitlin Harrison, "Education Under ISIS: A 'Generation in Darkness'," *The Borgen Project* 2015.
[461] Hosam Al-Jablawi, "A Closer Look at the Educational System of ISIS," *Atlantic Council* 2016.

uncertainty and potential for further radicalization. Charlotte McDonald-Gibson describes an instance in this regard, depicting a case of a boy trained in the ISIS culture of violence: “The 9-year-old boy didn’t like school. He didn’t like the other children, because he knew what they really were: evil unbelievers who deserved to die. So he did what he was trained to do — he attacked them. He was removed from the building on his first day back” [462]. Another former child-soldier in ISIS reports about his experience back in Europe: “When I returned, someone said to me: 'You’re a loser and if I were you I wouldn’t have done what you’ve done, no human being would. This is called failure'. I can’t forget the word 'loser'"[463].

Much criticized but offering an utterly different approach to the problem of radicalization and re-radicalization is presented by the reintegration programs in Denmark and Belgium. Both countries offer resources to help former jihadists with job search, integration, and inspiration for getting education[464]. While some see such treatment of former ISIS fighters that returned to Europe as full of reasons for skepticism and suspicion, others emphasize that this approach is not applied without the necessary screenings and conversations initiated on behalf of the authorities. A reintegration strategy could only benefit the state’s security in terms of the threat that former ISIS members pose when they return home. Regardless, its current outreach remains highly limited since approximately two countries in the EU are offering such programs. Furthermore, while a potentially positive influence over the lives of former jihadists is possible, the social stigma and the rejection, the lack of inclusion and the still powerful narrative about immigrants, Muslims and terrorism could play a significant role that may outweigh the efforts of the

[462] Charlotte McDonald-Gibso, "What Should Europe Do With the Children of ISIS?," *The New York Times* 2017, par. 1.
[463] Quentin Sommerville and Riam Dalati, "An education in terror," *BBC News* 2017.
[464] Alastair Reed, Jeanine de Roy van Zuijdewijn, and Edwin Bakker, "Pathways of foreign fighters: Policy options and their (un) intended consequences," in *ICCT Policy Brief*, ed. International Center for Counter-Terrorism (The Hague) (2015).

reintegration campaigns. To that conclusion contributes the following relationship as well: the higher the antagonism against Muslims on a neighborhood/community level, the higher the likelihood for support for ISIS expressed on social media[465]. Clearly, ISIS's online recruitment operations turned out to be a very successful tool in the arsenal of weapons that the organization has on its disposal. Being aware of this, Western governments have been facing unusual difficulties combating the propaganda spread by ISIS. The main reason for this is the problem of limiting such content distributed online since the freedom of speech is one of the most celebrated and fundamental tenets of democracy. Thus, restricting the online access of ISIS and other groups suspected to have connections with terrorist organizations could have damaging repercussions on the right of free access to information – a paradox that poses an important dilemma[466].

The case with Cambridge Analytica

Background. Ever since its creation in 2004, Facebook was becoming more and more popular to users. It kept adding different features, along with a messaging function and at one point even other, third-party applications started being offered through the platform. The core idea of Facebook was for people to share information and connect. And this is what they did. Various elements such as convenience, desire for developing and maintaining relationships and enjoyment[467] contributed to posting large amounts of personal information with, supposedly friends. What users did not know was that they were sharing and connecting (or being

[465] Mitts, "From isolation to radicalization: anti-Muslim hostility and support for ISIS in the West."

[466] Dylan Gerstel, "ISIS and Innovative Propaganda: Confronting Extremism in the Digital Age," *Swarthmore International Relations Journal* 1, no. 1 (2017).

[467] Hanna Krasnova et al., "Online social networks: Why we disclose," *Journal of information technology* 25, no. 2 (2010).

connected) to a lot more people than just their friends. They did not know, because they were not asked. Users unsuspiciously shared more and more of their personal information and increasingly with people who they do not consider friends or even acquaintances. Moreover, unknowingly, they were sharing locations, feelings, experiences, hobbies, and stories with complete strangers as well.

Facebook was not the first social media with millions of users, and it probably will not be the last. In fact, neither social network was the first place from which personal information of users was stolen, used without permission or even manipulated. The case with Cambridge Analytica and Facebook was not even the first one in which voters' personal information was used by political entities to gain leverage in elections. While there are numerous examples in the U.S. about deceased people surprisingly voting on elections[468], this tendency is global, especially in countries with authoritarian regimes or countries with high corruption levels[469]. Clearly, it is not the deceased who vote but someone using their personal information, typically, to support a particular political party. Fraudulent use of personal information always existed. With the emergence of social media, it only became more common online than in the physical space, because of the favorable digital conditions for personal data collection.

The first signs of users' loss of control over their information were evident in 2006 when Facebook introduced News Feeds where "every act undertaken by their Friends within the system – who befriended whom, who commented on whose Wall, who altered their relationship status to 'single', who joined what group and so on"[470] was on display. Users were outraged and began joining groups opposing Facebook. To prevent users from leaving the platform, Mark

[468] Jason Snead, "Voter Fraud Database Tops 1,000 Proven Cases," ed. The Heritage Foundation (2017).
[469] Vitali Shkliarov, "“Dead Souls” to swing Georgia's presidential election?," *New Eastern Europe* 2018.
[470] Danah Boyd, "Facebook's privacy trainwreck: Exposure, invasion, and social convergence," *Convergence* 14, no. 1 (2008).

Zuckerberg explained that the information that was displayed on the News Feed section was public anyway. What he missed to say was that it should not have been displayed without the users' permission at all. However, a compromise was reached and in further Facebook updates, News Feed no longer contained that detailed information about users and users' friends. This did not mean it stopped existing, it stopped being public or that it stopped being collected. It was just not on display. Users, on the other hand, were happy that their personal information no longer appeared on their friends' News Feed which was, at the time enough for their relative sense of privacy on Facebook. One study found that users on Facebook do not even realize how their information is exposed and what consequences this may have for them[471]. In addition, another set of findings points to the conclusion that even when given more privacy settings control, the users are not always sure how to use them accordingly because they are simply not designed in a user-friendly manner.

In 2018, with a new privacy settings update, Facebook allegedly allowed users to have more control over their information on the platform. It gave them the chance to opt-out in case they do not want their information to be collected by third-party applications and companies. This opportunity not only intentionally skipped to resolve the big problem with data collection and data selling but was, in addition, unnecessarily tedious, time-consuming procedure in which users have to uncheck all of the boxes of the applications/companies collecting their information one by one[472]. Also, every time Facebook identifies a new interest of the user, the latter should go to the privacy control menu and opt-out. However, Facebook does not provide an indication of when a new interest is added to the users' profiles, meaning that the users have no idea when

[471] Burcu Bulgurcu, Hasan Cavusoglu, and Izak Benbasat, "Understanding Emergence and Outcomes of Information Privacy Concerns: a Case of Facebook" (paper presented at the International Conference on Information Systems (ICIS), 2010).

[472] Eric Griffith, "How to Prevent Facebook From Sharing Your Personal Data," *PC Magazine*2018.

their information is started being shared so that they can discontinue this process. A corporation with that many resources and employees as Facebook should be able to offer a more user-friendly way for users to opt-out from personal data collection all at once, but it did not, leaving the impression that the option to opt-out has been made so difficult only to make users not take advantage of it. In fact, such universal opt-out option existed in the past but for a very short amount of time because it was removed by Facebook, just to be replaced with much more restrictions on the users' control over their own information. This universal opt-out existed in early versions of Beacon – Facebook's platform that generates and posts advertisements "based on items a user purchased or browsed on the websites of some forty-four partner sites and shared this information with a user's friends via the News Feed"[473]. Later modifications of the platform in favor of more privacy were implemented in Beacon, but the platform ceased existing altogether in 2009 after a class action lawsuit for $9.5 million.

Further updates included "social plug-ins (which added "like" and "recommend" buttons to third-party websites without clearly indicating to users when and how their profile information might be shared with these websites), and 'instant personalization' (which allowed a few select partners to personalize their web pages by using personal information that Facebook disclosed without a user's explicit consent)"[474]. After targeted advertisements started being posted on the users' Timelines, as a consequence of tracking the users' clicks on the *Like* button, another lawsuit followed, and another settlement, this time with the U.S. Federal Trade Commission (FTC). Zuckerberg declared that Facebook would introduce more measures to protect users' information. What he missed to say was that Facebook also created even more conditions for

[473] Ira S. Rubinstein and Nathaniel Good, "Privacy by design: A counterfactual analysis of Google and Facebook privacy incidents," *Berkeley Technology Law Journal* 28 (2013).
[474] Ibid.

digital entrapment of users' personal information. Facebook has a long history of promoting digital marketing on its platform whose initial motto was to bring people closer together. At one point, it started bringing marketing content closer and closer to the users, at the expense of their privacy. It was just a matter of time for political marketing to enter the Facebook scene as well, again, at the expense of the users' privacy, their independent choices and the democracy, as the case with Cambridge Analytica showed.

Overview. In the early months of 2018, news outlets broke the story of Cambridge Analytica and its collection of personal information through people's Facebook accounts. Questions started to arise as the most central one was whether Cambridge Analytica violated any rules, or it was Facebook that allowed the controversial data collection. As Cambridge Analytica was not a well-known company, at least not to most people, including those whose data was collected, the case became even more confusing and shocking – it was revealed that it gathered information from 50 million Facebook users. Cambridge Analytica was a political firm engaged with collecting data for companies, aiming to influence public opinion and behavior. One of the owners of Cambridge Analytica was Robert Mercer – one of the most generous donors of the Republican Party. Another stakeholder was also Stephen Bannon – Donald Trump's political advisor in his 2016 election campaign. Allegedly, the firm offered its services to a variety of companies including Mastercard, the New York Yankees and Joint Chiefs of Staff[475]. They were also involved in the campaign advocating for Brexit – Leave.EU.

Cambridge Analytica claimed that it collected users' information in an effort to construct psychological profiles that consider patterns of what they like, who do they communicate with (based on their friends on social media) and identifiable personal information, including the

[475] Kevin Granville, "Facebook and Cambridge Analytica: What You Need to Know as Fallout Widens," *The New York Times* 2018.

users’ location. Then, it would use these profiles to make marketing more efficient by designing advertisements and other online content tailored specifically to the target audience. As the company was not able to accomplish this mission on its own, it sought to collaborate with some psychologists from the Psychometrics Center at Cambridge University. The latter developed in 2014 a study in which Facebook users were asked to fill out a survey about themselves and then to download an application that handed over the information from their profiles to the researchers. This process was something that was not forbidden by Facebook at the time, as it claimed users were informed about their data potentially being used for academic purposes. However, the official position of the Center for the potential partnership with Cambridge Analytica was to decline the offer. This was not the end of the story, though. Aleksandr Kogan, a Russian-American psychologist at Cambridge University, agreed to work with Cambridge Analytica on this project. Previously, he has been receiving grants from the Russian government to study psychological states of users in social media[476]. He designed an application for Facebook, executing similar functions to the one built by the Psychometrics Center and together with Cambridge Analytica began collecting the data of the Facebook users.

From the beginning of this partnership, it was clear that the gathered users’ information was not going to contribute to any academic agenda, or at least not only, as Cambridge Analytica is a firm whose main service is to use data for profit, selling it to clients for marketing and political marketing purposes. The users, both those who took the survey and consented to their information being used and those who did not, were told, that the data will be used for academic purposes. That led to the accumulation of massive amounts of data that totaled approximately 50 million users, only 270,000 of which, consented to their information being used for academic

[476] Carole Cadwalladr, "‘I made Steve Bannon’s psychological warfare tool’: meet the data war whistleblower " *The Guardian* 2018.

(but not other) purposes[477]. Violating the social platform's policy that the users' data must not be sold to for-profit organizations, Facebook announced in 2015 that the users' information was deleted by Dr. Kogan and Cambridge Analytica. In the meantime, however, it became clear that Dr. Kogan could not discuss any details of the case as a clause of a non-disclosure agreement with both Facebook and Cambridge Analytica. Shortly after Facebook announced that the users' information was deleted, it turned out that copies of this information were still in existence.

On March 2018, Alexander Nix, the CEO of Cambridge Analytica was fired. His suspension was, among other things, a result of a story that the British Channel 4 News aired earlier in 2018. One of their reporters posed as a potential client to whom Nix, through Cambridge Analytica's subsidiary company SCL Group, offered variety of techniques that would win an election, including hiring Ukrainian women to seduce the opponent and to extort them for the footage, or simply videotaping them in a compromising scene in which they allegedly take a bribe[478]. Nix was also caught discussing that among the clients of the firm were politicians in the Caribbean and African countries "where privacy rules are lax or nonexistent and politicians employing SCL have been happy to provide government-held data, according to former employees"[479]. Additionally, Nix mentioned that some of their clients were reluctant to hire a foreign firm as a consulting agency for elections, thus they could pose as students, tourists, and other roles they could assume to not raise suspicion because, as he himself said: "the moment you think 'that's propaganda,' the next questions is, 'Who put that out?'"[480].

Nix also declared that the company does not possess and use data collected through Facebook. Directly confronting this statement is a dossier, presented to the National Crime

[477] Granville, "Facebook and Cambridge Analytica: What You Need to Know as Fallout Widens."
[478] Matthew Rosenberg, "Cambridge Analytica, Trump-Tied Political Firm, Offered to Entrap Politicians," ibid.
[479] Ibid., par. 10.
[480] Ibid., par. 15.

Agency in the U.K. by Christopher Wylie, a Canadian who was at the time involved in the Cambridge Analytica's data collection. The dossier revealed a large amount of Facebook users' data, belonging mostly to U.S. registered voters[481]. Regarding the main focus of the company, Wylie shares that they "exploited Facebook to harvest millions of people's profiles. And built models to exploit what we knew about them and target their inner demons. That was the basis the entire company was built on"[482]. Some of the Cambridge Analytica's business was also linked to Russia's oil producer Lukoil, whose CEO is very close to Vladimir Putin. Lukoil, the second biggest oil producer in Russia, is also popular in other parts of Europe, typically used to spread Russian influence in gas-dependent countries. Records show that Cambridge Analytica has been asked to outline how their methods could work toward Lukoil's agenda. The presentation that was prepared by Cambridge Analytica was almost entirely focused on *election disruption techniques*[483] through *psychographic messaging*[484].

Applied measures against this threat. The measures undertaken as a result of the Cambridge Analytica case could be listed in two groups: legal measures and policy measures. In May 2018, Christopher Wylie was questioned before Congress. He has been cooperating previously, providing evidence to both the U.K. and the U.S. regarding the case, the former through its National Crime Agency and the latter through FBI. Most of the questions during the hearing aimed to explore the relationship between the disinformation that the Russian government agencies were spreading in the U.S. before the 2016 Presidential Elections and the data collection of U.S. voters. Witnesses in the hearing were also academics that testified that

[481] Carole Cadwalladr and Emma Graham-Harrison, "Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach " *The Guardian* 2018.

[482] Ibid., par. 3.

[483] Carole Cadwalladr, "'I made Steve Bannon's psychological warfare tool': meet the data war whistleblower " ibid.

[484] Ibid.

even if Cambridge Analytica had some effect on the results of the election, it is still unlikely that their actions pre-determined them entirely[485]. Regardless, in his previous interviews, Wylie was convinced their psychological profile-modeling had a serious impact on people's perceptions and decision-making. In addition, he admitted to another controversy that was officially acknowledged also by the U.K. electoral commission – that the *Vote Leave* campaign broke the electoral laws in the country as it was financially linked to one of Cambridge Analytica's subsidiaries in Canada. However, Wylie underlines that despite these revelations, there were absolutely no consequences for this illegal "change to the constitutional settlement of the country"[486]. Interestingly, while the companies and the people involved in this conspiracy could be liable, Brexit cannot be reversed based on the fact that the Vote Leave campaign broke the law by exceeding the spending limits determined by the Electoral Commission because the referendum had merely advisory character[487]. Moreover, it would be very difficult a causal relationship between the voters' electoral behavior and the campaign to be established, even if reasonable suspicion of this effect is beyond doubt for many people, scholars and politicians. Similar to the other cognitive threats discussed in this study, it is almost impossible to prove that certain actions seeking to influence someone's behavior were actually successful because of these actions, and not because of an allegedly independent decision of the social perceiver.

At the same time, changing its position multiple times, Cambridge Analytica accused one of their contractors for stealing the Facebook data in question but firing their CEO, Alexander Nix in the meantime[488]. In the second half of May 2018, they filed for bankruptcy. Facebook was

[485] Issie Lapowsky, "Senators Grill Whistleblower on Cambridge Analytica's Inner Workings," *Wired* 2018.

[486] Carole Cadwalladr, "Cambridge Analytica a year on: 'a lesson in institutional failure' " *The Guardian* 2019, par. 43.

[487] Adam Ramsay, "The High Court found that Vote Leave broke the law in a new way," *Open Democracy* 2018.

[488] Donie O'Sullivan, Jeremy Herb, and Manu Raju, "Cambridge Analytica whistleblower to appear before Congress next week," *CNN* 2018.

the next in line for hearings. Mark Zuckerberg's testimony before Congress did not deliver the expected answers. Moreover, the evidence made it clear that Facebook knew about the privacy breach and did not notify the users whose data were stolen. Instead, they decided to conduct their own investigation not informing the authorities and the affected users. The initial statement of Facebook was that it requested that the users' information be deleted immediately, but later it turned out that the information in question had other copies that were still in existence. Zuckerberg's responses to Congress were problematic in another way as well: some of them were statements contradicting some of the evidence. Zuckerberg claimed that Facebook provides full ownership of users' content online to the users and the company did not and does not sell their information to anyone. Contrary to this, Facebook permitted variety of companies, whose number was more than 150 allegedly, to "view private user data, including private messages"[489]. Among these companies were American ones (Amazon, Microsoft, and Spotify), but also a Chinese one (Huawei) and a Russian one (Yandex).

While digital privacy protection remains a grey area for the U.S., mostly due to extensive lobbying by companies, the EU took decisive measures even before the incident with Cambridge Analytica. Regardless, the legislative measures were adopted after the scandal broke out so the fines that Facebook had to pay were much lower than what it would have, had the General Data Protection Regulation (GDPR) been adopted earlier than May 25, 2018. This way, Facebook was only fined £500,000, which was the highest possible fine that the previous data regulation act from 1998 set, instead of the roughly £1.4 billion that GDPR stipulates for such violations[490]. After the news about Cambridge Analytica became public, Facebook tried to bring some clarity

[489] Kara Alaimo, "Mark Zuckerberg has lost all credibility with Congress -- and the rest of us," ibid., par. 5.
[490] Alex Hern and David Pegg, "Facebook fined for data breaches in Cambridge Analytica scandal," *The Guardian* 2018.

to its users about how it collects information and for what purposes. In April 2019, it introduced its updated policy that was supposed to be understandable and accessible to users. Despite the efforts, the policies remained lengthy, inaccessible and incomprehensible to many users. Moreover, Facebook still preserves some of its rights to share users' information with Instagram and WhatsApp, and other apps as the account-holders have two options, as a result: they can either accept this or just leave the social platform to avoid future unpermitted data collection.

While the popularity of the case when the news about Cambridge Analytica and Facebook first made the headline was high, it slowly started to fade away. The same happened with the investigations in the U.S., and in the U.K., except for the fine that the latter imposed on Facebook, as it violated an EU-regulation. In both countries, strong political campaigns (Donald Trump's campaign and the U.K.'s Vote Leave campaign) took advantage of Cambridge Analytica's algorithms and the data they obtained from Facebook. As Donald Trump is now the U.S. President and the U.K. chose indeed to leave the EU after its referendum, changing the status-quo will be undesirable for the people and institutions with interest in preserving it. However, there are some efforts by senators to alleviate concerns about privacy[491]. They are preparing a bill that will enhance the privacy protection of users. It is unclear, however, if it will pass, considering the strong lobby of social media and companies collecting and using personal data. While changing the current situation is not impossible, the attention to the issues at hand has to grow back, as it is currently low after the Cambridge Analytica's bankruptcy and the relative loss of trust in Facebook. The case with both, while unique, is just symptomatic of a bigger problem in society that is still unresolved – the lack of regulation for coercive persuasion attempts, especially in the online space.

[491] Jim Isaak and Mina J. Hanna, "User Data Privacy: Facebook, Cambridge Analytica, and Privacy Protection," *Computer* 51, no. 8 (2018).

As the issue seems mostly related to corporate and political interests, headlines fail to underline another tendency, inherent for the academia, for which Vito Laterza is alarming. In his testimony, Christopher Wylie confirmed that "a lot of the papers that eventually became the foundation of the methods that we then used…all came out of research that was being done at the University of Cambridge, some which was funded in part by DARPA, for example, which is the US military research agency"[492]. As Laterza states, a significant amount of the researchers and professors who are relatively new in their academic positions are required or strongly encouraged to secure external funding for their projects. Even for senior professors, seeking grants outside of their institution is a sign of "influence and prestige"[493]. However, when a professor's position and future professional development is dependent on external funding, they seek to secure it, regardless of the potential application (and its ethics) of the research's results. Laterza advocates for a conversation among academics regarding the integrity of research produced with external funding, as the latter appears to be almost mandatory element in the reputable academic's resume.

The four case studies described in this chapter point to different actors who intend the threat. They also show a variety of political reasons that give room to psychological ways of executing these threats. The perpetrators in these scenarios view differently what they have to gain and lose, and so do the victims as well. The case studies reveal a range of conditions, relevant for all three levels of analysis, that makes the cognitive threats possible. What unites them is that they are all pertaining to the human psyche as an engine for certain changes in society and its political life. They also demonstrate that the existing measures aiming to prevent

[492] Vito Laterza, "Cambridge Analytica, independent research and the national interest," *Anthropology Today* 34, no. 3 (2018): 2.
[493] Ibid.

future cognitive threats are with limited significance. Therefore, in the following chapter, I offer a detailed examination of the factors composing them, and how they can inform various strategies designed to counter the threat.

