2021-03

MEDIA EFFECTS ON CYBER INTRUSIONS

McCarthy, Mitchell J.

Monterey, CA; Naval Postgraduate School

https://hdl.handle.net/10945/67152

NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

DISSERTATION

MEDIA EFFECTS ON CYBER INTRUSIONS

by

Mitchell J. McCarthy

March 2021

Dissertation Supervisor: Timothy C. Warren

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE	*Form Approved OMB No. 0704-0188*

Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington, DC, 20503.

1. AGENCY USE ONLY ***(Leave blank)***	**2. REPORT DATE** March 2021	**3. REPORT TYPE AND DATES COVERED** Dissertation

4. TITLE AND SUBTITLE MEDIA EFFECTS ON CYBER INTRUSIONS	**5. FUNDING NUMBERS**
6. AUTHOR(S) Mitchell J. McCarthy	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000	**8. PERFORMING ORGANIZATION REPORT NUMBER**
9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES) NPS Foundation, Monterey, CA 93940	**10. SPONSORING / MONITORING AGENCY REPORT NUMBER**

11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.

12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release. Distribution is unlimited.	**12b. DISTRIBUTION CODE** A

13. ABSTRACT (maximum 200 words)

In this current hyperconnected era, many could argue that multifaced daily news events, arranged into univocal storylines, generate effects well beyond the media environment. Empirically speaking, most explorations of media and cyberspace focus discretely on one or the other, parochially missing their potential interaction. More specifically, could negative media events, laced with dueling narratives, aimed at the United States and its interests by other countries on a given day, impact the level of cyber intrusions on U.S. networks the next day? The purpose of this study is to relate today's recorded cyber intrusions on a U.S. network to yesterday's media events using statistical regression models as the method of testing for the relationship's existence. The analysis begins with a broad investigation of all regimes, and then proceeds through specific regime types, before narrowing down to case studies of specific countries. The evidence provided from these models bears out that negative media narratives projected by other countries toward the U.S. generate measurable impacts on the level of ensuing intrusions on U.S. networks. Furthermore, these effects vary in important ways across countries and regime types contingent upon their unique culture, political context, and evolutionary setting.

14. SUBJECT TERMS media effects theory, narrative theory, two-level theory of international affairs, two-step flow of media effects, conflict and rivalry, digital panopticon, sharp power, democracies, anocracies, autocracies, negative media tone, negative media polarization, negative material narratives, negative verbal narratives, cyber intrusions	**15. NUMBER OF PAGES** 315
	16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT Unclassified	**18. SECURITY CLASSIFICATION OF THIS PAGE** Unclassified	**19. SECURITY CLASSIFICATION OF ABSTRACT** Unclassified	**20. LIMITATION OF ABSTRACT** UU

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release. Distribution is unlimited.

MEDIA EFFECTS ON CYBER INTRUSIONS

Mitchell J. McCarthy
Civilian, Department of the Navy
BBA, Texas A & M University, 1987
MS, Management, Naval Postgraduate School, 1999
MS, Industrial College of The Armed Forces, 2007

Submitted in partial fulfillment of the
requirements for the degree of

DOCTOR OF PHILOSOPHY IN INFORMATION SCIENCES

from the

NAVAL POSTGRADUATE SCHOOL
March 2021

Approved by:

Timothy C. Warren
Department of
Defense Analysis
Dissertation Supervisor

Raymond R. Buettner
Department of
Information Sciences

Douglas J. MacKinnon
Department of
Information Sciences

Wayne Porter
Department of
Defense Analysis

Dan C. Boger
Graduate School of
Operational and Information Sciences
Dissertation Chair

Approved by:

Alex Bordetsky
Chair, Department of Information Sciences

Orrin D. Moses
Vice Provost of Academic Affairs

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

In this current hyperconnected era, many could argue that multifaced daily news events, arranged into univocal storylines, generate effects well beyond the media environment. Empirically speaking, most explorations of media and cyberspace focus discretely on one or the other, parochially missing their potential interaction. More specifically, could negative media events, laced with dueling narratives, aimed at the United States and its interests by other countries on a given day, impact the level of cyber intrusions on U.S. networks the next day? The purpose of this study is to relate today's recorded cyber intrusions on a U.S. network to yesterday's media events using statistical regression models as the method of testing for the relationship's existence. The analysis begins with a broad investigation of all regimes, and then proceeds through specific regime types, before narrowing down to case studies of specific countries. The evidence provided from these models bears out that negative media narratives projected by other countries toward the U.S. generate measurable impacts on the level of ensuing intrusions on U.S. networks. Furthermore, these effects vary in important ways across countries and regime types contingent upon their unique culture, political context, and evolutionary setting.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF FIGURES

LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

AI	Artificial Intelligence
AIC	Akaike Information Criterion
AKP	Justice and Development Party (Turkey)
AME	Average Marginal Effect
B	Billion
BILGEM	Informatics and Information Security Research Center (Turkey)
BTK	Information and Communication Technologies Authority (Turkey)
CAMEO	Conflict and Mediation Event Observations
CCP	Chinese Communist Party
CCTV	Closed-Circuit Television
CIA	Central Intelligence Agency
CyCon	International Cyber Conflict Conference
GDP	Gross Domestic Product
ICANN	Internet Corporation for Assigned Names and Numbers
ICT	Information and Communications Technology
IDS	Intrusion Detection System
IRI	Islamic Republic of Iran
ISP	Internet Service Protocol
IT	Information Technology
Kbps	Kilobits per second
M	Million
MAE	Mean Average Error
Mbps	Megabits per second
NATO	North Atlantic Treaty Organization
NN	Negative Narratives
NSA	National Security Agency (a.k.a., No Such Agency)
PRC	People’s Republic of China
RIM	Research In Motion (Canadian IT Firm)
RMSE	Root Mean Square Error
SCS	Social Credit System (China)

TIB	Presidency of Telecommunications and Communications (Turkey)
TOR	The Onion Router
UID	Unique Identification Project (India)
UIDAI	Unique Identification Authority of India
UK	United Kingdom
USSR	Union of Soviet Socialist Republics
VIF	Variance Inflation Factor
ZULU	time zone indicator for Universal Time

ACKNOWLEDGEMENTS

I would like to thank my wife, Cindy, and son, Jacob, for their unwavering patient and gracious support throughout. Next, I would like to thank my committee, Doctors Boger, Warren, Porter, Buettner, and MacKinnon, for their consistent patience and mentorship through the research and writing of this dissertation. Also, I would like thank Professors Gates and Kang for lighting the spark that drove me to start and complete this journey. Finally, I would like to thank my Savior the Lord Jesus Christ, for without him none of this would have been possible.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

A. RESEARCH SETTING

Media reporting of cyber attacks seems to increase daily, as do the associated tangible or intangible costs of such attacks on individuals or organizations.[1] Examples span from the cyber intrusions on the Sony Corporation in 2011 and 2014, to the data breach at the Office of Personnel Management in 2014, to the more recent WannaCry ransomware attacks, and Equifax intrusion of 2017, to the most recent Solar Winds hack of 2021 (Andriotis & Minaya, 2017; BBC, 2017; Kroft, 2015; Goodman, 2015; Kantchev & Strobel, 2021; Paletta & Yadron, 2015; Paletta, 2015; Richwine, 2014).[2] The pervasive nature of the internet creates a perverse expectation in many individuals, leading them to believe they must remain connected 24 hours a day, 7 days a week (Goodman, 2015).[3] As this societal dependence on ubiquitous access to the internet continues to grow, so do the opportunities for nefarious actors to exploit an internet replete with vulnerabilities (Arquilla & Ronfeldt, 1993; Denning & Denning, 2010; FireEye, M-Trends, 2016; FireEye, M-Trends, 2017; Gandhi, et al., 2011; Goodman, 2015; Hoffman, 2011; Manion & Goodrum, 2000; Mims, 2017; Stavridis, 2015).

Over the last two decades, cyber intrusions have continued to rise in frequency and magnitude. Much has been written identifying the problem at hand, but little research has been done to identify where to begin to gain an understanding of what drives this behavior (CSIS, 2008; Curran, 2010; Denning, 2001; Donohue, 2013; Goodman, 2015; Hoffman,

[1] Definitions herein use language that is combined, synthesized, or taken verbatim from the cited source(s). See Appendix A for more information and a comprehensive glossary

Cyber-attack – a cyber-operation, whether offensive or defensive in nature, that is reasonably expected to cause injury or death to human beings or damage or destruction to objects (Schmitt, 2013, p. 106).

[2] Cyber – interactions through the use of computer or digital information systems or networks (Committee on National Security Systems, 2015, p. 40; Valeriano & Maness, 2015, p. 22).