CHAPTER 5

CONNECTING THE DOTS:

STRATEGIES FOR COUNTERING COGNITIVE THREATS

As evident from Chapter 4, fighting cognitive threats after they produce their adverse consequences does not generate meaningful results. Considering this insight, another option to confront them becomes more promising. As opposed to fighting the threats, attempting to block the threat before it occurs or before it delivers damages, appears to be more viable strategy. It consists of some elements of deterrence as a state policy, and some other complementary elements that serve the same goal but are instead focused on actions by individuals, the community and non-state actors of significance. As a state policy, deterrence is fit to counter elements of cognitive threats that are made by state actors and to a lesser extent by non-state actors, as the relationship between state actors and non-state actors is not regulated as well as those between two or more state actors. State policies would be more efficient against another state-actor sharing the same political mindset as the deterring entity, and less effective against those that do not share the same democratic values. In addition to this, deterrence state policies aimed at non-state actors over which the state actor has control are more productive than those aimed at non-state actors that are outside the scope of control of the state actor. State deterrence policies have some effect on the psychological experiences of the individual, but there are other measures with a deterrence effect on individual and community level that are better equipped to influence the human psyche. This is true especially since the impact on individual and community level will be more direct as the democratic state cannot enforce limitations on some channels that are facilitating cognitive threats. Such measures by individuals and the community could be complementary to the state policies as their meaning is underlined through the close connection the individual has with others, first, and second, as they are all part of a collective entity that state policies can influence on a broader, more abstract level.

The following sections analyze the characteristics of the case studies described in Chapter 4 in an effort to construct deterrence strategies for a variety of cognitive threats. It will also seek to capture common deterrence techniques for all of them if any. The analysis is divided into two sections for each of the case studies. The first cluster focuses on the actors and the factors that are part of the cognitive threat. Mainly, who is the perpetrator, who is the victim, what is the relationship between individuals, state- and non-state actors, what is the perpetrator winning or seeking to win and what is the victim losing/have to lose, according to the actor's own perception, is anyone else involved in the case and how, and what are the factors influencing it. The second set of questions that will help elucidate characteristics of a prevention strategy pertain to the nature of the problem and the suggested solutions. In particular: does the threat represent any potential for war or not, does the threat entail rules and weapons inherent for wars, what is the political mechanism/explanation for the threat, and what is the psychological mechanism/explanation for the threat.

Countering cognitive threats in Russian espionage cases

In the case of Maria Butina, the direct perpetrator is Maria Butina's herself. To some extent, her handler Alexandr Torshin could also be counted toward the direct perpetrators since he was actively involved in the mission to influence U.S. politics. As the case study revealed, Maria Butina is not the first female spy, who gained popularity for her espionage missions. Anna Chapman, among other men and women acting as sleeping cells, was also a spy in the U.K., and in the U.S. While undoubtedly, among the Russian agents, there are many men, women are particularly influential and successful in their missions as they raise less suspicion and their intelligence-gathering can go undetected for years. As for the victim(s) in this case, the persuasion was mainly directed toward members of the gun-lobby in the U.S. as well as toward some other influential politicians from the more conservative political circles. However, they could be considered victims as long as they had no knowledge of Maria Butina's allegiance to work as a foreign agent in the U.S. on behalf of Russia. There are some indirect perpetrators and victims in this case as well. Maria Butina would not have been acting as a spy, perhaps, if she was not stimulated, recruited or even ordered by Russia to do so. While difficult to prove, it is also likely that except for Vladimir Putin, Butina and Torshin, other people also knew about her mission and contributed to making it successful. In this group of people would also fall Americans, if any, who knew and supported Butina in her task. The list of indirect victims in Maria Butina's case is long. It would have included every citizen and U.S. resident who would have been affected by Butina's attempt to persuade powerful politicians in becoming closer to Russia, complying with the interests of Kremlin and implementing them in the U.S. in various ways. The immediate target of Butina's mission was her direct targets' cognition, particularly its decision-making mechanism.

As for the relationship between perpetrators and victims, it could be described as existing on multiple levels. The first relationship is the state-state one in which the antagonistic relationship between the U.S. and Russia underlines the desire of each actor to influence the other in a manner beneficial to their own goals. Had these two countries not been rivals, the intensive espionage campaigns would not have been that common.

Probably the most important relationship dyad of all is the individual – individual relationship without which the entire cognitive threat would not have been possible. Maria Butina actively interacted with other individuals conveying her ideas and making room for even more influence in the future. Presumably, her boyfriend, Paul Erickson also did not know about Butina's real intentions, as she was convincing him gradually to work toward her and Russia's cause. It is also likely that Butina only simulated a romantic interest to Erickson so that she could benefit from his contacts and his own influence in the gun-lobby circles.

Another interesting set of relationships is the one between individual and state – on the one hand, Maria Butina's relationship with the U.S., the country that she was spying, and on the other hand, her relationship with Russia, the country on which behalf she was committing the espionage. Accepting the risk of being caught, Butina probably sees the U.S. as an enemy, the same way Russia views it. At the same time, her actions and the communication she maintained with her handler showed that she had a strong sense of duty to Russia and its political interests. In addition, her strong sense of identity and loyalty to Russia was questioned when she started wondering whether she will be able to return and live safely in Russia after her mission was about to be exposed. That could be attributed to the fact that the disruptions in the individual-state relationship also brought ontological insecurity. It is not quite clear by the evidence what was Butina's concern about Moscow's reaction to her potential exposure, but evidence suggests that she was feeling afraid of negative actions against her. Another relationship between individuals and the state is the one between the direct victims of Butina's persuasion with Russia, and with the U.S. For Butina to penetrate so deeply into the political circles in the U.S. meant that the politicians with whom she was interacting were not suspicious of the fact that she was Russian, even if officially being in the country as nothing else but a Russian student with a boyfriend who was a U.S. citizen. However, despite the dividing factors between the politicians that Butina was seeking to influence and Russia, they still had a very important common interest – the gun laws, their expanding use in both the U.S. and in Russia and the increased profits that would logically come from this. Considering this component, for the politicians to be open to Butina's arguments, they focused more on their common interest rather than on the antagonistic and full of mistrust relationship between their two countries.

Non-state actors, while not completely recognized as influential entities in international relations, carry the meaning of a catalyst in this case. Not directly named in court documents, though evident that the described facts pertained to them, the NRA played a key role in the case, as an intermediary between Butina and the conservative U.S. politicians supporting the gun-lobby on one side, and between the U.S. and Russia, on the other. Undermined by IR-scholars, non-state actors, in this case, made possible all the other interactions in this scenario – on an individual level, on a state level, and on an individual-state level. The NRA's goals were the overlapping point for the connection between all of the parties involved in this case. Regarding its own relationship to Maria Butina, she was a vivid supporter of the organization, being a member herself, making possible multiple meetings between them and high-ranked Russian politicians. Similar was the NRA's relationship to their supporters in the U.S. as well. In terms of their relationship with state entities like the U.S. and Russia, it was a little more ambiguous than their relationship with individuals from these countries, mainly because they interacted with such who support NRA's goals. NRA's relationship with the U.S. is very controversial. While the organization has multiple supporters and a very strong lobby that earns policy-makers' support for NRA's interests and goals, the organization also has fierce opponents - citizens, activists, organizations and politicians. Its relationship with Russia makes its position in the U.S. society even more criticized. NRA's relationship with Russia is also interesting because as a non-state entity, NRA is driven by profits as a main goal, rather than by concerns typical for states or individuals. Therefore, what is most conducive to NRA's not openly friendly, but not unfriendly relationship with Russia is an interest, expressed in terms of profits. Evidence for this is the meetings that NRA members attended in Russia. Ambiguous was the position of the then-president of the organization, as he was possibly concerned that the closeness with Russia would inflict a serious harm to their reputation in the U.S., which is after all the core market and the core reason, through legislation and culture, for the profits that their products bring.

Considering prevention strategies, it is essential to outline what the sides involved in this case have to win and to lose, what they perceive as a win and as a loss. It is essential to mention, however, that wins, and losses cannot be identified categorically, as there are different levels that could be reached in both categories. A win, in its entirety, may not be achieved, but there may have been steps toward it that brings benefits which could still qualify as gains. Then this would be if not a complete success, then at least relative one. The same goes for losses as well.

Russia has been unequivocally described in the literature as interested in weakening the enemy, as opposed to the ages of the Cold War when their tactic was to defeat the enemy altogether. This intention has changed ever since, and it now reflects Moscow's focus on disruption and controlling the adversary through cognitive mechanisms, rather than through traditional military force. Therefore, for Russia, a win would be to manipulate U.S. politics in a way, favorable to them. In the case of the 2016 Presidential Elections - against Hilary Clinton and supporting Donald Trump. Another important threat in the Russian espionage plan is to gain information that they can further use to manipulate certain people of power to serve Russian interests. While it remains unclear how much leverage Russia accumulated against U.S.

politicians because of Maria Butina's actions, it is clear that the more favorable to Russia candidate won the elections, and to that extent, Russia scored a win. A loss to Russia would have been exposing Maria Butina long before she connected to Paul Erickson and high-ranked U.S. politicians. However, the meetings between Russian officials and NRA members have taken place, a fact that testifies for another win that Russia scored – establishing a relationship between the countries, one that was carrying the potential for even further influence over the U.S. political life. For the executor of Russia's plans, Maria Butina, individually, things were not so black-or-white. While she succeeded to make connections and potentially persuade U.S. activists and politicians to be more favorable toward some of the Russian interests, even if they have not realized that these interests are Russian, she was exposed and convicted. It is still unclear, as her sentencing is still pending as of April 2019, whether she will return to Russia as a hero or will have another fate. Considering the example of Anna Chapman, it is likely that Butina will follow her steps, and will be warmly welcomed in Russia.

In terms of what the U.S. has to lose, the answer is clear – democracy and independence, both political one, and one pertaining to choices. Russian campaign against the 2016 Presidential Elections was conducted on multiple fronts and the extent to which the particular case with Maria Butina's influence affected the general outcome of the elections is not entirely clear. However, if there was any influence at all, this should be perceived as a loss for the U.S. democracy –even though she was exposed and brought to justice. This assumption is supported by previous cases of Russian espionage in the U.S. in which the agents were caught and sentenced but the information they reported back to their handlers, the influence their exercised could not have been reversed. Besides, more spies were sent, with new missions, bringing new ways of disrupting democracy. The politicians, through which Butina was exercising influence also lost the cognitive battle, assuming they were not aware of Butina's real intentions. Had they known about them, they would have also risked a trial and a sentence for helping her with her plans.

Variety of factors also played their role in Maria Butina's case. First and foremost, culture. The American openness to the world, especially in terms of education kept Butina out of suspicion initially, as she was a student in a prestigious university from which later, she successfully obtained a graduate degree. Other countries, mostly authoritarian, are much more suspicious of foreigners, regardless of the occasion on which they are traveling. Another element in the U.S. is the gun-culture that opened the door to an intensified communication between Butina, Torshin, and other Russian politicians, on the one hand, and Paul Erickson, NRA, and members of the Republican Party in the U.S. The support that the gun-lobby enjoys in the U.S. both by politicians, and people, made the interaction between Russia and the NRA and their supporters, somewhat permissible from both political and moral point of view. Maria Butina's attachment to guns is also an indicator to a broader phenomenon. In one of her interviews, she admits that growing up in Siberia, guns were an absolute necessity for survival. As this is most likely the case indeed, it is intriguing that Butina sees herself and other people from the region as solely responsible for their own survival, not mentioning or recognizing the state's role for these conditions. Many residents of democratic countries would try to require the government's actions to ensure safe living conditions. At the same time, the Russian identity is very strong as one of its main characteristics is the responsibility of the citizen to the state, as opposed to the other way around. This culture shaped Maria Butina's thinking and, to a large extent, her determination to execute missions assigned by the Kremlin, even if they pose a severe risk of her being incarcerated, if exposed.

Another component that has its place in this case, is profits and power. For the relationship between Butina and Russia, and NRA and conservative politicians supporting it, there has to be a mutual interest. The NRA saw an opportunity for market expansion in collaborating with Russian officials, and the latter saw a possible way to influence U.S. politics through the NRA. The tripod profits-power-influence is particularly inherent for Maria Butina's case. Other espionage cases, while similar, typically do not include intermediaries that are, on the one hand, part of the adversary's political life and on the other, maintaining open channels of communication with entities perceived by the state as enemies. Interestingly, the NRA's role in the U.S. regarding the Russian interests resembles the one that far-right political parties have in Europe. Through them, Russia attempts to influence adversarial countries, especially in cases of disinformation.

Espionage is a traditional practice during war; it being *hot* or *cold*. After the Cold War, the Russian espionage did not disappear, it simply continued in the form of sleeping cells and its mission transformed into exercising influence to change the political course of the adversary. Despite Russia executing espionage-campaigns in the U.S. and in other countries in peacetime, even when exposed, such cases do not raise concerns about any potential war actions but instead just reaffirm hostility that has always present between the two countries. This fact is a double-edged sword, however. On the one hand, politicians feel certain that even if espionage cases are revealed, this will not escalate into a war. On the other hand, this is very bad news for deterrence of the enemy because the latter knows no further actions will be undertaken even if a spy's identity is exposed. The rules inherent for this peacetime conflict resemble the ones in wartime, mainly regarding the exchange of prisoners, as the one in Vienna between Anna Chapman and the other captured Russian agents, and agents captured by Russia proves. Other than the exchange of prisoners, another reaction to exposed espionage is political signaling through judges, U.S. attorneys, politicians and activists that aim to convey to Russia that their campaigns failed. The truth is, however, that, as I explained earlier, a win in espionage cases is a flexible notion because every intelligence-gathering task reported to handlers constitutes a little win for Russia and a little loss for the U.S. Just because, after some time the agents' operations were terminated, and they were sentenced this does not mean that harm has not been inflicted by them, even if it ended, eventually, with a court ruling, prison time and extradition, in cases in which the spy is a foreign national.

From a political point of view, the influence that Butina and Russia exercised could be attributed to a few reasons. First, the antagonistic relationship between the U.S. and Russia. Second, the state-supported espionage campaigns of the latter and the former's overall openness to foreigners, especially for educational purposes. Third, the overlapping points of interest between Russia and U.S. entities mostly related to the gun-lobby and the conservative circles in the society.

A very important element in the analysis of Maria Butina's case are the psychological mechanisms that made the espionage and its success possible. The factor that probably unites all the agents working for the Kremlin is their identity. The Russian identity before and during the Cold War was predetermined by imperialistic ambitions and thus having an imperialistic character[494]. After the end of the Cold War, Russians underwent a new identity formation that could have either assumed imperialistic characteristics from the past or reorient toward a more liberal understanding of the world in which Russia would have had its place among the other nations, brought closer by international institutions and norms. In 1996, Chafetz wrote that if the

[494] Yuri Teper, "Official Russian identity discourse in light of the annexation of Crimea: national or imperial?," *Post-Soviet Affairs* 32, no. 4 (2016).

statist and authoritarian powers in Russian politics take prevalence over the more liberally inclined ones, as it happened, then this “will reduce Russia's dependence on the West and deprive the West of leverage against possible Russian violations of international norms. Moscow under the statists, for example, is far more likely to intervene unilaterally against its neighbors to protect the Russian Diaspora than it would be under the leadership of the liberals”[495]. As this vision in 1996, becomes a reality in the two decades after this, central to the Russian identity remain imperialistic longings, also supported by the rhetoric that a key-influencer of the Russian identity has – the Russian Orthodox Church[496]. According to its narrative, traditional values have to be preserved at all cost, especially in times in which they are so severely endangered, mostly by the West, seen as an enemy bringing decay to the morality of all Slavs that Russia seeks to protect. Such narrative patterns, while not identical to the ones that the Soviet Union distributed, still strongly remind such ideas. Therefore, generations of Russians, either born in the Cold War era or afterwards were a product of identity formation that to a large extent retained the dimensions of the one inherent for the years of the Soviet Union. An example of this is the fact that Anna Chapman’s father was a former KGB agent, and Chapman herself was a Russian spy. Among the central elements of this Russian identity are patriotism and loyalty, as “in the Russian tradition, the notions of state and civil consciousness do not match, therefore a civil identity means belonging to the state”[497]. Evidently, the idea of the state in the mentality of Russian society has a very important role and is placed on a pedestal. Considering these insights, it is no wonder that so many young Russians are willing to put themselves in service to the Kremlin as

[495] Glenn Chafetz, "The struggle for a national identity in post-soviet Russia," *Political Science Quarterly* 111, no. 4 (1996).

[496] Alexander Agadjanian, "Tradition, morality and community: elaborating Orthodox identity in Putin’s Russia," *Religion, State & Society* 45, no. 1 (2017).

[497] Anatoly Vladimirovich Lubsky et al., "Russia in search of national integration model," *Mediterranean journal of social sciences* 6, no. 4 (2015): 210.

spies, risking exposure, being brought to justice, and sentenced in a foreign country. For them, this is simply a patriotic duty, an honor, part of who they are, in some cases, part of who their parents and relatives are. In Maria Butina's case, there was also another element that contributed to her mission – her persuasiveness that helped her avoid suspicion for a long period of time. Additionally, from a social-psychological standpoint, there was something about Butina's target audience that facilitated her mission. Mainly, it was an element of a sub-identity that Butina and her targets all shared – the support of gun rights.

Measures toward the indirect perpetrator – Russia. The first and the potentially most effective and invasive mechanism through which the Russian espionage could be countered pertains to a campaign that the U.S. can launch as a form of potential retaliation that could deter Russia. It should seek to inform Russian citizens about opportunities for civic engagement and actions to make the state itself more involved in domestic issues. Moreover, in some impoverished Russian regions, it is evident that the Kremlin has not done much to assure its people's welfare, in terms of socio-economic and political conditions. As the Russian espionage is an old strategy from the Cold War that just adapted to the new environment in the 21st century, the U.S. can also successfully employ some of its old weapons against the Soviet Union, weapons that led to the end of the Cold War with the symbolic victory of the U.S. What led to this victory was the collapse of the Soviet Union, which, among many other reasons was caused by people's desire to stop being isolated, economically, politically and informationally. Offering Russian people information that will empower them to be more politically and civically engaged, and to advocate for improvements in their welfare will be a step forward toward less authoritarianism.

The brutal repression of the Russian opposition and violence used against political protesters, especially in urban areas[498] is a clear sign that while Putin does not seem intimidated by many things, including the financial sanctions of the U.S., he fears a strong, active society that demands changes and a better future. The information campaign could be implemented in a variety of ways including VKontakte – the Russian version of Facebook. It is important, however, that the language used in the campaign is Russian and not English because the information may be regarded as false just because of the source, allegedly a foreign one, since the used language is not Russian. Once the U.S. shows Russia that such campaigns can be a credible threat, they could be used as a deterrence against future espionage cases, assuming that Russia unambiguously understands that the campaign is a result of another wave of captured Russian agents in the U.S. In terms of any concerns that this campaign may violate international law, the official UN language used to regulate interventions in foreign states constitutes that UN-members should not "intervene in matters which are essentially within the domestic jurisdiction of any state"[499]. A non-coercive influence as a result of an information campaign could not be understood as an intervention in this sense, especially since the Russian people's independent formation of civic position does not fall under the Russian jurisdiction. Moreover, an information campaign, containing real statistical data about Russia's economy, is not a crime. Instead, it is an expression of the democratic right to receive, send and exchange information. Even the proven Russian cyber interference in the U.S. Presidential Elections in 2016, for which Russian officers

[498] Cameron Ross, "State against civil society: Contentious politics and the non-systemic opposition in Russia," *Europe-Asia Studies* 67, no. 2 (2015).
[499] United Nations, "Charter of the United Nations, Chapter I," (2019), Article 2, par. 7.

were indicted, is unlikely to have any consequences, mostly because both U.S. and Russia have repeatedly interfered in foreign elections during the Cold War[500].

Measures toward the direct perpetrators – the Russian agents. A second mechanism is a variation of the one described above, but its target will be the Russian people, convincing them in that while they are loyal to the state, the state also has some responsibilities to its citizens that it does not execute very successfully. The reason for the poor welfare conditions should be attributed to the state's failure to provide them rather than to an external enemy, the defeat of which will bring prosperity and solution to internal state problems. Thus, the goal would be that potential Russian agents start questioning the extent to which they could be used in Russia's political maneuvering against the U.S. It is true that people's identities are difficult to change but they are, nevertheless, not perpetual but a subject of possible alterations. An example of such identity changes are the events that led to the Jasmine Revolution[501].

Measures toward the direct victims – the individuals. A third mechanism that considers the direct victims of espionage – the targeted U.S. individuals should envision the expansion of the awareness of the problem. In particular, the media have to pay more attention to summarizing cases of Russian espionage, the success of women who conduct it, as well as cases involving men. Another component that Americans, especially those assuming a public office or having political influence over the government should be vigilant for are foreign nationals, especially such from Russia, who are either too observant and silent or too active and engaging. Lastly, such U.S. politicians, activists and people of influence should be aware that even if they share some common interests with foreign nationals, seeking to establish friendly relationships, there is

[500] Andrew Fletcher, "Russian Hacking and the U.S. Election: Against International Law?," *Michigan Journal of International Law (MJIL)* 38 (2016).
[501] Naseema Noor, "Tunisia: The revolution that started it all," *International Affairs Review* 2011.

a caveat. By working toward the common goal that Americans and Russians have in mind, the former may not be aware that they will unknowingly fulfill a lot more than just the agenda of the collaborating individuals but the one of an entire country seeking to destabilize another.

Measures toward the indirect victim – the U.S. A fourth mechanism with a focus on the U.S. will be to change the narrative about Russia in an effort to stop vilifying it and therefore to present itself to the Russian people not as an *enemy*. Another long-term option will be that the U.S. attempts to change the antagonistic relationship with Russia. Regardless, considering decades of antagonism and the current political climate, the best course of action could be changing the narrative about Russia, rather than the relationship itself. Changing the relationship with Russia will be better than changing the narrative but very unlikely if the political status-quo in Russia and in the U.S. persists. In addition to this, the U.S. should be aware of potential points of contact between U.S. entities and Russian ones as it is evident that Moscow uses intermediaries from the adversary's domestic political scene that do not mind communicating and collaborating on shared goals with Russia.

Countering cognitive threats in Russian Disinformation cases

In terms of the perpetrators, similar to the case with Russian espionage in the U.S. is the one with the Russian disinformation campaigns. As these operations were supported by Russia, through the creation of the Internet Research Agency, the number of the state-actor victims from this campaign is much wider. Russia is the power behind the operation but the people executing the orders were not volunteers, but instead, paid to spread disinformation through social media and websites posts. According to former employees in the Internet Research Agency, located in

St. Petersburg, more than 600 people were engaged with the spread of disinformation[502]. They worked 12-hour shifts, as the related duties were continuing for the full 24-hour cycle of the day. Their mornings began with an e-mail with links leading to websites where the disinformation was supposed to be placed. Some of the employees were incentivized by the relatively good salary and the fact that they would have been, otherwise, unemployed. While the U.S. was among the main targets of such campaigns, it was not the only one. The EU-member states were also targeted. The countries in Eastern and Central Europe are more vulnerable as they still have some Russian-speaking population within their borders or a significant population that has pro-Russian political views. The Russian disinformation campaigns were tracked even beyond the EU and the U.S. as they reached some other countries as well such as Armenia, Azerbaijan, Finland, Moldova, and Serbia. Despite that state targets are the main actor that Russia intends to harm in the disinformation campaigns, the direct victims are the individuals who read the disinformation content and react in a certain way, typically in a manner that Russia intended – behaviors that express protest, anger, sadness, division, and exclusion of particular groups of the population. An interesting paradox is the dual capacity in which individuals who perceive the disinformation act. On the one hand, they are victims but unconsciously they also act as perpetrators themselves, spreading the disinformation, not knowing that it falsely represents facts.