[3] Internet – the single, interconnected, worldwide system of commercial, governmental, educational, and other computer or digital information systems or networks that share (a) the protocol suite specified by the Internet Architecture Board (IAB) and (b) the name and address spaces managed by the Internet Corporation for Assigned Names and Numbers (ICANN) (Committee on National Security Systems, 2015, p. 70; Valeriano & Maness, 2015, pp. 9-17). Used throughout this paper as synonymous with the World Wide Web (WWW), cyberspace, or cyber domain.

2011; Lukasik, 2011; Lynn III, 2010; Paletta D., 2015; Paletta & Yadron, 2015). Although some fundamental research has explored the cyber intrusion phenomenon by using predictive algorithms, graphic data presentations, simulation models, and case study analysis, researchers continue to pursue a common understanding of what drives cyber-intrusions (Bass, 2000; Choo, 2011; Czosseck, Ottis, & Taliharm, 2013; Gandhi et al., 2011; Qin & Lee, 2004; Valeur, Vegna, Kruegel, & Kemmerer, 2004; Valeriano & Maness, 2014; Vatis, 2001; Yang, Holsopple, & Sudit, 2006; Yang, Stotz, Holsopple, Sudit, & Kuhl, 2009).[4] Yet, to date, no research has gathered real-world cyber intrusion data to test a conjectured relationship between exogenous catalyst(s) and cyber intrusion activity using statistical methods. For example, could diplomatic tension between the United States (US) and Iran be driving the number of intrusions on U.S. servers?[5] Some evidence exists that cyber intrusion activity may be motivated by the level of political cooperation or conflict between sovereign nations (Arquilla & Ronfeldt, 1993; Denning, 2001a; Fitri, 2011; Gandhi et al., 2011; Jordan & Taylor, 2004; Manion & Goodrum, 2000; Samuel, 2004a; Vegh, 2002). Furthermore, some adversarial state or non-state actors, operating from within or outside of a given sovereign state's borders, could be responsible for cyber intrusion activity. Direct attribution to that state or non-state actor remains an unrealized goal. Yet, someone is performing these intrusions. They do exist and most information technology organizations record information about these intrusions every second of every minute, of every hour, of every day.

[4] Cyber Intrusion – a. an event or combination of multiple events, that constitutes a cyber-incident in which a hacker or an intruder gains, or attempts to gain, access to information residing on an information system (IT) or networks, without having authorization, in violation of security policies, security procedures, or acceptable use policies (Committee on National Security Systems, 2015, p. 61; Maness & Valeriano, 2016, p. 310; Valeriano & Maness, 2014; Vatis, 2001, pp. 11-12); b. any set of methods used to surreptitiously gain access to IT systems or networks that result in actual or potential compromise to the availability, integrity, or confidentiality of the information, residing on those systems (Committee on National Security Systems, 2015, p. 61; Maness & Valeriano, 2016; Valeriano & Maness, 2014; Vatis, 2001). For example, when an IT system or network is remotely accessed for the purposes of stealing, gathering, exfiltrating or manipulating information.

[5] Server – a computer in a network that provides services (such as access to files or shared peripherals or the routing of e-mail) to other computers in the network (Webster, 2017, sec. "server").

Hence, one could envision a scenario where two countries, country X and country Y, are engaged in the exchange of competing narratives over some matter that could potentially benefit or harm one or both. In the midst of this exchange of narratives, internal actors within country X may become activated by the reported dueling narratives, obtained from media outlets, causing these actors to seek access or hack into country Y's networks, initially flagged as cyber intrusion activity.[6] Thus at the outset of initial cyber intrusion activity, an actor or hacker within Country X desires, for myriad reasons, to intrude into a server within country Y, provoked by the media narrative describing the nature of the dialogue between the two countries.[7] Conversely, this internal actor in country X activated by the competing narratives played out in open source media, could seek to enlist the assistance of the hacktivist diaspora around the world to draw attention to country X's position in dialogue with country Y.[8] Given either scenario, one might raise the following research question.

[6] Hack – a. to gain unauthorized access to computers or to computerized, information systems or networks, (Floridi, 2008, p. 8; Himma, 2008, pp. 191-192; Webster, 2017, sec. "hack"); b. related form – Hacker, noun; c. related form – Hacking, transitive verb.