The relationships in the cases of disinformation are mainly three, one that concerns the state-state ties, another that pertains to the one that individuals have with a state, and a third one that represents the one between the different individuals involved. The relationship of Russia with the countries in which it disseminates disinformation is generally antagonistic, though, there

[502] J. J. Green, "Tale of a Troll: Inside the ‘Internet Research Agency’ in Russia," *Washington's Top News* 2018.

are various degrees to this. The most intensified campaigns were conducted in the U.S., Ukraine, and in the EU, as these three entities were also outlined as Russia's biggest rivals, according to a survey conducted in Russia[503]. When it comes to the EU, not all of the member-states are targets, but only the most influential states that have a greater role in maintaining the EU itself, and the ones in which Russia has geopolitical interests at stake.

In terms of the relationship between individuals and states, it should be mentioned first what is Russia's relationship with the individuals paid to disseminate information, and also what is its relationship with the ones for which the disinformation was intended. Information from former employees in the so-called *Troll factories* in Russia shows that among the most important reasons for people to seek employment in the Internet Research Agency was the lack of sufficient financial means or unemployment. Some of them were not aware about the nature of the job and quickly became disappointed by their daily duties. As opposed to the case with Russian spies, who were motivated among other things by patriotic duty and sense of identity, the employees in the Internet Research Agency were not so dedicated to implementing Russia's strategic goals but were inclined to participate purely for the monetary compensation. As for Russia's relationship with the people to whom it was conveying the disinformation, it could be claimed that the Kremlin sees individuals living in political rival countries as targets, vehicles for a desired change of the democratically established status-quo. As for the attitude of victim state-actors, such as the EU and the U.S., they treat the individuals posting disinformation posts in a dehumanizing way for which the multitude of articles repeating the noun *trolls* testifies. While it is true that these individuals are indeed doing a lot to make the disinformation campaigns successful, they also undertake these functions because of their employment, their need of

[503] ЛЕВАДА-ЦЕНТР, "Враги России."

income. Many of these individuals quit working for the Internet Research Agency after they find out about the nature of their duties. At the same time, while they are harming states with their online activities, it should not be forgotten that it is not volunteering that drove them to the Internet Research Agency, but financial incentives. The relationship between the direct victims of the disinformation operations and Russia also deserves some attention. Many of the social perceivers of disinformation are predisposed to trust such content because their own beliefs may overlap with the values that Russia seeks to promote – anti-globalization, a comeback to traditional values of the Orthodox Church, anti-immigration and anti-liberal values. Some victims of disinformation content do not share these values but may believe in the accuracy of the claims simply because a friend of theirs who happens to have views identical to those in the article shared or liked it in the social media. That said, individuals who have pro-Russian views, or interact with people with pro-Russian views may be much more vulnerable to disinformation and thus the main targets of these campaigns.

The last relationship that is going to be explored in this section concerns the individuals in this case – the ones who are victims of disinformation and the ones who disseminate it. Since the employees engaged in disseminating disinformation execute their tasks, as assigned, it is likely that they do not realize the full effect of their actions. Moreover, since their job is mostly in the online space and they do not see the recipients of their messages, their reaction and the broader effect it has, this anonymity helps them detach from what they are required to do and to depersonalize their victims[504]. At the same time, many of the disinformation recipients are not aware that what they read is not produced independently by journalists or independent bloggers

[504] John Synnott, Andria Coulias, and Maria Ioannou, "Online trolling: the case of Madeleine McCann," *Computers in Human Behavior* 71 (2017).

but instead is manufactured by a state-sponsored disinformation/propaganda factory seeking to polarize societies.

Analyzing what the sides involved in this conflict have to win and lose in the disinformation campaigns, it is easy to discover similarities between the case of Maria Butina and the disinformation ordered by the Kremlin against the Western allies and some Eastern countries with geopolitical significance. In particular, Russia seeks to destabilize these countries, weaken them and ideally, when the disinformation operations are conducted during important elections, to bolster the candidate that is friendly to the Russian interests. Moreover, in countries with a large Russian-speaking population, there is also another factor that was already mentioned previously – the attempt to erase their history and to convince them that Russia has a major role in it. Through the narrative change, the Kremlin seeks to expand its influence in Eastern and Central Europe but also to undertake even further actions, if possible, as the case with Crimea showed. In this context, since Russia seeks to destabilize, a win marked by the disinformation campaign will indicate varying degrees of weakening the rival, as an ultimate victory could be identified only in cases in which the disinformation helps the pro-Russian candidate in an election win. Another possible scenario of an ultimate win would be a civil war to break out in one of the countries with Russian-speaking population thus opening space for Russia to intervene in other ways, including militarily. The losses of countries - targets of the Russian disinformation could be derived by what Russia has to win with this approach. It should be underlined, however, how a win looks like in the eyes of the affected by disinformation countries. This would be a situation characterized by lack of disinformation campaigns or lack of effect of the disinformation campaigns on independent decision-making, on the civil peace, and on important elections and state affairs. As mentioned, there are also varying degrees in winning the conflict, as well as there are in losing it. For instance, a decrease in the number of fake news or in the successful Russian influence over independent decision-making will also mark a win, even if not an ultimate one.

Next, I would like to dedicate a few sentences to the effect of disinformation to the direct victims of it – the individuals who perceive it. Probably the most serious caveat hidden in disinformation is that the recipient of the message thinks that the newly perceived information actually benefits their decision-making by enhancing the amount of information that they have on their disposal. Contrary to this, it clouds the independent decision-making by imposing a view on a particular topic. This view is, in fact, the view of the sender of the message as the latter has the clear intention to coercively influence the perception of the recipient, thus making their judgment anything but voluntarily and freely formed. In an ideal scenario, a victory for the individual decision-maker would mean access to perfect information based on established facts, without external interpretations that inevitably reflect a particular point of view. While difficult to prove if this is the case at hand, an ultimate loss for a social perceiver would mean that they formed a decision that was expressed through their behavior only on the basis of the disinformation planted in their cognition.

The last section discussing the wins and the losses for the participants in the disinformation conflict is focused on the direct executors of the disinformation program. As the situation could be described in more concrete terms for other participants, many of the employees in the Internet Research Agency felt ambiguous about their activities, thus what would constitute a win for them is difficult to be defined. However, as the central incentive for what they are doing is money, a win would be to perform their job duties and receive the promised payment. That is valid only if the employees do not realize or are not concerned about the damages that their posts inflict. If they realize them and from this realization sense of guilt surfaces, then the win will be mixed with some moral losses as well.

While it is evident what is the chain of actions and results in cases of disinformation, somewhat peripheral remain the intermediaries that make the disinformation so successful. To some extent, it is known that websites, social media companies, and online search engines, have a crucial role in making the disinformation process possible. However, legally and morally, they mostly remain blameless because first, they do not want to exercise censure over content, and second, are not legally responsible for the type of information shared through their platform. Gradually, with the spread of disinformation, public opinion and policy-makers forced social media to enforce some limitations to the spread of disinformation. There were some boundaries to these restrictions because the central premise of creating a company is so that it can make profits. These profits, in the current market conditions, are made possible through the "attention economy where the most valued content is that which is most likely to attract attention"[505]. Therefore, it could be reasonably argued that disinformation was not hurting social media but just the opposite – it entailed more clicks, more attention, more shares, more likes, more discussion, and more profits. Having these facts in mind, while social media and the websites related to it are definitely part of the problem, they could be difficultly influenced as part of a solution. In the market economy, they are allowed to seek profits, the same way that public opinion and policy-makers seek restrictions to the spread of disinformation. These conditions shape a dilemma that makes any deterrence strategies focused on the intermediaries in disinformation cases likely to fail because of the conflicting interests of the actors involved. As for the society's role in the disinformation cases, it eagerly absorbed the *attention economy*

[505] Alice Marwick and Rebecca Lewis, "Media manipulation and disinformation online," *New York: Data & Society Research Institute* (2017): 42.

culture that slowly established itself as the dominant culture in the free market countries. As even reputable media started using more and more alarming and attention-provoking articles, the readers were paying less and less attention to headlines that merely stated facts without any implicit emotion-provoking agenda. This led to even more profits generated by the use of emotion-inducing headlines and entailed a decreased awareness of disinformation-disseminating articles that have almost the same alarmist character as the mainstream media.

Disinformation being one of the oldest weapons in warfare, it is not surprising that is still used in present days, even in peacetime, as channels and opportunities for communication grew exponentially in the past few decades. As an ancient and already known weapon, disinformation does not carry a risk of retaliation involving military means. Moreover, disinformation does not even constitute a crime, unlike espionage, for which the perpetrator can be punished, unless the disinformation opens the door for a defamation lawsuit. The process of Russian disinformation typically exploits the freedom of speech and of free information exchange through channels offered mostly by private companies, supposedly with no political interest invested in the opinions shared through them. As opposed to the years of the Cold War, when some of the most common sources of disinformation were the government-owned media, in the post-Cold War period, the disinformation spread by the Kremlin relies on the exploitation of democratic freedoms with the goal to make them work for an undemocratic agenda. While disinformation is not a crime and it is not a reason for war actions by itself, it is not considered unproblematic because it utilizes allowed means to achieve a forbidden result – interference in the domestic affairs of a foreign country. Considering these characteristics, the rules inherent for conflicts caused by disinformation campaigns should not be the same as those inherent for war conflicts. That said the only reasonable means to deter these operations should be actions permitted by the international law that will not lead the antagonistic relationship between Russia and its disinformation victim-states to escalate into hostilities.

The political mechanism that makes the Russian disinformation operations possible is the inimical relationship between Russia and some countries (such as EU-member states and the U.S.) on one hand, and countries that are object of Russia's geopolitical interests (countries in Eastern Europe and Asia, envisioned as part of the Eurasian project), on the other. In the disinformation campaigns, Russia sees the readers of disinformation content as a means to an end – to disrupt independent decision-making and influence the public opinion in a favorable to Russia manner. Disinformation is also made possible by the difficult economic conditions in Russia and the fact that many people do not have sufficient means for survival, which turns them to seek employment by the Internet Research Agency. Highlighting these circumstances, the following chain of actors and their actions becomes evident: Russia hires employees disseminating disinformation, they use social media to spread it, readers perceive the disinformation from social media and subsequently demonstrate attitudes consistent with Russian foreign policy goals. While influencing the outcome of elections in rival countries are among the most central goals in Moscow's strategic plans, disinformation is not and should not be perceived as a phenomenon that is only limited to such events. Disinformation seeks to cast doubt in values, to discredit politicians, to alter the course of decision-making on significant state problems, to polarize societies and plant the seeds of mistrust and contempt.

The three main mechanisms that could best explain disinformation are persuasion tactics, the confirmation bias and the preference to social networks constructed of like-minded individuals. The first mechanism is a broad category that includes the psychological tools to make the disinformation trustworthy. Namely, they evoke strong emotions that cloud the recipient's judgment as the conveyed information creates an anxious state in the individual's mind. In this *crisis state* induced by the alarming headlines, they look for more information, typically found in the article itself, thus automatically considering it as more trustworthy than it actually is. Moreover, the disinformation articles, in order to appear more credible, have some evidence supporting the inaccurate facts presented in the text. In the previous chapter, it was mentioned that, according to studies, even if false evidence is provided to support a particular false claim, the claim immediately becomes more reliable in the eyes of the reader. The topics that Russian disinformation exploits are proven to have a more notable impact on audiences that already have a predisposition to believe in the facts offered in the article, which tendency could be attributed to the confirmation bias – the inclination of people to interpret new information in a way that simply confirms their already formed views on a particular issue. Research also provides an evidence for another component that makes disinformation possible and rapidly expanding across social media – people's social networks. The human psyche is constructed in a manner that seeks to create relationships with like-minded individuals. A reason for this is the inherent desire to avoid cognitive dissonance (the opposition between attitudes and expected behavior). Thus, individuals seek to create social networks in which the members of the group typically share similar views, or at least for the most part in order to avoid cognitive dissonance. Therefore, if one of the group members perceives disinformation as reliable information and shares it with like-minded group members, it is likely that the latter will consider the information as reliable. This phenomenon occurs because first, the secondary recipients learned the information from a person who they trust, even if this person is not the original source, and second because the information overlaps with previous knowledge that the individual holds in their cognition.

Measures toward the indirect perpetrator – Russia. Focusing on the fact that Russia targets mostly countries that it considers rivals or such that are slipping away from its influence and moving toward the West, diplomacy measures are among the first ones to be mentioned in order to alleviate the tendency for Russia to feel threatened. Especially useful in this regard may be cultural ties that express the West's appreciation of Russian culture and art and their significant place in the world's history. This strategy may be even more critical in former Soviet states about which Russia feels that they are escaping from its influence, denying its importance and the values it treasures. Through such diplomatic means, a strong message could be sent that implies that Russia's importance could be recognized without it having to erase the influence of the West. Thus, Russia will receive some certainty about its position in the minds of European people, and at the same time will begin to see some of the countries, if not all, less as enemies and more as entities that acknowledge Russia's cultural legacy. Additionally, this way it will be harder for Russia to portray the West as an enemy that demeans Russian importance in Europe and in the world. Evidence that shows support for the potential success of this strategy is the fact that Russia perceives the EU as a coalition that refuses to acknowledge and treat it as a European state when it comes to discussing matters pertaining to the continent[506].

As opposed to this defensive, diplomatic step, a more offensive measure that could be undertaken regarding Russia as disseminator of disinformation is for state leaders of affected countries to officially recognize disinformation as an imminent threat with severe consequences, and Russia as a perpetrator, along with other entities that support its activities (nationalist parties, etc.). It is essential that in official statements, the people executing the disinformation, the so-called *trolls*, are not vilified but humanized and described through their involvement in these

[506] Fyodor Lukyanov, "Russia–EU: the partnership that went Astray," *Europe-Asia Studies* 60, no. 6 (2008).

operations mostly because of monetary and not political incentives. Currently, by vilifying not only Putin and disinformation, as his weapon, but also the Russian people who generate it and spread it, the West confirms its negative attitude toward the Russian nation and its population rather than expressing disapproval only toward its leader and the oligarchs close to him.

The public statements distributed by state leaders should also be bolstered by evidence showing Russia's involvement in the campaigns so that no doubt is left in the minds of the citizens that what they read in less-reputable sources may be a misleading content distributed as part of the disinformation operation of Russia. This method will also serve as a prevention strategy directed toward the consumers of disinformation, as it will increase their awareness of the ongoing cognitive threat against them and their countries. Paul Goble advises that state leaders expose disinformation as it represents "always a conscious policy and part of a larger policy agenda [and] not simply dishonestly of this or that official in response to a particular event"[507].

Another weapon in the arsenal against disinformation is the information campaign that was suggested as a measure in the fight with espionage. Maintaining a state that could be hardly described as a democratic one, Putin has proven on many occasions that he fears democracy and liberal rights for his citizens. The examples also include the oppression exercised over Putin's critics. In an effort to silence them, he even resorted to violence, as there are multiple cases involving poisoned dissidents[508]. Since democratic thinking and strong civic society are an unwanted obstacle to Putin's goals, according to his treatment of the opposition and the activists, then this could be a key to a stable strategy to counter the problem. There is one difference between the information campaign recommended for cases involving espionage and those

[507] Paul Goble, "Lies, damned lies and Russian disinformation," *Eurasia Daily Monitor* 13 (2014): par. 10.
[508] Elias Groll, "A Brief History of Attempted Russian Assassinations by Poison," *Foreign Policy* (2018).

involving disinformation. In the latter, there should be an emphasis on the Western consumers of disinformation as victims, and not enemies, which will humanize them in the eyes of Russian society. The information campaign may also focus on real stories of people reading disinformation content: how they happened to read it and how it changed their thinking about issues. Such accounts may lead to the Russian people making a parallel between their own experiences with Putin's disinformation and propaganda machines in the face of state-owned media, such as Russia Today (RT). Moreover, for this strategy, it will be crucial that Russian Internet Research Agency employees are not vilified but portrayed, together as the consumers of disinformation, as victims of Putin's illiberal regime. The narrative should include that, on the one hand the government forces people to take part in state-sponsored cognitive manipulation campaigns against independent thinking because many Russian citizens are left without a job or with an insufficient income, as this lack of choice leads them to join the Russian Internet Agency. On the other hand, the victims of disinformation, innocent people who are involuntary participants in political games, also suffer from Putin's strategic goals, just as much as the people employed to cause this harm, part of an operation designed by the Kremlin.

Measures toward the direct perpetrator – Internet Research Agency employees. A continuation of the solution to the disinformation problem focuses directly on the Internet Research Agency employees and mainly on the reasons they had to become part of it – money. This strategy can be labeled as neither offensive nor defensive. It aims to deprive Putin of hiring even more people who will execute his disinformation plan. NGOs and the private sector may directly target employees of the Internet Research Agency through advertisements in Russian, offering them alternative employment with a better compensation than what they would obtain if they stayed with their current employment. Sources say that in 2014 an average employee at the

Internet Research Agency made around $700 per month[509] – a salary that is below the minimum wage in the U.S. for the same year ($1,160), for instance. Even if most of the employees have no qualifications at all, their minimum wage, if employed by a U.S. entity will be higher. Evidence shows, however, that not all of the labor in the agency was unskilled. Among the employees working there were well-educated people such as journalists and writers[510]. Moreover, if it is assumed that an information campaign for Russian people is indeed a viable strategy undertaken by the West and its allies, then Russian-speaking people who know the Russian culture and the primary sources of communication will be an essential part of the campaign. Thus, Internet Research Agency employees would be discouraged from continuing to work for the Kremlin by Western employers offering them better remuneration. Furthermore, these same employees can be hired in campaigns to inform their co-citizens for their rights and benefits if the Russian regime was more open to the world.

Measures toward the direct victims – the disinformation consumers. As digital information and digital communication have become an integral part of life in the 21st century, it would be reasonably expected for educational systems to reflect the changes in technology and society. While many countries already developed traditions in information literacy, it is still mostly at the higher-education level rather than on an early-education level, especially in countries with lower GDP. Moreover, as it was previously emphasized, Central and Eastern European education systems rely more on memorization rather than on critical thinking. Additionally, the post-Soviet influence in these countries is still active and seeks to change the history in a way that assigns Russia a more prominent role in these societies, their history, and their culture. Therefore, a vital step is implementing information literacy courses, lectures,

[509] Simon Shuster and Sandra Ifraimova, "A Former Russian Troll Explains How to Spread Fake News," *Time* 2018.
[510] Ibid.

activities and awareness in schools as these educational methods should begin at an early age – possibly when children start using computers, other devices, and social networks. Students should be taught what disinformation is, how it differs from other phenomena, how to recognize potential disinformation and what to do with it. This way, the children will be capable of recognizing the seriousness of the problem and react in a civically responsible manner. As for the education systems in Central and Eastern Europe, the EU, NGOs and other entities should vigorously encourage implementation of critical thinking and a more comprehensive approach to teaching history and other subjects. Quality education is especially important since many of the textbooks, produced in the first years after the end of the communism, were written in a way that does not reflect major world events (e.g., the Cold War). In countries with a large Russian-speaking population, it is also important consumers of all ages to be offered reputable media, traditional and online, in Russian that will compensate for the disinformation and the propaganda of Russian-owned outlets such as RT. An example of this practice was already given by Estonia – a country that according to external evaluations is doing a lot to deter disinformation, moreover, successfully. In a broader context, the population within Russia's borders should also have an alternative source of information, for instance, a "satellite direct-to-home television broadcasting so that the US and the West can deliver messages to the peoples like the Russians who are now captives of their own government's dis-informing media"[511]. Such a strategy will follow the one from the Cold War times, mainly Radio Free Europe – an informational tool that proved itself very successful for the mission it set forth[512].

[511] Goble, "Lies, damned lies and Russian disinformation," par. 21.

[512] Arch Puddington, *Broadcasting freedom: the cold war triumph of radio free Europe and radio liberty* (Lexington, KY: University Press of Kentucky, 2000).

A measure that can also bring some clarity regarding facts that are part of narratives of Russian propaganda and disinformation would be the implementation of a state-owned website in countries affected by disinformation. It should contain facts of significance that were falsely presented in disinformation websites. This way, the state can establish a firm position on the accuracy of reported as news facts, explain others, that are left vague and discredit propaganda content that appears online. These tools can be concentrated in state-owned media that already have established credibility and enjoy popularity among the domestic population. In addition to the news reported by these media, there should be a section that focuses concretely on facts that were inaccurately represented as part of a disinformation content. Such efforts are already initiated by various countries, both on NGO-level and on state-level. However, with that many resources, consumers may get confused as to where to double-check certain information. Therefore, it is crucial for the source to be supported and maintained by the government, to enjoy credibility, and to be already known to users. After adding the fact-checking section on the state-owned media website, the new implementation should be promoted as an accurate method of delivering the news and simultaneously disproving any wrongful interpretations of them.

Measures toward the intermediaries – the traditional and social media. In terms of restricting the Russian disinformation officially distributed through state-owned media (RT), the U.S. made some particular steps already, however, with limited success. The Department of Justice forced the RT's U.S.-based company T&R to register under the Foreign Agent Registration Act (FARA)[513] as a form of warning to RT's viewers and readers that the media is a propaganda outlet. Legislation from the U.K. concerning impartiality of the media led to the

[513] Daniel Fried and Alina Polyakova, "Democratic defense against disinformation," ed. Atlantic Council (Atlantic Council Washington, DC, 2018).

courts fining RT[514], as a result of inaccurate reporting, thus serving a similar deterrence purpose as FARA. Regardless, neither of these state-enforced mechanisms are very efficient because they are time-consuming and it is challenging to keep track of all disinformation outlets, especially online. Therefore, a strategy different from the premises of FARA may be better even if it means the implementation of an entirely new system for monitoring digital media. In particular, this system should envision that the reputable news outlets should be invited to register, rather than the ones disseminating information. With a state-registration, the media will receive a license and the obligation to demonstrate through its website that is certified. The registration should include information about the media ownership, other companies with which the owners are associated and when the media was originally established. This way, monitoring the history of a medium may be an indicator for its credibility. Newer media should be an object of close observation until they establish themselves as renowned in time. State legislation should adopt a definition of the term *news outlet* that will differentiate between websites with news content and others (e.g. blogs) in order to delineate which websites are supposed to register and which do not have to undergo a registration process.

In case a medium fails to register and fraudulently uses the certification logo that the state will give to registered media, the legislation should incorporate fines. Moreover, websites that are not registered as news outlets should be obligated to disclose on their website in a visible way that they are not news agencies and the content does not necessarily have to be a subject of journalistic standards for accuracy and objectivity. Non-compliant websites who present news without registration or disclosure that they are not news sources should be deleted and the owners fined. The registration of the media should be free of charge so that equality between

[514] Ibid.

them is guaranteed and any chance for discrimination eliminated. Thus, readers will be immediately aware that they are reading content from either a registered source or one that is not certified. The role of intermediaries such as Facebook is also vital. Social media should only accept advertisements from other media that are compliant with the rules for digital news outlets.

An additional measure should be a state-sponsored campaign that seeks to discourage the evolution of the *attention-economy* culture. Headlines that adopt a more neutral tone should be preferred over such that subtly lead the reader to a conclusion directly with the headline, not leaving them any room for independent fact-assessment and decision-making. To this campaign should also be invited companies such as The New York Times and The Washington Post, who, among other media, set the tone of the entire information culture. While both companies are considered as renowned sources of information, they do not come free of charge. Instead, when the online reader exceeds a certain number of articles per week, they are asked to pay a certain fee to continue reading. Discouraged by the paid access, naturally, readers may turn to alternative sources that are free, but not reputable, accurate, or complying to journalistic standards. Therefore, it is essential that the states engage in a conversation about how to make the content of reputable news agencies accessible to readers so that they do not resort to sources that lack credibility.

The last measure that can have impactful consequences pertains to social media advertisements. Political or issue advertisements concerning election candidates on social media should be restricted unless they disclose the source of their funding clearly and directly through social media[515], without having to click on the specific advertisement. Furthermore, political/issue advertisements funded by foreign sponsors or donors should be prohibited, the

[515] Ibid.

same way that funding from non-native donors/sponsors/citizens is not allowed in elections, because ultimately both phenomena have the same effect – bolstering or diminishing a candidate’s campaign by a foreign entity. Also, social media should be obligated to track and report to a state communications commission the number of clicks that political advertisements receive so that the importance of social media as an arena for election campaigning is assessed, at least approximately. Such regulation would be particularly useful so that their accountability for election disruptions is out of doubt. Among other tracking measures that can be adopted, this one can serve as proof for the major impact social media companies have on independent thinking, voting, and democracy.

Countering cognitive threats in recruitment by radical Islamic organizations

While non-state actors appeared in cases of espionage and disinformation, along with the main state-actors, in the case with the recruitment by ISIS, the central actor is a non-state one, and the state-ones are playing a secondary role. The caliphate could be labeled as the main figure in the recruitment process, but it is important to delineate who was executing the recruitment operations in the name of ISIS. Those were mainly individuals who pledged allegiance to the terrorist group and, of course, its leaders who made direct appeals to people to join the caliphate and help develop it further. The case of ISIS recruitment is another example of how perpetrators could be, initially, in the role of the victims. Many of the recruits were victims of manipulations and deceit before they became recruiters themselves after they traveled to Iraq and Syria. Among these perpetrators who were victims at first, were men, women, and children. However, the circle of the victims does not end with just the people who chose to join ISIS. The families of all these individuals that did not suspect that they may not see their beloved ones again suffered tremendous emotional shocks after discovering that their sons, daughters, sisters, brothers, nieces and nephews joined the terrorist organization and pledged allegiance to its leaders. Moreover, there is another figure among the victims in the case of ISIS recruitment – the states from which the fighters came, and in many cases against which acts of terrorism were committed by their own citizens. The number of state victims in recruitment cases is very high since almost every country has anti-terrorism laws that could have been enforced against a captured ISIS-fighter, exemplifying that the war against terror was multilateral, regardless of the concrete victim. The state victims were not only professing Christianity and Judaism but were also Islamic and Hindu countries[516]. Therefore, the hypothesis that ISIS declared war only on Christian countries is not supported by evidence of the terrorist organization's acts of violence.

The three main conceptual relationships that surface are the non-state actors – state actor(s), non-state actor(s) – individuals, and state actors – individuals. First, the relationship between non-state actors and state actors. It is represented by ISIS, on the one hand, and the states to which its violence was directed, on the other. These state actors include populations with different religions. They are located on different continents and represent different socio-economic conditions, and culture. As an enemy, ISIS was very dangerous mostly because it had a practically unlimited number of enemies that could have been affected by terrorism at any point. Moreover, since it was not officially recognized state entity but rather a state-like organization without official recognition, diplomatic contacts and negotiations were not a possible solution to resolving or alleviating the issue. Deterrence as a state policy is also a limited option. Other non-state actors with significance in this case were the companies whose products ISIS was using to communicate and recruit new members – Facebook, Instagram,

[516] Counter Extremism Project, "ISIS's Persecution of Religions," (2017).

Twitter, WhatsApp, etc. While in other circumstances, these social media companies would have been responsible to some extent for facilitating the recruitment process, in this case, the ISIS recruiters were taking advantage of the main service these companies were providing. Their primary purpose is interaction and exchange of information, something that neither the companies nor the legislation are capable of restricting without any serious damages for the right to information and free speech, except in cases involving examples of hate speech and propaganda that were discovered by these companies and/or the law enforcement.

The next relationship is the one between the non-state actor(s) and individuals. The dual capacity in which ISIS recruits acted makes this relationship particularly interesting. The victims of ISIS in terms of cognitive manipulations began being the manipulators themselves after their recruitment ended successfully as they joined ISIS. Attempting to provide services and goods as a real state, ISIS resembled one a lot – it had a territory, population, some administrative apparatus even if not well developed, schools, hospitals, and profits. However, it also lacked various things, among which, the most central one was, the opportunity to provide to its people citizenship, passports and stability, especially considering the fact that it was spending a lot more than it could afford to pay. ISIS's main funding came, according to the Financial Action Task Force (FATF)[517] from profits gained from the occupied territories; ransoms from kidnappings; donations, fundraising and material support in other forms[518]. As stated above, the difference between Osama bin Laden's vision of Al-Qaeda and ISIS's under its leaders was that the former aimed to destroy the Western order and to establish a strong caliphate only when it has already gained local support and have built solid grounds for future development. As opposed to this

[517] Financial Action Task Force, "Financing of the Terrorist Organization Islamic State in Iraq and the Levant (ISIL)," (Paris 2015).

[518] Dimitrios Stergiou, "ISIS political economy: financing a terror state," *Journal of Money Laundering Control* 19, no. 2 (2016).

strategy, ISIS rushed into declaring the Islamic State with an imposed order based on brutal force. It had the mission to provide the survival of the caliphate and to simultaneously destabilize the West. This was an ambitious task that, according to estimates, in the early years of ISIS cost nearly $10 million per month only for the remuneration of 20,000 to 30,000 fighters, compared to Al Qaeda's operations in Iraq from 2004 that were evaluated to roughly $10.4 million per year[519]. Despite ISIS's desire to be perceived as a state, it was not, and this fact brought a lot of legal issues when it was defeated, and its fighters had to return home with no passports and no documents proving their identity, after destroying their old ones.

Other individuals who suffered from ISIS recruitment were the parents and the relatives of the people recruited. They experienced emotional trauma after realizing their beloved ones joined the organization. This shock came as a result of the little suspicion they had that members of their households have any attachment to ISIS. Moreover, evidence shows that most likely none or limited conversations were led at home about the radical organization before the radicalization occurred. At the same time, the active ISIS propaganda on social media switched the recruits' predisposition to one favorable to the organization. Undoubtedly, social media played an essential role in the recruitment that could not have been limited without censorship, potentially unjustified persecutions, restriction of connections and possible lawsuits. Facebook and similar channels for communication were very appealing to young people, they spent a lot of time engaging with them, and this made them easier targets for recruitment.

The third relationship that could be observed in the ISIS recruitment case is the one between state actors and individuals. It represents a complicated and challenging question: why citizens of a particular country would leave it to join an organization that commits acts

[519] W. A. Tupman, "Ten myths about terrorist financing," ibid.12 (2009).

potentially against this very same country. The reasons embrace a multitude of cultural, socio-economic and political factors, as it was discussed previously. Summarizing them leads to the conclusion that some states failed to provide enough certainty and comfort to their citizens and made them targets to recruitment. In addition, it is likely that the citizens did not feel attached to the state to a degree that made the recruitment and the violence directed against the state, an acceptable option. Further problematizing this question is another relationship that the states have with the victims of terrorist acts executed by ISIS. The grief and the trauma from these terrorist attacks gave rise to nationalist voices that demanded the state adopts further acts of repression against Muslims worldwide and Muslim communities in the state itself. As the far-right parties gained more and more supporters and seats in the national parliaments, many popular state narratives started transitioning from a fight against terrorism to a fight against Islam, which further alienated Muslims and exposed them to more opportunities for radicalization and recruitment. Moreover, after the world declared a win against ISIS and its members started returning home, many states refused to allow them to enter and even revoked their citizenships – a measure that has an ambiguous meaning for deterrence. It sends a clear message that for those who join terrorist organizations, there will be no coming back. While this may deter to some extent potential recruits that are still hesitant about joining ISIS, it also makes it impossible for newly added members to redeem themselves, to reintegrate society and to be motivated to stop seeing their former state as an enemy.

It was clear since the establishment of the Islamic caliphate that the next goal of ISIS will be to destroy the Western order. Its leaders sought this as well as its members. At the time, a loss in the eyes of ISIS members was a defeat that led to territories lost, decreased incomes from illegal trade, ransoms and drugs, and donations. Consequently, the more defeats ISIS suffered, the more significant the losses were in every regard including reputational, as the abilities to the state-like formation to continue existing were under question. Another phenomenon that could be considered a loss for ISIS, in a non-material sense, was the loss of supporters and the decline of the faith in the ISIS ideas and goals. However, while non-material, it was still a very important one, because ISIS may continue existing, at least ideologically, even without territories, funding, and profits, but if it loses credibility and supporters, this would mean that the organization is dead indeed. From another perspective, ISIS members suffered losses translated into the disappointment of some ISIS-members by the fact that the conditions promised by the caliphate did not match with reality. Moreover, for the families of the ISIS members, the losses of being away from their children and potentially not seeing them again represent a significant emotional burden, added to the realization of the fact their beloved ones joined a terrorist organization responsible for many deaths and other atrocities. The shock in the community from the news that people who previously did not express any attachment to ISIS or its ideas abandoned their everyday lives and their families abruptly to support terrorism also brings disappointment, sadness and even more questions.

As for the individuals or their close ones who were victims of ISIS violence, a win in their eyes was mostly getting their beloved ones back home. Among other desirable scenarios was the elimination of ISIS. Unfortunately, they did not realize that even without territorial presence the ideas of ISIS may still survive. A loss for these people meant even more terror, death and devastation. In terms of state wins and losses, the most significant damage is reputational probably, caused by the departure of many of the state’s citizens to join ISIS. This is, of course, in case the state has not suffered any terrorist attacks that will also bring losses of lives and material damages. Moreover, a trauma from a terrorist attack in the minds of the people is something that does not heal easily and could persist across generations. To this extent, not only the population of a particular country that has been victimized suffers a loss but potentially humanity in general. While different individuals in a society will have different views on how an ultimate win against ISIS looks like, in a broader context, a win for everyone opposing ISIS would be every loss, in its varying degrees, for the radical organization – from decrease in donations and profits from kidnappings to loss of territories and supports, and new recruits.

As already mentioned, the social media, in this case, had a supportive role as it facilitated, unintentionally, the recruitment of new ISIS members. However, aside from the social media and its consequences, a few other figures, who remained mostly in the shadows during the investigations of missing people who allegedly joined ISIS, are also present in the case. Studying ISIS recruitment shows that there was most likely a network of people who were responsible for recruiting new members, support them materially and with guidance, provide forged documents, and detailed itineraries for the trip to Iraq and Syria. Moreover, smugglers who were not necessarily connected to ISIS or its goals also emerged as facilitating factors in the recruitment operations, as their motivation to provide support was purely financial. The opportunity that some smugglers were ISIS-affiliates should not be excluded. Regardless, the focus of the investigations and the stories the media reported was on the ISIS recruits, rather than on the numerous people who made the entire process possible. More media and scholarly attention should be dedicated to such underground networks because, if their members remain anonymous or at large, then they will continue working for dangerous clients like ISIS.

Most of the factors that influence the case of ISIS recruitment strategies were already mentioned previously but still deserve to be highlighted to extract implications for prevention strategies against this threat. First, the culture of antagonism toward immigrants and toward

Muslims, in particular. Second, the family environment that shows in various cases with radicalization that some tragic event happened in the family – typically the loss of a parent. Another component that is also evident in the cases regarding the family environment is the possible views of a parent who expresses support toward radical Islamic groups. Thus, the parental example and the experienced trauma to a large extent set the conditions for the future radicalization of the household members. Interestingly, money is not among the most crucial factors for radicalization, even though in some cases it is present as a powerful incentive. In others, it was just a catalyzer that on the one hand, allowed young people to focus on spiritual rather than monetary issues, and on the other, to make the trip to Syria and Iraq financially possible.

As opposed to other cases described in this study, the one with ISIS recruitment could be considered as part of a war. That is, mostly because of the organization's terrorist acts and the war declared on terrorism. As recruitment is a direct source of human resources added to the ISIS capital, it could be said that the states fighting ISIS have declared war implicitly on recruitment as well, as the latter was recognized officially as a security threat of high importance. The rules of wars were applicable in this situation which was further facilitated by the fact that ISIS resembled a state-like entity but was, nevertheless, not an officially recognized state. Thus, any legal justifications about military measures undertaken against them as a response to their aggression were not necessary. However, as the destruction of ISIS could be perceived as a powerful weapon against future recruitment and a hit on the ISIS reputation and ideology, the recruitment itself cannot be fought only with conventional weapons, as many have already realized since the physical defeat of Al-Qaeda did not stop recruitment or the ideational existence of the organization.

The political mechanism used in the case of ISIS recruitment is closely related to the organization's primary goal – to destroy the Western liberal order and replace it with one dominated by the Islamic norms. As this assumption appears in works of radical Islamic ideologues, it was originally accompanied by another one – to create a caliphate after the end of the Western value system. While Al-Qaeda planned to dismantle the Western order and then create a caliphate, ISIS declared the beginning of the caliphate and turned eyes toward the second task assigned by radical Islamist doctrine. Both Al-Qaeda and its somewhat similar but ideological continuation – ISIS included recruitment as an important activity upon which the future of the radical formation is dependent. Both Al-Qaeda and ISIS still have supporters, although they have been defeated, at least territorially. The fact that they gain material and non-material support for their goals despite their losses over the years shows that recruitment is still a threat and will be as long as radical Islamic leaders believe in their idea and see the potential for support in populations across the globe. The latter use religion, along with other factors, as a main driving force for achieving political gains – the creation of a state that will fight against other states in order to impose its, perceived as superior, ideological principles.

The recruitment operations led by ISIS were enjoying success mostly because of a few psychological mechanisms. In all of the cases examined by researchers, and in the ones that I used for this work, there is one element always present – the perceived loss of control over one's life. The loss of control can be in one or more regards, including financial, spiritual, cultural, emotional, etc. In some cases, this pattern was a result of a loss of a loved one, a crisis of identity, and in others a cognitive dissonance produced by the conflict between the liberal environment and conservative expectations in terms of cultural norms. Undoubtedly, the persuasion of the ISIS recruiters was also a powerful force that contributed to adding more members to the ISIS-army of men, women, and children. However, the victims of recruitment were vulnerable to this persuasion because some or all of the psychological conditions that I mentioned have been present in their lives. For instance, in cases of recruitment of women, it was at first glance evident that they were almost perfectly integrated into the Western way of life – they had good grades, they were even outperforming their peers, they were engaged in extracurricular activities, they enjoyed the company of friends and family. Nevertheless, their religion and their culture were composed of more conservative values, based on modesty and obedience to senior family members who determined to a large extent the life of their children, including marriage. At the same time, the West offered a sharp alternative to these traditions. With the realization of how significant the contrast between Western society and one's conservative community can be, the cognitive dissonance in people who later became victims of ISIS recruitment started to grow. Psychological studies show as I outlined previously, that in times of cognitive dissonance and a perceived loss of control over one's life, the need for information needed to provide a solution to the problem increases. The human cognition when operating under stress searchers for *more* information, as this often happens at the expense of *quality* information. At the same time, ISIS recruiters offered pieces of information connected in a narrative – a desirable alternative for regaining control by rejecting the discomfort from clashing values and lifestyles.

Measures toward the indirect perpetrator – ISIS. While the defeat of ISIS was a powerful step towards future deterrence, ideologically, ISIS still exists and has supporters. In peacetime, rather than when ISIS or similar radical organizations are on the rise, states should be consistent with their deterrence tactics. Mainly, they should focus on discrediting the leaders of ISIS, the more popular faces that appear in their propaganda videos, and the ISIS ideology altogether. The counter-narrative should be distributed through the same sources and using the same means as ISIS when disseminating their messages – social media, hashtags that ISIS use, or any other way through which the target-audience could be reached. The core nature of the ISIS counter-narrative should be the illusionary picture that is drawn by ISIS recruiters, in material and non-material terms. In this message, the main reasons for people to join ISIS should be carefully considered. They should be addressed in a way that exposes the fallacy of the promises made by ISIS. The goal of this campaign should be that potential recruits realize that they will not regain control over their own life, but just the opposite – joining ISIS will be just a different path leading to even more loss of control.

Measures toward the direct perpetrator and victims – current and potential ISIS members, and the indirect victims – countries of origin/former residence of ISIS members. Due to the highly intertwined nature of the problem, in which perpetrators are victims, and vice versa, the measures focused on the remaining actors involved in the case will be listed together in this section.

To counter cognitive threats that result from recruitment operations, it is essential that ISIS members do not join the organization and do not become future recruiters themselves. Among the strategies that could be used in this regard is the development of religious education programs that will clearly distinguish between Islam and radical Islam. For this effort to be successful, participants from academia, community, religious institutions, and policy-makers should join efforts and work together. Religion by itself is not the force making radicalization possible. It is typically accompanied by some loss in the recruit's life and in these moments of desperation, many people turn to religion, as a way to heal. Compensating for this loss of control should be the main strategy against recruitment. It should envision programs that aim to provide monetary and emotional support for people who are vulnerable of becoming radicalized. Moreover, individuals who have gone through a similar path and have considered joining radical organizations should be included as an example of the illusionary world that ISIS promises. Former ISIS members should not be deprived of citizenship because this way they will know that they cannot re-integrate into society under any circumstances and may re-radicalize after they returned from ISIS and found no place to go, no place to which to return. Re-entry programs should be offered to such individuals, but not without the necessary caution. Making an enemy of the West was the central premise on which ISIS commits violence by claiming it declared war on Islam. To refute this assumption, the West has to prove that it has not declared war on Islam, or Islamic people, even those who were misled by ISIS. If a way of re-integrating back to Western societies is not offered, then any narrative portraying the West as not seeking to create enemies will fail.

Especially for children who were raised in the West but spent time in the ISIS system of terror, there should be resources for re-integration. Many immigrants, even those who have not joined ISIS, have seemingly accomplished a successful physical adaptation to the environment that their new location offers but not a mental one which reflects on their identity - the way they see themselves. Policy-makers and societies should recognize the importance of the struggle for mental migration that many immigrants experience in terms of culture. It is also one of the central reasons why so many allegedly *integrated* young immigrants with impeccable school records were easily victimized by ISIS recruitment. Their physical adaptation to the conditions of the West was completed but not their mental one. These young people had questions, doubts, and concerns that remained unaddressed. Therefore, a successful strategy in this regard will begin from the home where adolescents can raise concerns in a safe environment, without judgment.

Through such re-connection, older family members will be informed of the experiences of the younger ones and thus will be alert if there are any signs of intended life-transitions such as joining a radical organization. Moreover, since there may be an inevitable clash between the liberal culture of the West and the more conservative culture of the East, family members should be the ones to helping with the balance in the mind of their young sons, daughters, and siblings. A balance that will eliminate the cognitive dissonance with which many of them struggle through a secure channel of communication that will lead to openness, conversations and compromising thus reducing vulnerability and potential recruitment by radical organizations.

Measures toward the intermediaries – people engaging with document frauds and human trafficking. As smugglers and individuals issuing false documents are not among the main actors in recruitment operations, they are still important figures for facilitating this process. As most of the attention of the law enforcement, the scholars and the media is focused on perpetrators and victims, somewhat peripheral remain figures of people who make the recruitment possible. That said the law enforcement should engage in campaigns to identify, discover and capture anyone who is involved in the recruitment chain from smugglers to those who aid and abet terrorist organizations' in any other way. Special laws should impose more severe sanctions for these crimes. The issue is that some states have weak law enforcement apparatus and judiciary. Therefore, the individual communities that are among the most interested sides in preventing recruitment have to take responsibility for providing information about smugglers and human traffickers to local but also international law enforcement agencies. Traditional and online channels for communications between the communities and these agencies should be established, especially in states that are corrupt and lack resources. Smugglers and human traffickers may be considered a problem only of the state law enforcement agencies, but when it comes to terrorism, this should be framed as an international problem and capturing such individuals and preventing them from making recruitment possible – a global task of high importance.

Countering cognitive threats in cases of political profiling by companies

The case with Cambridge Analytica reveals events in which leading figures were non-state actors, similarly to the case with ISIS. As opposed to the latter, however, the Cambridge Analytica one involved not radical terrorist organizations but corporations, democratically established entities in compliance with the existing laws. Moreover, Cambridge Analytica was not looking to recruit people to help them achieve the company's goals. The people were already recruited, or more accurately - they voluntarily posted their information on Facebook, from where Cambridge Analytica obtain it contrary to regulations established by Facebook. Cambridge Analytica could be identified as the main non-state perpetrator in this case, with some help, to some extent by Facebook as the latter did not provide strong guarantees that the users' data will not be exploited by third-party applications. Interestingly, in this case, the direct victims were deceived in not one but two ways. First, their information was stolen and used without their permission. Second, this personal information was then skillfully used for the construction of psychological profiling of political advertisements whose targets were the very same people from which the information was stolen. While there is no obvious direct state victim, in this case, the consequences from the cognitive victimization of individuals reflect on the democratic processes in various states, mainly through disruption of the independently formed political attitudes and behaviors. One of the central arenas for Cambridge Analytica's profiling was the 2016 Presidential Elections in the United States, but the range of state targets who suffered from the company's operations also includes European and African countries as well.