Hacking – refers to acts in which a person or groups of people gain unauthorized entry to computers, information systems or networks (Floridi, 2008, p. 8; Himma, 2008, pp. 191-192; Webster, 2017).

Network(s) – Information system(s) implemented with a collection of interconnected components. Such components may include routers, hubs, cabling, telecommunications controllers, key distribution centers, and technical control devices (Committee on National Security Systems, 2015, p. 86).

[7] Hacker – an expert at programming and solving problems with a computer; a person who gains unauthorized access to and sometimes tampers with information in computers, information systems or networks (Committee on National Security Systems, 2015, p. 56; Floridi, 2008, pp. 3-24; Himma, 2008, pp. 191-192; Webster, 2017).

[8] Hacktivism – a. refers to the marriage of hacking and activism. It covers operations that use hacking techniques against a targets Internet site with the intent of disrupting normal operations but not causing serious damage. Examples are Web sit-ins and virtual blockades, automated e-mail bombs, Web hacks, computer break-ins, and computer viruses and worms (Denning D. E., 2001a, pp. 70-75); b. the commission of an unauthorized digital intrusion for the purpose of expressing a political or moral position (Himma, 2008, pp. 200-201); c. the (sometimes) clandestine use of computer hacking to help advance political causes (Manion & Goodrum, 2000, pp. 14-19); d. the nonviolent use of illegal or legally ambiguous digital tools in pursuit of political ends, combining the transgressive civil disobedience with the technology and techniques of computer hackers (Samuel A. , 2004a, p. 2); e. related form – Hacktivist, noun or adjective.

Motivation for Inquiry: How do competing narratives, reported by news media sources, between the United States (U.S.) and other sovereign states, relate to the level of future cyber-intrusion activity targeting U.S.-based information technology?

Figure 1. Research Question

Several theories exist that may assist us in our explanation.[9] The section that follows will explore the two-level model of diplomatic and domestic politics, the two-step flow model of communication, the digital panopticon concept, and the sharp power model, each of which may contribute to the theoretical basis needed to explore the cyber intrusion phenomenon that this research seeks to explain (Bentham, 2012; Galič, Timan, & Koops, 2017; Lazarsfeld, Berelson, & Gaudet, 1944; Loadenthal, 2018; Putnam, 1988; Strong, 2017; Walker & Ludwig, 2017; Walker, Kalathil, & Ludwig, 2020).

B. THEORETICAL UNDERPINNINGS

This section intends to explore how two theories, the two-level theory of diplomatic and domestic politics and two-step flow of communication, may operate together to explain how certain hacktivist's or cyber intruder's behavior is heavily influenced by the regime type of their home country. Next, a description is provided of where the requisite data resides, which will be used to develop dependent and independent variables to test the hypotheses defined at the end of the literature review. Further, an exploration of how modern era social scientists have resurrected the *panopticon effect*, originally posited by Jeremy Bentham in the late 1700s, describes how certain regime types execute and possess

[9] Explanatory inference, as used within this paper, means to derive and compare hypotheses about the hidden frameworks that may be responsible for the data (i.e., cyber-intrusions), then use an epistemic branch of science, in this case statistical correlations, to test the strength of the hypothesized relationships between the dependent variable and independent or *explanatory* variables (Godfrey-Smith, 2003, pp. 190-201).

different levels of social or societal control.[10] First, a review of the two-level theory of diplomatic and domestic politics is in order.

1. Putnam's Two-Level Theory

The two-level theory posits that a country's leadership simultaneously engages in negotiations with another country at two levels (Putnam, 1988; Trumbore, Boyer, Gibson, Harvey, & Wilkenfeld, 2000; Walton & McKersie, 1965). At level-one, country X's leadership engages in international negotiations or dialog with country Y, preferably to achieve some outcome beneficial to X. Yet, the leadership of country X must manage the narrative as they engage with country Y to achieve a desired outcome or win-set, while simultaneously managing the domestic narrative at level-two (Conceição-Heldt & Mello, 2017; Putnam, 1988; Trumbore, Boyer, Gibson, Harvey, & Wilkenfeld, 2000; Walton & McKersie, 1965). This theory describes how a nation's ruling class wields the *information* instrument of national power, not only externally as in level-one discussions with other nations, but also internally in level-two to manage or control the ongoing domestic narrative.[11] Thus, this theory provides a foundation from which to build an explanation of the cyber intrusion phenomenon.