The role of the individuals, in this case, is also particularly intriguing. As some of them were victims of the profiling, others were involved in the profiling algorithm and the marketing activities of Cambridge Analytica. After the news about the political profiling broke, some of the people collaborating with the company showed remorse about the company's strategies, and others did not. Aside from potential political motivations for their involvement in Cambridge Analytica's activities, their primary incentive was undoubtedly financial, as all of them had been associated with the company through employment or grants. As for the Facebook employees who were aware of possible adverse consequences resulting from third-party applications, they were motivated by the company's main goal, to increase profits. It is unclear what amount of Facebook's profits is generated through relationships with advertisers and third-party applications, but they are likely significant, considering the company reported around $40 billion revenue from advertising in 2017[520].

There are three levels of relationships existing in this case: non-state actors – individuals; non-state actors – state-actors; and individuals – state actors. The first relationship represents the dyad *perpetrators – victims*, except for when individuals were employees of the non-state actor (the corporation) involved in the case. The non-state actors perceived the individuals in this scenario as a means to an end, and the individuals, while realizing that companies benefit from the services delivered to them were nevertheless enjoying the free product left on their disposal – the social media platforms. However, as privacy concerns have always been a serious issue in social media, it never escalated to the extent to which the users completely abandoned social

[520] Kurt Wagner, "This is how Facebook uses your data for ad targeting " *Recode* 2018.

media. Some of the users agreed their information to be utilized by third-party applications, for research purposes, as suggested by Facebook, but the majority had no idea how their data will actually be used, and they never consented to give it to anyone. The second relationship – that between non-state actors and state-actors is a very complex one. The non-state actors typically lobby before the state actors so that more comprehensive privileges are afforded to them, assumingly leading to more profits. At the same time, democratic countries are free-market societies in which companies, their development, and competition are encouraged officially by the state. Considering this context, the specific legislation limiting the freedom of social media platforms to use the users' information was a sensitive issue. States were reluctant to impose strong measures out of fear of being accused of authoritarianism and censorship. Moreover, due to social media's strong lobby, politicians were reluctant to draw limits to the social media's use of personal data, because this could restrict a lot of their income from advertisements. The third relationship illustrates the interaction between individuals and state-actors. Countries are generally obligated to adopt laws in protection of the rights of the citizens, as they are cognizant of its tremendous popularity among the users. They are also aware of the thin line between strict measures and censorship, when it comes to media, and especially digital media – a grey area that is still not very well regulated even in developed Western countries. Individuals, recognizing the role of the state as a protector of their privacy and social media's primary goal of profiting from the services offered, were caught unprepared for a unanimous position on the issue. Most of them blamed Facebook directly for the violations, that led to Cambridge Analytica collection of their data for political goals[521]. For others, leaving Facebook turned out to be a much more difficult task, as many users have deleted their accounts only to go back to the platform soon

[521] Tiffany Hsu, "For Many Facebook Users, a 'Last Straw' That Led Them to Quit," *The New York Times* 2018.

after, realizing what significant part of their lives it occupied[522]. Much like an addiction. An addiction that studies confirm to exist. One study on the topic showed that “correlations between symptoms of addictive technology use and mental disorder symptoms were all positive and significant”[523]. Meanwhile, the voices of users that accused the states of lack of regulations that led to the scandal were very few, perhaps realizing that the state was put in a very peculiar position, as the digital privacy laws are still immature, and the freedom of speech and free market economy initiatives should be protected at all cost. The states themselves were caught somewhat unprepared at how easy it is for huge data breaches to occur in social media. A proof for this is that the fines for them were, before the Cambridge Analytica scandal, disproportionally small in comparison to their profits from advertisements.

When discussing what constitutes wins and losses for the sides involved in the Cambridge Analytica case, the interests of the three central figures have to be considered. First, non-state actors (Cambridge Analytica and Facebook), second, states whose citizens’ user information was stolen and who were consequentially targeted by aggressive political advertisements aiming to influence elections outcome, and third, the individuals who were the direct victim of the data appropriation. For Cambridge Analytica, a win will mean to gain more clients and popularity while at the same time maintaining a low profile regarding the company’s preferred methods for winning elections, political disputes, and generating profits. As for Facebook, their main end-goal is the same as Cambridge Analytica’s and similar to them, they have to maintain their clients (users) satisfied with the offered product in order to keep making profits. That said Facebook skillfully maneuvered between users’ content with the platform, its

[522] Ibid.

[523] Cecilie Schou Andreassen et al., "The relationship between addictive use of social media and video games and symptoms of psychiatric disorders: A large-scale cross-sectional study," *Psychology of Addictive Behaviors* 30, no. 2 (2016): 252.

regulations for privacy protection, and the income from advertisers for whom users' data is an invaluable tool for their own goals. In that sense, a loss for Cambridge Analytica and Facebook will mean loss of profits, which could be a consequence from loss of clients (users) or from another reason leading to the same effect. For states, wins and losses in this case would be defined differently than the ones for the non-state actors. A win for states would be a well-balanced environment in which companies thrive but not at the expense of selling users' information to third parties who will, in turn, use the information against them, turning them into victims of coercive political persuasion. A loss for states, in this context, would be to lose the balance between non-state actors and citizens, especially when this influences outcomes of elections or other issues of national importance. As for the individuals who were victims of the profiling a win would mean their privacy to be guaranteed on social media, to have control and ownership over the content they post. A loss would be if social media withdraw or limit any of these rights or mislead the users to believe their information will be used in a particular way when it is in fact used for entirely different purposes.

Two of the figures that are not central for the case with Cambridge Analytica but still have some role are the ones of politicians and researchers. Many politicians were more lenient to Facebook because of lobbying. They were also the ones who were clients of Cambridge Analytica or one of its subsidiaries and benefitted from their profiling methods. Furthermore, the politicians using Cambridge Analytica's services were not only from one country but from different countries almost on every continent. Without politicians profiting from Cambridge Analytica's algorithms, there would be no market for political profiling and thus business for companies like Cambridge Analytica. The other figure mentioned previously that has to do with the case is the one of researchers. Their studies and conclusions, as one of the former Cambridge

Analytica's employees admitted, contributed to a large extent to the development of the profiling tool later used for the design of the digitally distributed advertisements. As researchers' main task is to produce knowledge on a subject matter, very often circumstances lead to the production of knowledge that serves to achieve undemocratic goals. Researchers produce science benefitting all people, but in the Cambridge Analytica's case, this science was used against them.

Among the interfering factors in the Cambridge Analytica's case are culture, society, corporate profits, and politics. The creation of Facebook stimulated the growth of a culture of oversharing in the digital space. As this was still a new environment, many users were unaware of the results from posting online a large number of personal details and thoughts. This culture got slowly incorporated into societies and gained the dimensions of an addiction that was controlled by social media corporations. This dependency was created, stimulated and perpetuated by Facebook in order to keep its current users and gain new ones. Having more users generally translates into more profits for the company, as they form a broader audience that could be easily reached and influenced by the right tools of persuasion. From the dawn of political thinking and politics, persuasion has been the driving force between uniting and dividing people over different issues of social interest. The case with Cambridge Analytica is a bright example of the interaction between culture, society, profits and politics and how they are intertwined in a way that reveals a long-known pattern: the losses for one actor are gains for another thus leaving very little space for a compromise between the political interests of state, non-state actors and individuals.

As this case represents one of the most recent types of cognitive threats, and currently lacks even legal regulation, it can be claimed that it does not constitute a reason for war. None of the traditional war weapons would be applicable in this case. The primary tool for reaction in cases of profiling for political purposes remains the adoption of laws and regulations serving as deterrence. Moreover, because persuasion is still perceived as a non-invasive weapon that can only slightly, if at all, influence thinking but not predetermine it altogether, targeted political advertisements are still not defined as a serious threat. As argued previously, this could be attributed to the difficulty of proving that independent decision-making could be violated by coercive persuasion to the extent to which the decision maker's behavior changed consistently with what the author of the persuasion message desired. A lack of conclusive proof for this causal relationship does not mean, however, that the causal relationship does not exist. It is just difficult to be proven beyond doubt since it pertains to psychological processes. The fact that a domestic or foreign entity has an invested interest in affecting the process of independent decision-making by voters is a fact concerning enough to provoke concrete measures to counter this threat. The fact that the perpetrator is a non-state entity (corporation), be it Cambridge Analytica, Facebook or other social media platform, leads to the conclusion that the most effective means to combat profiling for political purposes may be administrative, legal and psychological, rather than military or foreign-policy oriented.

The political mechanisms making the case with Cambridge Analytica possible are the following. First, for Cambridge Analytica to get access to users' data, the latter existed within Facebook, and the company collected them. Next, after Cambridge Analytica was in possession of the data, it used them in a way that led ultimately to serving the company's clients and thus generating profits for itself. At the same time, the individuals whose data were exploited for the production of political advertising campaigns were losing the battle for control over their personal information. As Cambridge Analytica scored wins, financial and reputational, so did their clients who were supported by the political profiling algorithm developed by the company.

As individuals were losing more and more privacy control over their own personal information, the democratic process and independent thinking became endangered more and more.

As for the psychological mechanism for influence that led to the success of Cambridge Analytica, there are few aspects to be considered. As mentioned, Facebook and other social media created a culture of oversharing that gained quickly the dimensions of an addiction. Addiction, that was orchestrated by social media and its tools to subtly persuade users to spend more and more time on their platform so that they share more and more of their life. Getting users to agree on posting something once, leads to them agreeing even more in the future. This is a phenomenon in social psychology related to attitudinal commitment and behavior consistency[524]. According to these principles, people want to preserve some consistency in their future behavior. Thus, getting them to commit to something once, would predict a possible pattern in their behavior for the future. That said Facebook initially asked users to provide basic information about themselves, and as time went by, it was asking for more and more information to be shared, with which most users complied. Moreover, Facebook was constantly offering its users potential contacts, labeled as friends by the platform in an effort for the user to increase their level of intensity of the communication and people outreach. This outreach also increased Facebook's depth of knowledge about people's social circles and relationships. As users already shared a lot of information and had access to so many of their friends and acquaintances, leaving Facebook was not so easy because it meant leaving commitment, leaving information flow, leaving contacts.

While so many other means of communication exist, Facebook was connecting people in a way that no other media did. Once adjusted to receiving and providing an increased volume of

[524] Robert B. Cialdini, *Influence: The psychology of persuasion* (New York, NY: Collins 2007).

information from and to friends and acquaintances, it was difficult for users to delete their social media profiles and resist the instinct to seek and exchange information. Facebook knew this, so did Cambridge Analytica as well. The latter sensed that social circles on Facebook reveal patterns that could be exploited for political gains, if appropriately conceptualized. Their algorithm had hundreds of elements that were used for micro-targeting, a campaign that aimed to send an individually designed message to a social perceiver, that will evoke a predictable reaction in them, typically benefitting the sender of the message. Based on the *likes* on social media, Cambridge Analytica's algorithm was able to extract information about people's basic characteristics, name, age, race, income, and sexual orientation but the capabilities of the profiling strategy were not limited only to this. Surprisingly, they could also predict attributes such as childhood trauma, intelligence, political views, and other elements of a psychological portrait that included "openness to experience, conscientiousness, extraversion, agreeableness and neuroticism"[525]. In terms of its role in the U.S. elections, the accuracy of the model was very high too, ranging from 85% accuracy for distinguishing between Democrats and Republicans reaching 95% accuracy for distinguishing black users from white users[526].

Even with these high levels of predictability of users' behavior, it is difficult to believe that Cambridge Analytica's algorithm completely changed users' political predisposition to vote for one candidate or another. What is not difficult to believe is that influence over particular groups of the population was exercised in a way that made them more likely to prefer a particular candidate and to vote for them – a fact that in close elections plays a significant role. Regardless of the levels of exposure to Cambridge Analytica's political profiling model in the U.S., in the

[525] Alex Hern, "Cambridge Analytica: how did it turn clicks into votes?," *The Guardian* 2018, par. 10.
[526] Matthew Hindman, "How Cambridge Analytica's Facebook targeting model really worked – according to the person who built it," *The Conversation* 2018.

U.K. and in other countries in which politicians used their services, voters' profiling was born as a strategy in political marketing, and threatens to stay and expand its influence, if measures are not undertaken. As Facebook is undoubtedly part of the problem, it is not the only company that makes profiling possible. Others, such as Netflix, Amazon, Google, and Uber[527] also develop their own prediction algorithms based on users' data. The common denominator between all of them is the information that consumers themselves provide through their online searches that give companies clues about their interest in different products. Such hints are often used across multiple companies. It is only needed for a user to search for a single keyword in one search engine/retailer so that others, with which this search engine/retailer collaborates, begin to micro-target the user with tailored advertisements based on the keyword entered.

In the following sections, I will address a few possible strategies to counter these threats that are focused on the different participants in the case. First, measures toward the indirect perpetrators in this case (Facebook and other related social media). Second, measures toward the direct perpetrator – Cambridge Analytica. Third, measures toward the direct victims (the social media users). Fourth, actions toward the indirect victims (the states whose democratic processes were violated). Fifth, measures toward the intermediaries that made the exploitation of users' data possible.

Measures toward the indirect perpetrator – Facebook and other social media. One of the most reliable strategies pertaining to Facebook and other social media is that the state, through regulations and sanctions forces them to provide more freedom for users to control their information and how it is used. This control should be given through opt-in functions rather than through opt-out functions, so that users are in charge of who sees their information at all times.

[527] Jathan Sadowski, "Companies are making money from our personal data – but at what cost?," *The Guardian* 2016.

Moreover, all guidelines and regulations of to users' privacy should be explained in an easy, understandable manner. Also, Facebook has to provide guarantees that chats between users through the Messenger application are not recorded and used for any purposes by Facebook or third parties.

Measures toward the direct perpetrator – Cambridge Analytica. As for measures toward Cambridge Analytica and other companies using similar techniques for political persuasion, it is needed that legislative measures regulate specifically the boundaries of their activities. State authorities should obligate companies engaged with political campaigns to obtain written (digital as well) consent from every user who receives targeted political advertisements through social media, as this consent could be withdrawn at any time. Moreover, both social media companies and those working on political campaigns should develop advertisements in a way that clearly shows if the user seeing them is a subject of targeted advertising. An opt-out function should also be provided.

Measures toward the direct victims – the social media users. Studies show that social media users generally do not take advantage of more privileges presented to them regarding online privacy. So far, however, these privileges have not been given in a way that makes them practical to most users. The process of opting-out of some of the functions leading to marketing and political marketing profiling is complicated and has to be executed every time a new interest of the user was discovered and automatically added by Facebook. Thus, Facebook should be obligated to clearly indicate when a new interest is added to the user's profile, and such should be identified only if the users add themselves a specific interest to their profile. Another option for defense against political profiling is that digital users develop civil consciousness that pertains to the online space. They should demand their online rights to be respected, protected and guaranteed by state- and non-state entities. Moreover, users should require legislative changes that will lead to more control over personal information. They should also be prepared to boycott social media in case the practice of selling and exploiting their data is not terminated. Social media corporations know that their products are highly addictive, and they rely on this to keep their users, even if they are not satisfied with how their data is being handled. Facebook became so popular and hard to leave because people increased in number and interconnectedness. If this is true, the same process can diminish the role of Facebook when users start leaving and become less connected through Facebook. The latter will lose popularity and usefulness. Moreover, as the need for communication and maintaining relationships is apparent, an alternative to the known free social media should be developed. It could be paid or free of charge, but offering users guarantees that their data will not be collected, sold or used in any manner. Such transitions are not surprising considering MySpace – Facebook's predecessor. People claim they left MySpace and migrated to Facebook because they found something that the former did not have, but the latter offered[528]. Considering this tendency, Facebook's shortcomings may also be the reason for another rising social media platform that will compensate for Facebook's mistakes regarding data privacy and other related scandals damaging its reputation. However, it is in the hands of the politicians to create conditions and in the hands of the people to create the demand for a social platform that is better for both their needs and rights than previous ones.

Measures toward the indirect victims – states whose democratic processes were violated. As states have most power concentrated in their hands over both individuals and companies, their obligation to limit the damages that political profiling inflicts should be

[528] Sean P. Aune, "Why Did Everyone Leave MySpace For Facebook?," TechnoBuffalo.

commensurate to their ability to influence changes. As argued before, the fines for violations that are made by companies are not proportional to their gains – thus devaluing the quality of the future prevention measures. Consequently, fines should be designed in a way that reflects the profits the companies register. Also, profits generated through the violation should be confiscated, despite how difficult it may be to establish how much of the company's profit came from the prohibited activities. This principle should be established as a law standard in all countries in which political profiling is present. Moreover, in serious violations, substantial personal responsibility should be envisioned for senior executives in these firms, who knowingly disregarded the law and allowed or encouraged the violation. Prosecutors and the courts should carefully examine the extent to which senior executives knew about them.

Based on all of the described factors facilitating political profiling, it is evident that contemporary society is in a desperate need of state regulatory apparatus of social media and online communications in general. Such agency, on national, or on supranational level should be engaged mostly with monitoring social media and if they comply with the norms regarding privacy laws. The U.S. Federal Trade Commission executes similar functions, but its range of responsibilities includes a lot more than just controlling media companies. As they are expanding and growing stronger, there should be a regulatory agency established specifically for the digital space, as it has been increasingly becoming an arena for political warfare.

Measures toward intermediaries – politicians and researchers. A few words about the prevention mechanisms focused on politicians and researchers also have to be mentioned. First, Cambridge Analytica was profiting from its algorithm that exploited Facebook users' data because it had clients who requested this service. Therefore, politicians emerge as a figure that knowingly or unknowingly encouraged the privacy violations. To prevent politicians aiming to influence voters on political issues, laws should mandate that political targeting based on individuals' data used without their permission should be punishable. Moreover, companies that help with political campaigning should be obligated to inform their clients (politicians) about how the users' data for the profiling was gathered. If it is established that the politician knew that the data was gathered without the permission of the user, then they should be criminally liable, along with the company providing the service. As for researchers, especially junior faculty members, they are a vulnerable target for companies needing their services because of the grants the latter offer to the former. External funding is known as a highly treasured asset for a successful career in academia. As the pressure for securing grants by faculty members increases, the more agreeable they will become to contribute to studies whose results will be used for unethical purposes that may represent violations or even crimes. Using science for unethical purposes is not a new phenomenon in the history of humanity. It has been so far and to some extent limited, however. For instance, a lot of the science behind some of the world's most devastating weapons is publicly available, but this does not mean that people use it on a regular basis to do harm. There are many reasons behind this, among which an appreciation of the threat that such weapon can produce, and laws prohibiting even attempts for constructing or using these weapons. Therefore, if legislation restricts the use of personal information in political profiling, the knowledge produced by scholars working on grants will be still benefitting society. At the same time, it will be in the public domain but not used for unethical purposes that could violate the right of independent decision-making, free of any coercive persuasion.

CHAPTER 6

CONCLUSIONS, POLICY IMPLICATIONS, AND THE ROAD AHEAD

Currently, Google shows more than 5 million results produced by the search of the phrase *cognitive hacking*. While it refers mostly to hackers taking advantage of psychological vulnerabilities of the human cognition, it shows that the problem has gained alarming dimensions. Some identify it as a public health crisis[529], others as an issue of the cybersecurity field[530]. However, very little attention the problem gathered as one of the overlapping points between the public health discipline and the cybersecurity – politics. Cognitive threats have always been present in the world history, and they were so well integrated and common in warfare that there is almost no research that linked ancient espionage and deception practices to political profiling of voters whose information is used against them in a way that exploits their greatest fears. The problem has always been the same, but because of the level of technological and political development of societies, it was manifesting itself differently. This psychological exploitation of the mind was continuously present in peacetime and warfare because humanity was helpless against threats that come from within the individual. Public health cannot label influenced thinking as a disease because even the healthiest cognition is exposed to threats due to the way it is constructed and how people are socialized. At the same time, legally, perpetrators of these cognitive attacks are not committing a crime by influencing other individuals because this has always been part of the interaction between people. It almost seems like cognitive threats are not a problem at all or at least they are not officially declared to represent one. Yet they are, and

[529] Leah Brown, "Why cognitive hacking is a public health crisis," *TechRepublic* 2017.
[530] George Cybenko, Annarita Giani, and Paul Thompson, *Cognitive Hacking*, vol. 60 (2004).

have always been, even if the causal relationship between an outcome of affected by coercive persuasion decision-making and the coercive persuasion itself cannot be established beyond doubt. The harm that has been inflicted by cognitive threats over the different historical epochs is obvious – lost wars, executed monarchs, thousands of recruits of radical organizations, millions of online users whose data and whose fears were used for material and non-material profits of a politician, political party or even companies.

As adverse as the consequences of cognitive threats can be, I aimed to prove in this study that through prevention strategies, their effects could be mitigated to some extent. To summarize the findings, I followed the sequence of the questions from the analysis chapter. First, regarding the perpetrators in the cases, as main actors appear states, non-state actors and individuals. In particular, in Maria Butina's case, the state was a perpetrator through the individuals who were politically motivated to collaborate with Moscow. The state also conducted disinformation campaigns through individuals, but here, they were not politically but financially incentivized. The case with ISIS reveals a non-state actor as a perpetrator through individuals who were politically motivated to collaborate and undertook the roles of both victims and perpetrators. As for the case with Cambridge Analytica, the main perpetrator(s) were non-state actors, as they achieved their goals through individuals who were not politically or financially motivated to collaborate. Instead, they had little to no knowledge of how they contributed to the non-state actor(s) goals. The individuals who voluntarily posted their data on Facebook were unknowing collaborators to the perpetrator's aim but also victims in this case. That said, all of the perpetrators were achieving their goals through individuals who acted driven by different motivations or no motivations at all as they were contributing unknowingly. Half of the perpetrators represent state actors and the other half - non-state actors as direct perpetrators.

In terms of the range of victims in the case studies, in the case of Maria Butina, the direct victim was the U.S. as well as the individuals through which the damage was inflicted. In the case of disinformation, the range of direct victims expanded to include other Western states, in addition to the U.S. and such that are objects of Russian geopolitical interests. The following case, that with ISIS recruitment showed an even enlarged circle of victims that practically included countries of all religions, from the West, from the East, the North and the South. Similar to the almost unlimited range of victims of ISIS recruitment is the case with Cambridge Analytica as well. Victims were whatever countries and individuals a politician who hired Cambridge Analytica wanted to influence. The number of victims, in this case, includes also the Facebook users who, despite those who deleted their profiles in the social media, are still billions.

The perceived wins by the actors could be summarized in the following way. In three out of the four case studies that I explored, the gains of the perpetrators were related to the destabilization of the enemy, establishment of influence over them, and achieving more power. In the fourth case, involving Cambridge Analytica, the wins of the perpetrator were related to profits, more power, and establishing influence over their client's target audience. As for Facebook, the wins still meant profits that could translate into power to lobby to maximize profits even more. Losses, for all mentioned perpetrators, would mean any perceived outcome that leads to decreasing the chances of wins (power/profits).

The analysis chapter in this study also included sections for other figures involved in the cases, typically with a subsidiary role. Among them, emerge mostly individuals who knew what the perpetrator wanted to achieve, and either supported them actively or implicitly through complying with the ongoing threat, without resisting it. Another section in the analysis chapter delineated the factors that had a role in the case. In this regard, elements such as the pattern of digital oversharing, the attention economy culture, overconfidence or insecurity in terms of identity, the influence of the family, emotional trauma and sense of control over one's life appear as essential reasons for the success of the cognitive threats.

Another aspect that informed the prevention strategies pertains to whether the cognitive threats represent any potential for war actions or not. The majority of the case studies do not reveal any potential for military measures because of the following reasons. First, in the case of espionage, this cognitive threat is used both in wartime and peacetime. Second, in the case of Russian disinformation, the threat is not even a crime. Third, in the case of Cambridge Analytica, their actions were in the grey zone between legal and illegal. Only in the case with ISIS, the cognitive threat represents some war potential but only because of the terrorist attacks of ISIS, and not because of the recruitment itself.

Next, as I explored the political mechanisms making the cognitive threat possible, I discovered that in three out of the four case studies, they are related to the antagonistic relationship between perpetrators and victims, and because of overlapping interest between individuals living in the enemy-state, and the perpetrators themselves. The only case that does not correspond to these conclusions is the one with Cambridge Analytica, in which the political mechanism, driving the cognitive threat is the desire for profits and the lack of legislation regulating the company's allowed tactics for making these profits.

In terms of the psychological mechanisms bringing cognitive threats to life, the results showed that in the case with Maria Butina, it was the concept of identity, that was among the reasons for the infiltration along with persuasion and the ability to deceive and avoid suspicion. In the second case, persuasion also appears as an engine behind the disinformation campaign along with the power of the confirmation bias and the construction of social networks that contain predominantly, if not exclusively, like-minded individuals. In the case of ISIS recruitment, the psychological mechanism was the victim's perceived loss of control over their life. The addictive nature of social media, the culture of oversharing and psychological profiling were the mechanisms through which Cambridge Analytica became successful in their political campaign services. Except for persuasion, that was possible because of unique factors inherent for each case, there is no other overlap between psychological techniques that were used in the listed cases of cognitive threats.

Based on the findings from this research, some policy recommendations should be outlined. The concrete prevention strategies against cognitive threats, produced by the analysis of the case studies showed measures that have to be adopted in six categories. First, state and non-state actors, supported by local communities should create alternatives to the incentive (e.g., a product, a content, lifestyle or employment) offered by the state or non-state perpetrator of the cognitive threat to the victims, or even to some direct individual perpetrators who are employees of the state/non-state perpetrator. Second, the narrative about individuals who were either victims before they become perpetrators themselves or the ones who were forced to collaborate to the state-perpetrator's goals out of financial necessity has to be changed. They should not be vilified but described as victims of particular circumstances and political goals. Moreover, the narrative should illustrate the downsides and the potential fallacy of the promises the perpetrators made to the individuals in an attempt to fulfill their agenda. Third, the stakeholders involved in cases of cognitive threats, especially states, should have unequivocal positions on what happened, why it happened, who did it, and what will be done to prevent the threat in the future. Fourth, strong legislative measures should be an integral part of a successful defense against cognitive threats.

They should aim to regulate the actions in the digital space, including disinformation, political targeting and any other adverse effects on the free, democratic processes. Besides, some administrative agencies, such as a regulatory commission responsible for the digital space, could also be established, as a result of introducing new pieces of legislation on a state or supranational level. Fifth, another critical element in preventing cognitive threats is education about the digital space, religion, and misinterpretations of religious readings and premises. Another component that has to be addressed through education pertains to immigrants in the conditions of the expanding globalization. Mainly, how to achieve a harmonious balance between physical and mental migration, how to address differences between conservative and liberal cultures, between emotional trauma that may lead to radicalization and grief that makes room for a healthy way of healing. The sixth mechanism for countering cognitive threats is the awareness of them that should be promoted by state and non-state actors (including the media and the academia). In particular, they should address how cognitive threats occur, why they are harmful, and what are their consequences for the individual, the community, the state and the democracy itself.

A few paragraphs should be dedicated to the limitations of the proposed strategies and the conditions under which they have the potential to be effective. First, creating alternatives for the victims of cognitive threats requires a large amount of funding that has to be invested in this prevention mechanism to be successful. As states are the units with most authority to implement measures against cognitive threats, and assuming they should be the ones investing the material resources for this strategy, they may be incapable of allocating such funds or just reluctant to do so. This outcome could be due to personal interests of politicians and their party affiliations with various state and non-state actors, pressure by different lobbies, unstable economic conditions of the state itself or merely because they do not recognize cognitive threats as a risk deserving of such significant amount of resources. Regarding the cultural aspects of creating alternatives for the victim of cognitive threats, communities and families may be skeptical to having open conversations about some conservative norms that older generations expect younger generations to obey without any resistance or without questioning their rightfulness (e.g., religion, arranged marriages at a young age, conversations regarding controversial events in the world). Additionally, the strategy for creating alternatives may fail to produce the desired effects in cases of espionage because the spies may feel as they have no other choice but to serve the state out of fear for retribution if they refuse to cooperate. As for disinformation, the confirmation bias in humans could turn out to be a tendency difficult to change, especially when the recipient of the information has a predilection to the stance taken through this information. Thus, the goal to reorient readers of deceitful information delivered by untrustworthy websites to other sources of information containing proven facts could hide various caveats. The culture of oversharing on social media, the addiction to these platforms and the predictable reaction of people experiencing fear could also be challenging to overcome when it comes to cognitive threats. Moreover, the civic consciousness of people regarding the digital space may not develop for many years or not even at all unless they begin to perceive consequences from violations of their privacy in the digital space the same way they assess harm in the physical space.

The second group of strategies that pertains to the recommended change in the narrative about victims and perpetrators of cognitive threats also should be examined with some caution. If intense hostility between states existed for extensive periods of time (e.g., the Cold War), it may be difficult to change the narrative about the rival country or at least, it will be difficult for the people of the vilified country to be persuaded that they are no longer seen as enemies. In addition, a significant role in creating the public image of a rival state has the media. Obeying the contemporary requirements of the attention-economy culture, they may prefer to circulate headlines that stimulate strong reactions in people, mostly pejorative in nature, because this increases their attention and hence, their profits. Lastly, states, non-state actors and some politicians may not be inclined to invoke a change in the narrative simply because they purposefully use people's fear of *enemies* for political gains.

Establishing unambiguous state positions on cognitive threats as a third strategy that I suggest could also be a challenging task. This tendency is observed in cases when politicians and party/parties in power have an interest in maintaining the status-quo, especially when the threat comes from an entity that they are favorable of, supporting, or when the existing threat creates more political gains for them than losses. Diplomatic considerations are also among the reasons why many state officials abstain from taking a firm stance against cognitive threats made by another state.

The same concerns also translate to establishing legislative measures about the digital space. Pressure by lobbyists, personal investments of politicians or interest in maintaining the current legislation beneficiary to some power structures (so that they can use cognitive threats domestically or against opponents abroad) could reveal notable obstacles to creating and implementing strong legislation for violations in the digital space. Another element that could exacerbate the level of success of this mechanism is the possibility, existing with any law, that it could be still somehow circumvented.

Education, as a prevention strategy against cognitive threats, also has some limitations that should be mentioned. On the one hand, it would be most effective with young people who still have not formed an established view on issues. For adults, on the other hand, education could be effective only if the recipient of the educational content intentionally seeks it or they are at least open to considering some information potentially contradicting some of their beliefs. However, for people, especially such who are firmly convinced in the rightfulness of a specific position or stance, education could not be an applicable mechanism for defense against cognitive threats. Even for people who are open to obtaining new educational information, the confirmation bias, their group identity, and their social networks typically consisting of like-minded people could be posing some obstacles to the success of this strategy. Undoubtedly, some of them could be introduced to new educational information regarding cognitive threats that they will accept even if it is not in full accordance with their current beliefs and those of their peers. That said, education would be most effective when offered to younger people and adults who could be persuaded to learn to recognize and resist attempts for cognitive threats by malicious actors. At the same time, problems with implementing educational information could also be encountered in the party responsible for distributing these educational campaigns – states, non-state actors, and individuals. States may decide not to allocate the funding for such campaigns or to choose to promote the message in ways that fail to reach the desired audience. Besides, politicians may be reluctant to advocate for such campaigns because it would decrease political benefits that they get from the existence of cognitive threats. Some NGOs may also fail to promote the educational messages because of lack of resources (material and human), because of flaws of the campaign itself or the way it is intended to reach the recipients.

Similar arguments and concerns could be repeated for the last strategy that I recommended – bringing awareness of the problem. In addition to them, another considerable obstacle for the applicability of this technique could be the relative lack of recognition of cognitive threats as such and the need for their prevention in public policy and scholarly agendas. For the first category, the problem with attribution of the act brings a diplomatic dilemma that may make state officials hesitant to attract attention to a problem without being capable of providing evidence implicating the perpetrator. At the same time, due to the nature of this threat and the fact it concerns the human cognition and psychological rather than material processes, political scientists may be reluctant to focus on the problem and examine it. Influence, information processing, and decision-making are categories that could hardly be quantified and their causal relationship to politics and international security could hardly be proven beyond doubt.

In light of these limitations, some strategies under some conditions, appear more useful and applicable than others. The state as the most powerful figure among communities and individuals has the most authority to counter cognitive threats on a large scale. Therefore, the strategies based on state involvement have the most potential for combatting cognitive threats and should be perceived as primary. In particular, creating alternatives for victims and perpetrators of cognitive threats and establishing clear state positions and creating legislation for regulating the digital space would be viable strategies only for states that have the material resources to support such programs, states that are not dependent on actors who are benefitting from cognitive threats and such that recognize the problem and have the determination to combat it. Community participation in creating alternatives for victims and perpetrators of cognitive threats could be dependent on various individual factors, and its impact will be significant only if a large number of communities join efforts in creating a conversation about culture, religion and religious formations, immigration, and adaptation. Changing the narrative about victims and perpetrators of cognitive threats also includes many different actors with sometimes conflicting interests. The process also takes a lot of time to produce the desired results. Considering these requirements, it is less likely that strategies that do not require state involvement will succeed and to this extent, they should be perceived more as supplementary, secondary mechanisms for mitigating cognitive threats. As such, education and awareness of the problem as strategies will also become dependent on the level of state intervention in the fight against cognitive threats.

Since cognitive threats have always been an integral part of warfare and conflicts and in more recent times also in marketing, it would be unreasonable to believe they will disappear since they have been so successful. Advances in Artificial Intelligence (AI) and the proliferation of the Internet of Things (IoT) devices present practically endless opportunities for data collection by companies whose users unknowingly provide large amounts of information through smart devices. This fact is what makes cognitive threats even more severe issue than before. The expectations are that societies will become more reliant on technologies, more interconnected. Thus, the companies controlling the services in the technology and communications sector will become even more powerful. Without a stable legislative framework and civic consciousness about this changing environment, individuals will be increasingly exposed to digital privacy violations. No state policy is capable of eliminating the problem completely, as advances in the protection from cognitive threats will result in commensurate advances in the ways cognitive threats are made and executed. However, a combination of state policies and actions, community engagement, and the awareness of the pertinent threat posed to human cognition has a strong potential to at least mitigate the threat.

So far, cognitive threats in their diverse manifestations are somewhat recognized as a problem in various academic fields but not in politics. If academics identify cognitive threats, first, as a weapon in the post-modern warfare, and second as a strategy, deeply integrated into marketing and political marketing fields, state intervention will become more likely. Introducing the problem in its entirety on a state- and even multistate level will help with limiting the harmful consequences from cognitive threats. However, if they keep existing only as an anonymous enemy, conceptually ignored by the study of politics, and by policy-makers, the eventual solutions to the problem will become more and more distant. In this case, humanity's fate will be to relive the repercussions of the Trojan Horses in peoples' cognitions again, and again.

BIBLIOGRAPHY

Abrams, Steve. "Beyond propaganda: Soviet active measures in Putin's Russia." *Connections: The Quarterly Journal* 15, no. 1 (2016): 5-31.

Adams, Stephen, Andy Bloxham, and Gordon Rayner. "Anna Chapman: profile of a 'Russian spy'." *The Telegraph*, 2010.

Agadjanian, Alexander. "Tradition, morality and community: elaborating Orthodox identity in Putin's Russia." *Religion, State & Society* 45, no. 1 (2017): 39-60.

Ahmed, Sara. *The cultural politics of emotion.* New York: Routledge, 2004.

Aistrope, Tim. "Social media and counterterrorism strategy." *Australian Journal of International Affairs* 70, no. 2 (2016): 121-38.

Akkerman, Nadine. "The Postmistress, the Diplomat, and a Black Chamber?: Alexandrine of Taxis, Sir Balthazar Gerbier and the Power of Postal Control." In *Diplomacy and Early Modern Culture*, edited by Robyn Adams and Rosanna Cox, 172-88. New York, NY: Palgrave Macmillan, 2011.

Al-Jablawi, Hosam. "A Closer Look at the Educational System of ISIS." *Atlantic Council*, 2016.

Alaimo, Kara. "Mark Zuckerberg has lost all credibility with Congress -- and the rest of us." *CNN*, 2018.

Alford, Stephen. "Some Elizabethan Spies in the Office of Sir Francis Walsingham." In *Diplomacy and Early Modern Culture*, edited by Robyn Adams and Rosanna Cox, 46-62. New York, NY: Palgrave Macmillan, 2011.

Almohammad, Asaad. "ISIS Child Soldiers in Syria: The Structural and Predatory Recruitment, Enlistment, Pre-Training Indoctrination, Training, and Deployment." edited by The International Centre for Counter-Terrorism –The Hague, 2018.

Ames, Roger T. *Sun-Tzu: The Art of Warfare.* New York, NY: The Random House Publishing Group, 1993.

Andreassen, Cecilie Schou, Joël Billieux, Mark D. Griffiths, Daria J. Kuss, Zsolt Demetrovics, Elvis Mazzoni, and Ståle Pallesen. "The relationship between addictive use of social media and video games and symptoms of psychiatric disorders: A large-scale cross-sectional study." *Psychology of Addictive Behaviors* 30, no. 2 (2016): 252.

Aro, Jessikka. "The cyberspace war: propaganda and trolling as warfare tools." *European View* 15, no. 1 (2016): 121-32.

Asmundson, Gordon J. G., Jenora L. Kuperos, and G. Ron Norton. "Do patients with chronic pain selectively attend to pain-related information?: preliminary evidence for the mediating role of fear." *PAIN* 72, no. 1 (1997/08/01/ 1997): 27-32.

Assembly, United Nations General. "Universal declaration of human rights." 1948.

Atkinson, Richard C., and Richard M. Shiffrin. "Human memory: A proposed system and its control processes.". In *Psychology of Learning and Motivation* edited by Kenneth W. Spence, and Janet Taylor Spence, 89-195. London: Academic Press, 1968.

Augustyn, Joseph. "Maria Butina Is Not Unique." *The Atlantic*, 2019.

Aune, Sean P. "Why Did Everyone Leave MySpace For Facebook?" TechnoBuffalo.

Awan, Imran. "Cyber-extremism: Isis and the power of social media." *Society* 54, no. 2 (2017): 138-49.

Bachmann, Sascha Dov, and Hakan Gunneriusson. "Hybrid Wars: The 21st-Century's New Threats to Global Peace and Security." *Scientia Militaria, South African Journal of Military Studies* 43, no. 1 (2015): 77-98.

Balibar, Etienne. "The nation form: history and ideology." *Review (Fernand Braudel Center)* 13, no. 3 (1990): 329-61.

Barber, Peter. "'Procure as many as you can and send them over': Cartographic Espionage and Cartographic Gifts in International Relations, 1460–1760." In *Diplomacy and Early Modern Culture*, edited by Robyn Adams and Rosanna Cox, 13-29. New York, NY: Palgrave Macmillan, 2011.

Bargh, John A. "The four horsemen of automaticity: Awareness, intention, efficiency, and control in social cognition." In *Handbook of social cognition*, edited by Robert S. Wyer Jr, and Thomas K. Srull. Basic Processes, 1-40. New York: Psychology Press, 1994.

Barnes, Susan B. "A privacy paradox: Social networking in the United States." *First Monday* 11, no. 9 (2006-09-04 2006).

Batchelor, Oliver. "Getting out the truth: the role of libraries in the fight against fake news." *Reference services review* 45, no. 2 (2017): 143-148.

Benmelech, Efraim, and Esteban F. Klor. "What Explains the Flow of Foreign Fighters to ISIS?". *Terrorism and Political Violence* (2018): 1-24.

Bennetts, Marc. "Anna Chapman: Agent provocateur " *The Guardian*, 2011.

Bennhold, Katrin. "Jihad and Girl Power: How ISIS Lured 3 London Girls." *The New York Times*, 2015.

Biddle, William W. "A psychological definition of propaganda." *The Journal of Abnormal and Social Psychology* 26, no. 3 (1931): 283-95.

Bigo, Didier. "Security and immigration: Toward a critique of the governmentality of unease." *Alternatives: Global, Local, Political* 27, no. 1 (2002): 63-92.

Bjola, Corneliu, and James Pamment. "Digital containment: Revisiting containment strategy in the digital age." *Global Affairs* 2, no. 2 (2016): 131-42.

Black, Joseph Laurence. "Setting the tone: Misinformation and disinformation from Kyiv, Moscow, Washington and Brussels in 2014." In *The return of the cold war: Ukraine, the west and Russia*, edited by Joseph Laurence Black and Michael Johns, 163-94: Routledge, 2016.

Blitz, Marc Jonathan. "Lies, Line Drawing, and (Deep) Fake News." *Oklahoma Law Review* 71, no. 1 (2018): 59-116.

Bloom, Mia. "Constructing expertise: Terrorist recruitment and “talent spotting” in the PIRA, Al Qaeda, and ISIS." *Studies in Conflict & Terrorism* 40, no. 7 (2017): 603-23.

Boden, Margaret A. "Précis of the creative mind: Myths and mechanisms." *Behavioral and brain sciences* 17, no. 3 (1994): 519-31.

Booth, Ken. *Strategy and Ethnocentrism* New York: Routledge, 2014.

Boswell, Christina, Andrew Geddes, and Peter Scholten. "The role of narratives in migration policy-making: A research framework." *The British Journal of Politics and International Relations* 13, no. 1 (2011): 1-11.

Bourdieu, Pierre, and Samar Farage. "Rethinking the state: Genesis and structure of the bureaucratic field." *Sociological theory* 12, no. 1 (1994): 1-18.

Bower, Gordon H. "Mood and memory." *American psychologist* 36, no. 2 (1981): 129-48.

Boyd, Danah. "Facebook's privacy trainwreck: Exposure, invasion, and social convergence." *Convergence* 14, no. 1 (2008): 13-20.

Branquinho, João. "The foundations of cognitive science." Oxford: Clarendon Press, 2001.

Brinker-Gabler, Gisela, and Sidonie Smith. *Writing new identities: gender, nation, and immigration in contemporary Europe.* MInneapolis, MN: University of Minnesota Press, 1997.

Brown, Harold I. *Problems of philosophy: Their past and present. Rationality.* New York: Routledge, 1988.

Brown, Leah. "Why cognitive hacking is a public health crisis." *TechRepublic*, 2017.

Bruner, Jerome S., Jacqueline J. Goodnow, and George A. Austin. *A study of thinking.* New York: John Wiley, 1956.

Bueno de Mesquita, Bruce, David Newman, and Alvin Rabushka. *Forecasting political events the future of Hong Kong.* New Haven, CT: Yale University Press, 1985.

Bulgurcu, Burcu, Hasan Cavusoglu, and Izak Benbasat. "Understanding Emergence and Outcomes of Information Privacy Concerns: a Case of Facebook." Paper presented at the International Conference on Information Systems (ICIS), 2010.

Buzan, Barry, Ole Wæver, and Jaap De Wilde. *Security: a new framework for analysis.* Boulder, CO: Lynne Rienner Publishers, 1998.

Byman, Daniel L., and Kenneth M. Pollack. "Let us now praise great men: Bringing the statesman back in." *International Security* 25, no. 4 (2001): 107-46.

Cadwalladr, Carole. "Cambridge Analytica a year on: ‘a lesson in institutional failure’ " *The Guardian*, 2019.

———. "‘I made Steve Bannon’s psychological warfare tool’: meet the data war whistleblower " *The Guardian*, 2018.

Cadwalladr, Carole, and Emma Graham-Harrison. "Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach " *The Guardian*, 2018.

Cahill, Caitlin. "'Why do they hate us?'Reframing immigration through participatory action research." *Area* 42, no. 2 (2010): 152-61.

Campbell, David. *Writing security: United States foreign policy and the politics of identity.* Minneapolis, MN: University of Minnesota Press, 1992.

Caute, David. *The dancer defects: the struggle for cultural supremacy during the Cold War.* Oxford, UK: Oxford University Press, 2003.

Chafetz, Glenn. "The struggle for a national identity in post-soviet Russia." *Political Science Quarterly* 111, no. 4 (1996): 661-88.

Chanowitz, Benzion, and Ellen J. Langer. "Premature cognitive commitment." *Journal of Personality and Social Psychology* 41, no. 6 (1981): 1051-63.

Chapman, C. Richard. "Pain, perception and illusion." In *The psychology of pain*, edited by Richard A. Sternbach, 153-79. New York: Raven Press, 1986.

Chebel d'Appollonia, Ariane. *Frontiers of Fear: Immigration and Insecurity in the United States.* Ithaca, NY: Cornell University Press, 2012.

Cialdini, Robert B. *Influence: The psychology of persuasion.* New York, NY: Collins 2007.

Ciampaglia, Giovanni Luca. "Fighting fake news: a role for computational social science in the fight against digital misinformation." *Journal of Computational Social Science* 1, no. 1 (January 01 2018): 147-53.

Čižik, Tomáš. "Information Warfare–Europe's New Security Threat." *CENAA Policy Papers* 3 (2016).

———. "Russian Information Warfare in Central Europe." *Information Warfare–New Security Challenge for Europe. Bratislava: Centre for European and North Atlantic Affairs* (2017): 8-34.