In this case, two countries duel each other with their narratives, each trying to gain some competitive advantage over the other (Porter, 1991).[12] These two narratives remain *verbal* as the negotiation over an issue continues; however, as the negotiation verbally

[10] Digital Panopticon – an internet enabled, digital version of a structural design and theoretical concept that allows a single individual to monitor an entire institution without the observed subject's awareness of their observation. This presumes that if individuals – such as prisoners, students, workers, or citizens – understand that they may be under observation at any time; these individuals will act as though they are under examination; thus, they will self- police (Foucault, 1977, p. 216; Loadenthal, 2018, pp. 1-3; Manokha, 2018, pp. 219-237; Pinkaew, 2016, pp. 195-214).

Social Control – the rules and standards of society that circumscribe individual action and civil discourse through the inculcation of conventional sanctions and the imposition of formalized mechanisms (Webster, 2017, sec. "social control"). Used in and throughout this text as synonymous with Societal Control.

[11] Instruments of National Power include Diplomacy, Information, Military, and Economic (DIME) (Farlin, 2014, pp. 9-38; Mattis, 2018, p. 4).

[12] Competitive advantage – the unique ability of a state to utilize its resources effectively, managing to improve its value and position itself ahead of its economic or military rival (Choucri, 2012; Diehl & Goertz, 2001; Porter, 1991; Valeriano, Jensen, & Maness, 2018; Vasquez & Leskiw, 2001).

culminates, the results become real or *material* to each of these audiences. At face value, it seems as though autocracies and anocracies, because of their higher levels of *societal control*, may be more capable than democracies at controlling their level-two domestic narratives during these level-one interactions.· Ceteris paribus, democracies possess less societal control, more transparency, and less censorship over media and internet modalities, then autocracies and anocracies (Akgül & Kirlidoğ, 2015; MacKinnon, 2012; Sinpeng, 2013). So then, how does a theory based on a two-step flow of communication add to this explanation?

2. Lazarsfeld's Two-Step Theory

The two-step flow theory falls within the *minimal effects* branch of media effects theory (Katz, 2001; Postelnicu, 2008; Werder, 2009). At its heart, this two-step flow rests on the notion that people talking with or communicating with other people carry greater currency than the consumption of mass media products (Habermas, 1987, p. 437; Katz, 2001; Lazarsfeld, Berelson, & Gaudet, 1944). First (i.e., step one), opinion leaders or elites digest the latest narratives covering topical issues of the day as presented in the media, and subsequently decide upon their given position on the issue.[13] Next (i.e., step two), opinion leaders articulate this position to the populous leading to the adoption of certain aspects of their narrative by the general public (Klapper, 1960; Lazarsfeld, Berelson, & Gaudet, 1944; Neuman & Guggenheim, 2011; Postelnicu, 2008). In this modern era, these opinion leaders communicate their views about these narratives almost instantaneously, via Twitter, Facebook, Snapchat, and other forms of social media.

The conjecture here is that the two-step flow operates and reinforces within Putnam's level-two (i.e., domestic) communications between a country's leaders and the population, as depicted in the logic map found in Appendix C. While the level-two media signal may flow through the two-step process, the hackers may be part of diverse groups ranging from citizen hackers triggered by the event, to hackers affiliated with some social

[13] Elites – individuals and small, cohesive groups who wield a disproportionate level of power or influence affecting national and supranational political outcomes in a substantial way on a continuing basis (Best & Higley, 2018, p. 3; Higley & Burton, 2006, p. 14). Throughout this text, elite is synonymous with opinion or proximate leader.

movement, or to patriotic or government sponsored hackers (Anderson & Sadjadpour, 2018; Best & Higley, 2018; Biçakci, Doruk, & Mitat, 2015; Calamur, 2017; Deibert & Rohozinski, 2010; Denning D. E., 2011; Goodman, 2015; Keck & Sikkink, 1998; Kello, 2013; Lindsay J., 2014; McAdam, McCarthy, & Zald, 1999; MacKinnon, 2012; Nye, 2011; Pinkaew, 2016; Singer & Friedman, 2013; Sinpeng, 2013; Snegovaya, 2015; Thorton & Miron, 2019; Valeriano & Maness, 2015; Valeriano, Jensen, & Maness, 2018). Certainly, each of these could receive the information via the two-step flow from elites across this spectrum; whereas, the hacktivist executing the cyber intrusion may be aligned with or part of either unassociated or associated groups—as described in the scholarly literature cited here (Best & Higley, 2018; Conceição-Heldt & Mello, 2017; Higley & Burton, 2006; Higley, 2018; Lazarsfeld, Berelson, & Gaudet, 1944; Putnam, 1988; Strong, 2017). Nevertheless, parsing out specifically which grouping or movement these intrusive hackers are a part of remains beyond the scope of this research.