Collins, International Spy Museum with Denis. *Spying the secret history of history.* New York, NY: Black Dog & Leventhal, 2004.

Connell, Michael, and Sarah Vogler. "Russia's Approach to Cyber Warfare." edited by Center for Naval Analysis, 2017.

Costa Jr., Paul T., and Robert R. McCrae. "Four ways five factors are basic." *Personality and individual differences* 13, no. 6 (1992): 653-65.

Cowan, Joseph L. *Pleasure and Pain: A Study in Philosophical Psychology.* Vol. 19, London: Macmillan, 1968.

Crawford, Neta C. "Institutionalizing passion in world politics: fear and empathy." *International Theory* 6, no. 3 (2014): 535-57.

Cuomo, Serafina. *Technology and culture in Greek and Roman antiquity.* New York, NY: Cambridge University Press, 2007.

Cybenko, George, Annarita Giani, and Paul Thompson. *Cognitive Hacking.* Vol. 60, 2004. doi:10.1016/S0065-2458(03)60002-1.

———. "Cognitive Hacking: A Battle for the Mind." *Computer* 35, no. 8 (2002): 50-56.

Damasio, Antonio R. *Descartes' error emotion, reason, and the human brain.* New York: G.P. Putnam, 1994.

———. "Reflections on the neurobiology of emotion and feeling." In *The foundations of cognitive science*, edited by João Branquinho, 99-108. Oxford: Clarendon Press, 2001.

Danilova, Maria. "Truth and the Russian media." *Columbia Journalism Review*, 2014.

Davidson, Donald. "What thought requires." In *The foundations of cognitive science*, edited by João Branquinho, 121-32. Oxford: Clarendon Press, 2001.

Daybell, James. "Gender, Politics and Diplomacy: Women, News and Intelligence Networks in Elizabethan England." In *Diplomacy and Early Modern Culture*, edited by Robyn Adams and Rosanna Cox, 101-19. New York, NY: Palgrave Macmillan, 2011.

De Mesquita, Bruce Bueno. *Principles of International Politics.* Thousand Oaks, CA: SAGE Publications, 2013.

De Oliver, Miguel. "Nativism and the obsolescence of grand narrative: Comprehending the quandary of anti-immigration groups in the neoliberal era." *Journal of Ethnic and Migration Studies* 37, no. 7 (2011): 977-97.

Debatin, Bernhard, Jennette P Lovejoy, Ann-Kathrin Horn, and Brittany N Hughes. "Facebook and online privacy: Attitudes, behaviors, and unintended consequences." *Journal of computer-mediated communication* 15, no. 1 (2009): 83-108.

Decety, Jean, and Claus Lamm. "Empathy versus personal distress: Recent evidence from social neuroscience." In *The social neuroscience of empathy.*, edited by Jean Decety and William Ickes. Social neuroscience., 199-213. Cambridge, MA: MIT Press, 2009.

Department of Justice. "Grand Jury Indicts 12 Russian Intelligence Officers for Hacking Offenses Related to the 2016 Election." news release, 2018, https://www.justice.gov/opa/pr/grand-jury-indicts-12-russian-intelligence-officers-hacking-offenses-related-2016-election.

———. "Russian National Charged in Conspiracy to Act as an Agent of the Russian Federation Within the United States." news release, 2018, https://www.justice.gov/opa/pr/russian-national-charged-conspiracy-act-agent-russian-federation-within-united-states.

———. "Sioux Falls Man Charged with Wire Fraud and Money Laundering." news release, 2019, https://www.justice.gov/usao-sd/pr/sioux-falls-man-charged-wire-fraud-and-money-laundering-0.

———. "Ten Alleged Secret Agents Arrested in the United States." news release, 2010, https://www.justice.gov/opa/pr/ten-alleged-secret-agents-arrested-united-states.

Disinformation Review. "Top 3 targets of disinformation." *EU vs. Disinformation*, 2018.

Dornbusch, Sanford M., Albert H. Hastorf, Stephen A. Richardson, Robert E. Muzzy, and Rebecca S. Vreeland. "The perceiver and the perceived: Their relative influence on the categories of interpersonal cognition." *Journal of Personality and Social Psychology* 1, no. 5 (1965): 434-40.

Drever, James. *A dictionary of psychology.* Oxford, England: Penguin Books, 1952.

Dulles, Allen. *The craft of intelligence: America's legendary spy master on the fundamentals of intelligence gathering for a free world.* Guilford, CT: The Lyons Press, 2006.

Dvornik, Francis. *Origins of Intelligence Services: The Ancient Near East, Persia, Greece, Rome, Byzantium, the Arab Muslim Empires, the Mongol Empire, China, Muscovy.* New Brunswick, NJ: Rutgers University Press, 1974.

Ellul, Jacques. *False presence of the kingdom.* Seabury Press, 1972.

Ennaji, Moha. "Recruitment of foreign male and female fighters to Jihad: Morocco's multifaceted counter-terror strategy." *International Review of Sociology* 26, no. 3 (2016): 546-57.

Eysenck, Michael W. *Anxiety: The cognitive perspective.* Hove, UK: Lawrence Erlbaum Associates Ltd. Publishers, 1992.

Eysenck, Michael W., and Mark T. Keane. *Cognitive psychology: A student's handbook.* 3 ed. Hillsdale, NJ, US: Larence Erlbaum Associates Ltd. Publishers, 1995.

Eysenck, Michael W., Colin MacLeod, and Andrew Mathews. "Cognitive functioning and anxiety." *Psychological research* 49, no. 2-3 (1987): 189-95.

Eysenck, Michael W., Karin Mogg, Jon May, Anne Richards, and Andrew Mathews. "Bias in interpretation of ambiguous sentences related to threat in anxiety." *Journal of abnormal psychology* 100, no. 2 (1991): 144-50.

Faris, Robert, Hal Roberts, Bruce Etling, Nikki Bourassa, Ethan Zuckerman, and Yochai Benkler. "Partisanship, propaganda, and disinformation: Online media and the 2016 US presidential election." edited by Berkman Klein Center for Internet & Society at Harvard University, 2017.

Farwell, James P. "Countering Russian Meddling in US Political Processes." *Parameters* 48, no. 1 (2018): 37-47.

———. "The media strategy of ISIS." *Survival* 56, no. 6 (2014): 49-55.

Feldman, Ofer, and Linda O. Valenty. *Profiling political leaders: Cross-cultural studies of personality and behavior.* Westport, CT: Greenwood Publishing Group, 2001.

Feldman, Ruth. "On the origins of background emotions: From affect synchrony to symbolic expression." *Emotion* 7, no. 3 (2007): 601-11.

Ferrara, Emilio. "Disinformation and social bot operations in the run up to the 2017 French presidential election." *First Monday* 22, no. 8 (2017).

Festinger, Leon. *A theory of cognitive dissonance.* Vol. 2, Palo Alto, CA: Stanford University Press, 1962.

Festinger, Leon, and James M. Carlsmith. "Cognitive consequences of forced compliance." *Journal of Abnormal and Social Psychology* 58, no. 2 (1959): 203-11.

Financial Action Task Force. "Financing of the Terrorist Organization Islamic State in Iraq and the Levant (ISIL)." Paris 2015.

Firozabadi, Babak Sadighi, Yao-Hua Tan, and Ronald M. Lee. "Formal definitions of fraud." In *Norms, logics and information systems-new studies in Deontic logic and computer science*, edited by Paul McNamara and Henry Prakken, 275-88. Amsterdam, Netherlands: IOS Press, 1999.

Fiske, Susan T., and Shelley E. Taylor. *Social cognition.* Reading, MA: Addison-Wesley Publishing Company, 1984.

Fletcher, Andrew. "Russian Hacking and the U.S. Election: Against International Law?". *Michigan Journal of International Law (MJIL)* 38 (2016).

Foner, Nancy, and Patrick Simon. *Fear, anxiety, and national identity: Immigration and belonging in North America and Western Europe*. Russell Sage Foundation, 2015.

Foran, Clare, Sara Murray, and Jessica Schneider. "Democratic lawmakers ask NRA for answers over 2015 Moscow trip and alleged Russian ties." *CNN*, 2019.

Fried, Daniel, and Alina Polyakova. "Democratic defense against disinformation." edited by Atlantic Council: Atlantic Council Washington, DC, 2018.

Friedman, Thomas L. "DOScapital." *Foreign Policy*, no. 116 (1999): 110-16.

Fukuyama, Francis. *The end of history and the last man.* New York, NY: Simon and Schuster, 2006.

———. "Immigrants and family values." *Commentary* 95, no. 5 (1993): 26-32.

Garnham, Alan. *The Mind in Action: A Personal View of Cognitive Science.* London: Routledge, 1991.

Gavin, Harvey. "Germany ‘to strip ISIS fighters of citizenship’ with new law." *Express*, 2019.

Gelders, Dave, and Øyvind Ihlen. "Government communication about potential policies: Public relations, propaganda or both?". *Public Relations Review* 36, no. 1 (2010): 59-62.

George, Frank. *Cognition.* London: Methuen, 1962.

Gergen, Kenneth J. *The psychology of behavior exchange.* Topics in Social Psychology. Edited by Charles A. Kiesler. Oxford, England: Addison-Wesley Publishing Company, Inc., 1969.

Gerstel, Dylan. "ISIS and Innovative Propaganda: Confronting Extremism in the Digital Age." *Swarthmore International Relations Journal* 1, no. 1 (2017): 1-9.

Girodo, Michel, and Douglas Wood. "Talking yourself out of pain: The importance of believing that you can." *Cognitive Therapy and Research* 3, no. 1 (1979): 23-33.

Goble, Paul. "Lies, damned lies and Russian disinformation." *Eurasia Daily Monitor* 13 (2014).

Gordts, Eline. "This Is What Education Under ISIS In Raqqa Will Look Like " *The Huffington Post*, 2014.

Goubert, Liesbet, Kenneth D. Craig, and Ann Buysse. "Perceiving others in pain: Experimental and clinical evidence on the role of empathy." In *The social neuroscience of empathy*, edited by Jean Decety and William Ickes. Social neuroscience., 153-65. Cambridge, MA: MIT Press, 2009.

Govani, Tabreez, and Harriet Pashley. "Student awareness of the privacy implications when using Facebook." *Carnegie Mellon University* (2005).

Govier, Trudy. *The Philosophy of Argument.* Newport News, VA: Vale Press, 1999.

Granville, Kevin. "Facebook and Cambridge Analytica: What You Need to Know as Fallout Widens." *The New York Times*, 2018.

Green, J. J. "Tale of a Troll: Inside the 'Internet Research Agency' in Russia." *Washington's Top News*, 2018.

Greenberg, Karen J. "Counter-radicalization via the internet." *The ANNALS of the American Academy of Political and Social Science* 668, no. 1 (2016): 165-79.

Griffith, Eric. "How to Prevent Facebook From Sharing Your Personal Data." *PC Magazine*, 2018.

Groll, Elias. "A Brief History of Attempted Russian Assassinations by Poison." *Foreign Policy* (2018).

Gross, Ralph, and Alessandro Acquisti. "Information revelation and privacy in online social networks." Paper presented at the Proceedings of the 2005 ACM workshop on Privacy in the electronic society, 2005.

Habeck, Mary R. *Knowing the enemy: Jihadist ideology and the war on terror.* New Haven, CT: Yale University Press, 2007.

Hadzhidimova, Lora, and Brian K. Payne. "The profile of the international cyber offender in the US." *International Journal of Cybersecurity Intelligence & Cybercrime* 2, no. 1 (2019): 40-55.

Hall, Richard. "What happens to ISIS fighters when they are captured." *Public Radio International (PRI)*, 2016.

Hamilton, David L. "Cognitive representations of persons." Paper presented at the Social cognition: The Ontario Symposium, Ontario, CA, 1981.

Hampson, Fen Osler. "Human Security." Chap. 19 In *Security Studies: An Introduction*, edited by Paul D. Williams, 279-94. New York, NY: Routledge, 2012.

Harrison, Caitlin. "Education Under ISIS: A 'Generation in Darkness'." *The Borgen Project*, 2015.

Heider, Fritz. *The psychology of interpersonal relations.* New York: Wiley, 1958.

Herman, Michael. "Diplomacy and intelligence." *Diplomacy and statecraft* 9, no. 2 (1998): 1-22.

Hermann, Margaret G. "Explaining foreign policy behavior using the personal characteristics of political leaders." *International Studies Quarterly* 24, no. 1 (1980): 7-46.

Hern, Alex. "Cambridge Analytica: how did it turn clicks into votes?" *The Guardian*, 2018.

Hern, Alex, and David Pegg. "Facebook fined for data breaches in Cambridge Analytica scandal." *The Guardian*, 2018.

Hindman, Matthew. "How Cambridge Analytica’s Facebook targeting model really worked – according to the person who built it." *The Conversation*, 2018.

Hobbes, Thomas. *Leviathan.* New York: London & Toronto, J. M. Dent & sons, ltd.

New York, E. P. Dutton & co., 1965.

Hogg, Michael A, and Dominic Abrams. *Social identifications: A social psychology of intergroup relations and group processes.* London: Routledge, 1988.

Hollander, Edwin Paul. "Conformity, status, and idiosyncrasy credit." *Psychological Review* 65, no. 2 (1958): 117-27.

———. *Leaders, groups, and influence.* New York, NY: Oxford University Press, 1964.

Holmes, David S., and B. Kent Houston. "Effectiveness of situation redefinition and affective isolation in coping with stress." *Journal of Personality and Social psychology* 29, no. 2 (1974): 212-18.

Hopf, Ted. "The logic of habit in international relations." *European journal of international relations* 16, no. 4 (2010): 539-61.

Houston, B. Kent. "Dispositional anxiety and the effectiveness of cognitive strategies in stressful laboratory and classroom situations." In *Stress and anxiety*, edited by C D Spielberg and Irwin G Sarason. New York: Wiley, 1977.

Hsu, Tiffany. "For Many Facebook Users, a 'Last Straw' That Led Them to Quit." *The New York Times*, 2018.

Hutchinson, Robert. *Elizabeth's spymaster: Francis Walsingham and the secret war that saved England.* London, UK: Weidenfeld & Nicolson, 2006.

Hutchison, Emma. "Trauma and the politics of emotions: constituting identity, security and community after the Bali bombing." *International Relations* 24, no. 1 (2010): 65-86.

Hutchison, Emma, and Roland Bleiker. "Theorizing emotions in world politics." *International Theory* 6, no. 3 (2014): 491-514.

Hyman, Ray. "The psychology of deception." *Annual review of psychology* 40, no. 1 (1989): 133-54.

Ickes, William. "Empathic accuracy." *Journal of personality* 61, no. 4 (1993): 587-610.

Ifraimova, Simon Shuster and Sandra. "A Former Russian Troll Explains How to Spread Fake News." *Time*, 2018.

Innes, Alexandria J. "When the threatened become the threat: The construction of asylum seekers in British media narratives." *International Relations* 24, no. 4 (2010): 456-77.

Innes, Alexandria, and Brent Steele. "Memory, trauma and ontological security." In *Memory and Trauma in International Relations: Theories, Cases and Debates*, edited by Erica Resende and Dovile Budryte. New York: Routlege, 2013.

Isaak, Jim, and Mina J. Hanna. "User Data Privacy: Facebook, Cambridge Analytica, and Privacy Protection." *Computer* 51, no. 8 (2018): 56-59.

Jaitner, Margarita Levin, and Harry Kantola. "Applying Principles of Reflexive Control in Information and Cyber Operations." *Journal of Information Warfare* 15, no. 4 (2016): 27-38.

Janis, Irving L., and Leon Mann. *Decision making: A psychological analysis of conflict, choice, and commitment.* New York: Free Press, 1977.

Jensen, Benjamin, Brandon Valeriano, and Ryan Maness. "Fancy bears and digital trolls: Cyber strategy with a Russian twist." *Journal of Strategic Studies* 42, no. 2 (2019): 212-34.

Jervis, Robert. "Leadership, post-Cold War politics, and psychology." *Political Psychology* 15, no. 4 (1994): 769-77.

———. "Political psychology: Some challenges and opportunities." *Political Psychology* 10, no. 3 (1989): 481-93.

Jessie K. Liu, United States Attorney. "United States v. Mariia Butina." edited by U.S. Department of Justice. Washington, DC 2018.

Johnson, Carrie. "Paul Erickson, Boyfriend Of Russian Agent Maria Butina, Charged In Fraud Scheme." *NPR*, 2019.

Johnson, Jean E. "Psychological interventions and coping with surgery." In *Handbook of Psychology and Health*, edited by Andrew Baum, Shelley E. Taylor and Jerome E. Singer, 167-87. Hillsdale, NJ: Erlbaum, 1984.

Jowett, Garth S., and Victoria O'Donnell. *Propaganda & persuasion.* Sage Publications, 2014.

Kahneman, Daniel, and Amos Tversky. "Prospect Theory: An Analysis of Decision under Risk." *Econometrica* 47, no. 2 (1979): 263-92.

Kanouse, David E., and L. Reid Hanson Jr. "Negativity in evaluations." In *Attribution: Perceiving the Causes of Behavior*, edited by Edward E Jones, David E Kanhouse, Harold H Kelley, Richard E Nisbett, Stuart Valins and Bernanrd Weiner, 47-62. Morristown, N.J.: General Learning Press, 1972.

Katzenstein, Peter J, ed. *The culture of national security: Norms and identity in world politics*. New York, NY: Columbia University Press, 1996.

Katzenstein, Peter J. *The culture of national security: Norms and identity in world politics.* New York, NY: Columbia University Press, 1996.

Katzenstein, Peter J., and Nobuo Okawara. "Japan, Asian-Pacific security, and the case for analytical eclecticism." *International Security* 26, no. 3 (2002): 153-85.

Kelley, Harold H. "Attribution theory in social psychology." Paper presented at the Nebraska symposium on motivation, Lincoln, NE, 1967.

Keohane, Robert O., and Joseph S. Nye. *Power and interdependence.* 4th ed.. ed. Boston, MA: Longman, 2012.

Kiesler, Charles A., Barry A. Collins, and Norman Miller. *Attitude Change: A Critical Analysis of Theoretical Approaches.* New York: Wiley, 1969.

King, Gary, Jennifer Pan, and Margaret E Roberts. "How the Chinese government fabricates social media posts for strategic distraction, not engaged argument." *American Political Science Review* 111, no. 3 (2017): 484-501.

Kinnvall, Catarina. "Globalization and religious nationalism: Self, identity, and the search for ontological security." *Political psychology* 25, no. 5 (2004): 741-67.

Koschut, Simon, Todd H. Hall, Reinhard Wolf, Ty Solomon, Emma Hutchison, and Roland Bleiker. "Discourse and emotions in international relations." *International Studies Review* 19, no. 3 (2017): 481-508.

Kotowski, Jan Michael. "Narratives of Immigration and National Identity: Findings from a Discourse Analysis of German and US Social Studies Textbooks." *Studies in Ethnicity and Nationalism* 13, no. 3 (2013): 295-318.

Kragh, Martin, and Sebastian Åsberg. "Russia's strategy for influence through public diplomacy and active measures: the Swedish case." *Journal of Strategic Studies* 40, no. 6 (2017): 773-816.

Krasnova, Hanna, Sarah Spiekermann, Ksenia Koroleva, and Thomas Hildebrand. "Online social networks: Why we disclose." *Journal of information technology* 25, no. 2 (2010): 109-25.

Kratochwil, Friedrich V. *Rules, norms, and decisions: on the conditions of practical and legal reasoning in international relations and domestic affairs.* Vol. 2, New York, NY: Cambridge University Press, 1991.

Krause, Keith, and Michael C. Williams. "Broadening the Agenda of Security Studies: Politics and Methods." *Mershon International Studies Review* 40, no. 2 (1996): 229-54.

Kremlin Watch. "The Prague Manual: How to Tailor National Strategy Using Lessons Learned from Countering Kremlin's Hostile Subversive Operations in Central and Eastern Europe." In *European Values Protecting Freedom*, 2018.

Krueger, Joachim, and Russell W. Clement. "The truly false consensus effect: An ineradicable and egocentric bias in social perception." *Journal of personality and social psychology* 67, no. 4 (1994): 596-610.

Kurilla, Ivan. "Shaping new narratives: How new histories are created." In *The return of the cold war: Ukraine, the west and Russia*, edited by Joseph Laurence Black and Michael Johns, 195-200: Routledge, 2016.

Lanoszka, Alexander. "Russian hybrid warfare and extended deterrence in eastern Europe." *International affairs* 92, no. 1 (2016): 175-95.

Lapowsky, Issie. "Senators Grill Whistleblower on Cambridge Analytica's Inner Workings." *Wired*, 2018.

Lasswell, Harold D. "The Theory of Political Propaganda." *American Political Science Review* 21, no. 3 (1927): 627-31.

Laterza, Vito. "Cambridge Analytica, independent research and the national interest." *Anthropology Today* 34, no. 3 (2018): 1-2.

Leavitt, Harold J. "Some effects of certain communication patterns on group performance." *The Journal of Abnormal and Social Psychology* 46, no. 1 (1951): 38-50.

Lerner, Melvin J. "The desire for justice and reactions to victims." In *Altruism and helping behavior: Social psychological studies of some antecedents and consequences*, edited by Jacqueline Macaulay and Leonard Berkowitz, 205-29. New York: Academic Press, 1970.

Leshchenko, Sergii. "The Media's Role." *Journal of Democracy* 25, no. 3 (2014): 52-57.

Leyens, Jacques-Philippe, Paola M Paladino, Ramon Rodriguez-Torres, Jeroen Vaes, Stephanie Demoulin, Armando Rodriguez-Perez, and Ruth Gaunt. "The emotional side of prejudice: The attribution of secondary emotions to ingroups and outgroups." *Personality and social psychology review* 4, no. 2 (2000): 186-97.

Leyens, Jacques-Philippe, Vincent Yzerbyt, and Georges Schadron. *Stereotypes and social cognition.* Thousand Oaks, CA: Sage Publications, Inc, 1994.

Lindemann, Albert S. *A history of modern Europe from 1815 to the present.* Malden, MA: John Wiley & Sons, 2013.

Lough, John, Orysia Lutsevych, Peter Pomerantsev, Stanislav Secrieru, and Anton Shekhovtsov. "Russian influence abroad: Non-state actors and propaganda." *Chatham House* 24 (2014).

Lubsky, Anatoly Vladimirovich, Alina Gavrilovna Lurje, Alexander Vasilievich Popov, Irina Borisovna Serikova, and Dmitry Sergeevich Zagutin. "Russia in search of national integration model." *Mediterranean journal of social sciences* 6, no. 4 (2015): 209.

Lukyanov, Fyodor. "Russia–EU: the partnership that went Astray." *Europe-Asia Studies* 60, no. 6 (2008): 1107-19.

Lyman, Peter. "The Domestication of Anger: The Use and Abuse of Anger in Politics." *European Journal of Social Theory* 7, no. 2 (2004): 133-47.

MacFarquhar, Neil. "Russian Trolls Were Sloppy, but Indictment Still 'Points at the Kremlin'." *The New York Times*, 2018.

Machiavelli, Niccolò. *The prince.* Edited by Harvey C. Mansfield. 2nd ed. Chicago, IL: University of Chicago Press, 1998.

Madden, Pete, Matthew Mosk, and Kyra Phillips. "Lover or cover? Maria Butina and the romance at the heart of an alleged Russian influence operation." *ABC News*, 2018.

Magra, Iliana. "Dutch ISIS Fighter, Husband of Shamima Begum, Wants to Return Home With Family." *The New York Times*, 2019.

Mamadouh, Virginie. "The scaling of the 'Invasion': A geopolitics of immigration narratives in France and The Netherlands." *Geopolitics* 17, no. 2 (2012): 377-401.

Mann, Richard D. "A review of the relationships between personality and performance in small groups." *Psychological bulletin* 56, no. 4 (1959): 241-70.

Marcus, George E., W. Russell Neuman, and Michael MacKuen. *Affective intelligence and political judgment.* Chicago: University of Chicago Press, 2000.

"Maria Butina: Russian gun activist in U.S. conspiracy case." *BBC*, 2018.

Marshall, Gary D., and Philip G. Zimbardo. "Affective consequences of inadequately explained physiological arousal." *Journal of Personality and Social Psychology* 37, no. 6 (1979): 970-88.

Marwick, Alice, and Rebecca Lewis. "Media manipulation and disinformation online." *New York: Data & Society Research Institute* (2017).

Maslach, Christina. "Negative Emotional Biasing of Unexplained Arousal." *Journal of Personality and Social Psychology* 37, no. 6 (1979): 953-69.

McDermott, Rose. "The feeling of rationality: The meaning of neuroscientific advances for political science." *Perspectives on politics* 2, no. 4 (2004): 691-706.

———. *Political psychology in international relations.* Ann Arbor, MI: University of Michigan Press, 2004.

McDonald-Gibso, Charlotte. "What Should Europe Do With the Children of ISIS?" *The New York Times*, 2017.

McGeehan, Timothy P. "Countering Russian Disinformation." *Parameters* 48, no. 1 (2018): 49-57.

Mearsheimer, John J. "The false promise of international institutions." *International security* 19, no. 3 (1994): 5-49.

Mejias, Ulises A., and Nikolai E. Vokuev. "Disinformation and the media: the case of Russia and Ukraine." *Media, Culture & Society* 39, no. 7 (2017): 1027-42.

Milardo, Robert M. "Personal Choice and Social Constraint in Close Relationships: Applications of Network Analysis." In *Friendship and Social Interaction*, edited by Valerian J. Derlega and Barbara A. Winstead, 145-66. New York, NY: Springer, 1986.

Milgram, Stanley. *Obedience to authority an experimental view.* 1st ed. New York: Harper & Row, 1974.

Milner, Helen V. *Interests, institutions, and information: Domestic politics and international relations.* Princeton, NJ: Princeton University Press, 1997.

Mitts, Tamar. "From isolation to radicalization: anti-Muslim hostility and support for ISIS in the West." *American Political Science Review* 113, no. 1 (2019): 173-94.

Morgenthau, Hans Joachim. *Politics among nations the struggle for power and peace.* 4th ed. New York, NY: Knopf, 1967.

Mullen, Brian, and George R. Goethals. "Social projection, actual consensus and valence." *British Journal of Social Psychology* 29, no. 3 (1990): 279-82.

Murray, Sara. "Special counsel briefly interviewed Maria Butina, sources say." *CNN*, 2019.

United Nations, "Charter of the United Nations, Chapter I." 2019.

North Atlantic Treaty Organization. "Cooperative Cyber Defence Centre of Excellence - About us."

———. "Strategic Foresight Analysis." Norfolk, VA 2017.

Newcomb, Theodore M. *The acquaintance process.* The acquaintance process. New York, NY: Holt, Rinehart & Winston, 1961. doi:10.1037/13156-000. doi:10.1037/13156-000.

Nichols, Marden Fitzpatrick. *Author and Audience in Vitruvius' De Architectura.* Washington, DC: Cambridge University Press, 2017.

Niklewicz, Konrad. "Weeding Out Fake News: An Approach to Social Media Regulation." *European View* 16, no. 2 (2017): 335-35.

Nimmo, Ben. "Identifying disinformation: an ABC. Policy Brief Issue 2016/01-February 2016." In *Archives of European Integration (AEI)*, edited by Institute for European Studies (IES), 2016.

Nolan, Cathal J. *The Age of Wars of Religion, 1000-1650: An Encyclopedia of Global Warfare and Civilization.* Vol. 2, Westport, CT: Greenwood Publishing Group, 2006.

Noor, Naseema. "Tunisia: The revolution that started it all." *International Affairs Review*, 2011.

Nussbaum, Martha C. *Upheavals of thought: The intelligence of emotions.* New York: Cambridge University Press, 2003.

Nye Jr., Joseph S., and Sean M. Lynn-Jones. "International security studies: a report of a conference on the state of the field." *International security* 12, no. 4 (1988): 5-27.

O'Sullivan, Donie, Jeremy Herb, and Manu Raju. "Cambridge Analytica whistleblower to appear before Congress next week." *CNN*, 2018.

Oates, Sarah. "The neo-Soviet model of the media." *Europe-Asia Studies* 59, no. 8 (2007): 1279-97.

———. "When Media Worlds Collide: Using Media Model Theory to Understand How Russia Spreads Disinformation in the United States." In *American Political Science Association 2018 Annual Meeting, Boston MA*. Boston, MA, 2018.

Ost, David. "Politics as the Mobilization of Anger: Emotions in Movements and in Power." *European Journal of Social Theory* 7, no. 2 (2004): 229-44.

Ozumba, Geoffrey O. "National consciousness, value reorientation and identity: An Integrative Humanist Approach." *Journal of Integrative Humanism* 3, no. 2 (2014): 147-55.

Paul, Christopher, and Miriam Matthews. "The Russian "firehose of falsehood" propaganda model." *Rand Corporation* (2016): 2-7.

Peresin, Anita, and Alberto Cervone. "The western muhajirat of ISIS." *Studies in Conflict & Terrorism* 38, no. 7 (2015): 495-509.

Perry, David L. ""Repugnant Philosophy": Ethics, Espionage, and Covert Action." *Journal of Conflict Studies* 15, no. 1 (1995).

Polyakova, Alina. "Putinism and the European Far Right." *Institute of Modern Russia* 19 (2016): 2016.

Porotsky, Sophia. "Social media and the access it provides to voter data give Russian active measures the ability to influence the outcome of an election." *Global Security Review*, 2018.

Post, Jerrold M. "Current concepts of the narcissistic personality: Implications for political psychology." *Political Psychology* 14, no. 1 (1993): 99-121.

Powell, Jason. "Scholars, Servants, Spies: William Weldon and William Swerder in England and Abroad." In *Diplomacy and Early Modern Culture*, edited by Robyn Adams and Rosanna Cox, 30-45. New York, NY: Palgrave Macmillan, 2011.

Praks, Henrik. "Hybrid Or Not: Deterring and Defeating Russia's Ways of Warfare in the Baltics: the Case of Estonia." (2015).

Project, Counter Extremism. "ISIS's Persecution of Religions." 2017.

Puddington, Arch. *Broadcasting freedom: the cold war triumph of radio free Europe and radio liberty.* Lexington, KY: University Press of Kentucky, 2000.

Pun, Darien. "Rethinking espionage in the modern era." *Chi. J. Int'l L.* 18 (2017): 353.

"Putin spokesman Peskov's daughter working as E.U. intern." *BBC*, 2019.

Ramsay, Adam. "The High Court found that Vote Leave broke the law in a new way." *Open Democracy*, 2018.

Reed, Alastair, Jeanine de Roy van Zuijdewijn, and Edwin Bakker. "Pathways of foreign fighters: Policy options and their (un) intended consequences." In *ICCT Policy Brief*, edited by International Center for Counter-Terrorism (The Hague), 2015.

Reuter, Christopher. "The Terror Strategist: Secret Files Reveal the Structure of Islamic State." *Der Spiegel*, 2015.

Riehle, Kevin, and Michael May. "Human-cyber Nexus: the parallels between 'illegal'intelligence operations and advanced persistent threats." *Intelligence and National Security* 34, no. 2 (2019): 189-204.

Rogowski, Ronald. "The Rise of Experimentation in Political Science." In *Emerging Trends in the Social and Behavioral Sciences*, edited by Robert A. Scott, Marlis C. Buchmann and Stephen M. Kosslyn. New York, NY: John Wiley & Sons Inc., 2016.

Romerstein, Herbert. "Disinformation as a KGB Weapon in the Cold War." *Journal of Intelligence History* 1, no. 1 (2001): 54-67.

Rosenberg, Matthew. "Cambridge Analytica, Trump-Tied Political Firm, Offered to Entrap Politicians." *The New York Times*, 2018.

Ross, Cameron. "State against civil society: Contentious politics and the non-systemic opposition in Russia." *Europe-Asia Studies* 67, no. 2 (2015): 171-76.

Ross, Lee. "The Intuitive Psychologist And His Shortcomings: Distortions in the Attribution Process." In *Advances in Experimental Social Psychology*, edited by Leonard Berkowitz, 173-220. New York, NY: Academic Press, 1977.

Rousseau, David L., and Rocio Garcia-Retamero. "Identity, power, and threat perception: A cross-national experimental study." *Journal of Conflict Resolution* 51, no. 5 (2007): 744-71.

Rubinstein, Ira S., and Nathaniel Good. "Privacy by design: A counterfactual analysis of Google and Facebook privacy incidents." *Berkeley Technology Law Journal* 28 (2013): 1333.

Rudnitsky, Jake, and Evgenia Pismennaya. "NRA-Linked Russia Central Banker Retires." *Bloomberg*, 2018.

Russell, Frank Santi. *Information gathering in classical Greece.* Ann Arbor, MI: University of Michigan Press, 1999.

Russett, Bruce M., and John R. Oneal. *Triangulating peace democracy, interdependence, and international organizations.* New York, NY: Norton, 2001.

"Russian woman charged with spying in the U.S.". *BBC*, 2018.

Sadowski, Jathan. "Companies are making money from our personal data – but at what cost?" *The Guardian*, 2016.

Saltman, Erin Marie, and Charlie Winter. "Islamic state: The changing face of modern jihadism." *London: Quilliam Foundation* (2014): 1-71.

Scannell, Kara, Sara Murray, and Mary Ilyushina. "The Russian accused of using sex, lies and guns to infiltrate U.S. politics." *CNN*, 2018.

Schachter, Stanley, and Jerome Singer. "Cognitive, social, and physiological determinants of emotional state." *Psychological review* 69, no. 5 (1962): 379-99.

Schacter, Stanley. "The psychology of affiliation: Experimental studies of the sources of gregariousness." Stanford, CA: Stanford University Press, 1959.

Schoth, Daniel E., Vanessa Delgado Nunes, and Christina Liossi. "Attentional bias towards pain-related information in chronic pain; a meta-analysis of visual-probe investigations." *Clinical Psychology Review* 32, no. 1 (2012/02/01/ 2012): 13-25.

Searle, John R. "Rationality and Action." In *The Foundations of Cognitive Science*, edited by João Branquinho, 197-210. Oxford: Clarendon Press, 2001.

Security, Commission on Human. "Human Security Now." New York, NY 2003.

Shane, Scott. "These Are the Ads Russia Bought on Facebook in 2016." *The New York Times*, 2017.

Shaver, Kelly G. "Defensive attribution: Effects of severity and relevance on the responsibility assigned for an accident." *Journal of Personality and Social Psychology* 14, no. 2 (1970): 101-13.

———. "Redress and conscientiousness in the attribution of responsibility for accidents." *Journal of Experimental Social Psychology* 6, no. 1 (1970): 100-10.

Shaw, Tony, and Denise Jeanne Youngblood. *Cinematic Cold War: The American and Soviet struggle for hearts and minds.* University Press of Kansas Lawrence, 2010.

Shehabat, Ahmad, and Teodor Mitew. "Black-boxing the black flag: anonymous sharing platforms and ISIS content distribution tactics." *Perspectives on Terrorism* 12, no. 1 (2018).

Sheldon, Rose Mary. *Intelligence Activities in Ancient Rome: Trust in the Gods But Verify.* New York, NY: Frank Cass, 2005.

Shkliarov, Vitali. "“Dead Souls” to swing Georgia’s presidential election?" *New Eastern Europe*, 2018.

Siegel, Harvey. "Rationality and judgment." *Metaphilosophy* 35, no. 5 (2004): 597-613.

Silk, Michael S., Ingo Gildenhard, and Rosemary Barrow. "The Classical Tradition: Art, Literature, Thought." Hoboken, NJ: John Wiley & Sons, Incorporated, 2013.

Simon, Herbert A. "Human nature in politics: The dialogue of psychology with political science." *American Political Science Review* 79, no. 2 (1985): 293-304.

———. "Rationality in political behavior." *Political psychology* (1995): 45-61.

Singer, P. W., and Emerson T. Brooking. *LikeWar: The Weaponization of Social Media.* New York, NY: Eamon Dolan Books, 2018.

Slack, Tim, and Leif Jensen. "Underemployment across immigrant generations." *Social Science Research* 36, no. 4 (2007): 1415-30.

Small, Deborah A., and Jennifer S. Lerner. "Emotional Policy: Personal Sadness and Anger Shape Judgments about a Welfare Case." *Political Psychology* 29, no. 2 (2008): 149-68.

Smith, Adam. *The theory of moral sentiments.* New York, NY: Penguin, 2010.

Snead, Jason. "Voter Fraud Database Tops 1,000 Proven Cases." edited by The Heritage Foundation, 2017.

Sommerville, Quentin, and Riam Dalati. "An education in terror." *BBC News*, 2017.

Speckhard, Anne. "ISIS and the Rise of Homegrown Terrorism in the West." *Security Solutions Magazine* 24 (2015).

Stelzenmüller, Constanze. "The impact of Russian interference on Germany's 2017 elections." *Testimony before the US Senate Select Committee on Intelligence June* 28 (2017).

Stergiou, Dimitrios. "ISIS political economy: financing a terror state." *Journal of Money Laundering Control* 19, no. 2 (2016): 189-207.

Stewart, Brian T. W., and Samantha Newbery. *Why Spy? The Art of Intelligence.* London, UK: Hurst & Company, 2015.

Stotland, Ezra, and Arthur L. Blumenthal. "The reduction of anxiety as a result of the expectation of making a choice." *Canadian Journal of Psychology/Revue canadienne de psychologie* 18, no. 2 (1964): 139-45.

Sullivan, Kate, and Sara Murray. "Political operative who was dating alleged Russian spy Maria Butina indicted." *CNN*, 2019.

Sultan, Christopher. "Russian Spy Anna Chapman Finds Celebrity at Home." *Spiegel*, 2010.

"Sweden Democrats call on government to strip Isis fighters of citizenship." *The Local*, 2019.

Synnott, John, Andria Coulias, and Maria Ioannou. "Online trolling: the case of Madeleine McCann." *Computers in Human Behavior* 71 (2017): 70-78.

Szpiler, Jack A., and Seymour Epstein. "Availability of an avoidance response as related to autonomic arousal." *Journal of Abnormal Psychology* 85, no. 1 (1976): 73-82.

Tacchini, Eugenio, Gabriele Ballarin, Marco L Della Vedova, Stefano Moret, and Luca de Alfaro. "Some like it Hoax: Automated fake news detection in social networks." Paper presented at the 2nd Workshop on Data Science for Social Good, SoGood 2017, 2017.

Teper, Yuri. "Official Russian identity discourse in light of the annexation of Crimea: national or imperial?". *Post-Soviet Affairs* 32, no. 4 (2016): 378-96.

Thomas, Timothy. "Russia's reflexive control theory and the military." *Journal of Slavic Military Studies* 17, no. 2 (2004): 237-56.

Thucydides. *The complete writings of Thucydides. The Peloponnesian war.* Edited by Richard Crawley and Joseph Gavorse. New York, NY: The Modern Library, 1934.

Tudjman, Miroslav, and Nives Mikelic. "Information science: Science about information, misinformation and disinformation." *Proceedings of Informing Science+ Information Technology Education* (2003): 1513-27.

Tulving, Endel. "Episodic and semantic memory." In *Organization of memory*, edited by Endel Tulving and Wayne Donaldson, 381-403. London: Academic Press, 1972.

Tupman, W. A. "Ten myths about terrorist financing." *Journal of Money Laundering Control* 12, no. 2 (2009): 189-205.

Turner, John C. "Social categorization and the self-concept: A social cognitive theory of group behavior." In *Advances in group processes*, edited by Edward J. Lawler, 77-121. Greenwich, CT: JAI Press, 1985.

———. "Towards a cognitive redefinition of the social group." In *Social identity and intergroup relations*, edited by Henri Tajfel, 15-40. Cambridge: Cambridge University Press, 1982.

Tversky, Amos, and Daniel Kahneman. "Judgment under Uncertainty: Heuristics and Biases." *Science* 185 (1974): 1124-31.

U.S. Department of the Treasury. "Treasury Designates Russian Oligarchs, Officials, and Entities in Response to Worldwide Malign Activity " news release, 2018, https://home.treasury.gov/news/press-releases/sm0338.

Valentino, Nicholas A., Vincent L. Hutchings, Antoine J. Banks, and Anne K. Davis. "Is a Worried Citizen a Good Citizen? Emotions, Political Information Seeking, and Learning via the Internet." *Political Psychology* 29, no. 2 (2008): 247-73.

Vallacher, Robin R. "Objective self awareness and the perception of others." *Personality and Social Psychology Bulletin* 4, no. 1 (1978): 63-67.

Van Herpen, Marcel H. *Putin's Propaganda Machine: Soft Power and Russian Foreign Policy.* Rowman & Littlefield, 2015.

Veebel, Viljar. "Russian propaganda, disinformation, and Estonia’s experience." edited by Foreign Policy Research Institute, 2015.

Vogel, Gretchen. "Scientists probe feelings behind decision-making." *Science* 275, no. 5304 (1997): 1269-69.

Von Clausewitz, Carl. *On War.* Translated by Michael Howard and Peter Paret. Princeton, NJ: Princeton University Press, 1976.

Wagenaar, Willem A. "My memory: A study of autobiographical memory over six years." *Cognitive psychology* 18, no. 2 (1986): 225-52.

Wagner, Kurt. "This is how Facebook uses your data for ad targeting " *Recode*, 2018.

Walker, Stephen G., and Lawrence S. Falkowski. "The Operational Codes of U.S. Presidents and Secretaries of State: Motivational Foundations and Behavioral Consequences." *Political Psychology* 5, no. 2 (1984): 237-66.

Walster, Elaine. "Assignment of responsibility for an accident." *Journal of personality and social psychology* 3, no. 1 (1966): 73-79.

Walt, Stephen M. "The Renaissance of Security Studies." *International Studies Quarterly* 35, no. 2 (1991): 211-39.

Waltz, Kenneth Neal. *Theory of international politics.* 1st ed. Boston, MA: McGraw-Hill, 1979.

Wegner, Daniel M. "Attribute generality: The development and articulation of attributes in person perception." *Journal of Research in Personality* 11, no. 3 (1977): 329-39.

Wegner, Daniel M., and John A. Bargh. "Control and automaticity in social life." In *The Handbook of Social Psychology, Vols. 1-2, 4th ed.*, 446-96. New York, NY: McGraw-Hill, 1998.

Wegner, Daniel M., and Robin R. Vallacher. *Implicit psychology: An introduction to social cognition.* New York: Oxford University Press, 1977.

Weiner, Bernard, Irene Frieze, Andy Kukla, Linda Reed, Stanley Rest, and Robert M. Rosenbaum. "Perceiving the causes of success and failure." In *Attribution: Perceiving the Causes of Behavior*, edited by Edward E Jones, David E Kanhouse, Harold H Kelley, Richard E Nisbett, Stuart Valins and Bernanrd Weiner, 95-120. Morristown, N.J.: General Learning Press, 1972.

Wendt, Alexander. *Social theory of international politics.* Cambridge, UK: Cambridge University Press, 1999.

Wendt, Alexander E. "The agent-structure problem in international relations theory." *International organization* 41, no. 3 (1987): 335-70.

Wiggins, Jerry S., and Aaron L. Pincus. "Personality: Structure and assessment." *Annual review of psychology* 43, no. 1 (1992): 473-504.

Williams, Paul D. *Security Studies: An Introduction.* New York, NY: Routledge, 2012.

Windsor, Leah. "The Language of Radicalization: Female Internet Recruitment to Participation in ISIS Activities." *Terrorism and Political Violence* (2018): 1-33.

Wortman, Camille B., and Jack W. Brehm. "Responses to Uncontrollable Outcomes." In *Advances in experimental social psychology*, edited by Leonard Berkowitz, 277-336. New York: Academic Press, 1975.

Wright, Rex A., and Sharon S. Brehm. "Reactance as impression management: A critical review." *Journal of Personality and Social Psychology* 42, no. 4 (1982): 608-18.

Yayla, Ahmet S., and Anne Speckhard. "Telegram: The mighty application that ISIS loves." edited by International Center for the Study of Violent Extremism, 2017.

Younger, Neil. "Robert Peake (c1551—1619) and the Babington Plot." *The British Art Journal* 14, no. 2 (2013): 65-67.

Zaller, John, and Stanley Feldman. "A simple theory of the survey response: Answering questions versus revealing preferences." *American Journal of Political Science* 36, no. 3 (1992): 579-616.

ЛЕВАДА-ЦЕНТР. "Враги России." 2018.

VITA

Lora Pitman has a PhD in International Studies at Old Dominion University. She earned her MA degree in Humanities at ODU in 2014. She also holds an LL.M. degree from Sofia University, Bulgaria. Previously, she completed internships with the Operational Analysis branch in NATO-ACT and the Joint Forces Staff College in Norfolk, VA. Her publications appear in the International Journal of Cybersecurity Intelligence & Cybercrime, Criminal Justice Studies, the International Journal of Criminal Justice Sciences, and in POLITIKON, the IAPSS Journal of Political Science. She is also a co-editor of Advances in Defense Analysis, Concept Development and Experimentation, published by NATO HQ-SACT.