Thus, national leaders communicate via various media platforms to opinion leaders or elites, who in turn consume the narrative, form their opinions, and transmit them to the population. Their actions effectively alert the population, including its hacktivist elements (e.g., average citizens, members of a social movement, or government sponsored groups), to the narrative and the behavior expected. This leads to the final step in this theoretical account, whereby the hacktivists, motivated by the freshly adopted elite narrative, ply their trade and begin to conduct cyber intrusions.

Data collected by prior work in events coding nests well with media effects theory and provides volumes of data collected daily to use in formulating models to explore the above research question. Events coding began as a manual process in the early 1990s, developing over the intervening years into an electronic textual content *scraping* procedure.[14] Each scraped media event describes the *tone* of the narrative or discourse between two states (i.e., dyad) and receives a score on the Goldstein scale (Goldstein,

[14] Scraping refers to a discrete form of machine learning or [electronic] statistical learning techniques, whereby, digital text on a given website or set of websites is scanned for a predefined set of words or phrases; once discovered the information is extracted from the sources website and placed into a database for various uses such as, in this case, political discourse analysis (Monroe & Schrodt, 2008, p. 353; Monroe, Pan, Roberts, Sen, & et al., 2015, p. 71; Schrenk, 2012, pp. 227-237).

1992).[15] Essentially, the Goldstein scale ordinally places each article narrative in a directional dyad between two states spanning a cooperative (+10) narrative to a conflictual (–10) narrative. This ordinal scale allows researchers to gauge the *tone* or tenor of the media narrative directionally between states. Subsequently, events scholars break these narratives into quadrant counts depicting *verbal* cooperation, *material* cooperation, *verbal* conflict, and *material* conflict. These two variables, the Goldstein score and the material or verbal counts, provide measures of the level of discourse between states, which will be used to formulate independent or explanatory variables. This methodological process has improved considerably with the advent of scraping technology, enhanced by advances in computational capability, which allows for the scraping of hundreds of thousands of articles daily, amassing a huge resource of scaled media events data (Goldstein, 1992; Howell, 1983; Schrodt, 2012; Schrodt, 2017). This data will be used to gauge the impact of tone (e.g., negative or positive), variation in tone, and type of narrative (e.g., material or verbal) on cyber intrusions as a manifestation of the two-step flow operating and reinforcing at level-two of the domestic level, as depicted in Appendix C.

Now, depending on the regime type this effect may range from clearly to obscurely observable. For example, democracies may reside on the obscure end, because they exercise modest societal control, whereas, anocracies and autocracies may manifest clear results, due to their elaborate use of mechanisms for societal control (Freedom House, 2017; Marshall & Elzinga-Marshall, 2017). Instead of viewing the internet as a *liberating technology*, most anocracies and autocracies view and use it as a *repressive technology* uniquely suited for surveillance, censorship, and propaganda (Gunitsky, 2015; MacKinnon, 2012; Morozov, 2011; Rød & Weidmann, 2015). Some scholars refer to the internet and all of its associated technologies as the *digital panopticon* operating in these countries (Bentham, 2012; Galič, Timan, & Koops, 2017; Loadenthal, 2018; MacKinnon, 2012, pp. 75–86; Manokha, 2018).

[15] Dyad – an interaction between two elements or parts, in this case two states or countries (Oxford Dictionary, 2015, sec. "dyad").

3. Digital Panopticon Theory

The panopticon effect, so named by Jeremy Bentham, an English social theorist of the late 1700s, described a physical prison structure in which all inmates could find themselves under surveillance by unseen guards at any time (Bentham, 2012). As a result, this had the effect of causing the inmates to self-police their behavior to conform to the disciplinary norms of the prison. Foucault (1977) extended this theory by describing how government could control society as a whole (Loadenthal, 2018), while Chesterman (2011) extended the theory to describe the *digital panopticon* that is emerging across all regime types (MacKinnon, 2012; Manokha, 2018). However, the digital panopticon effect seems particularly evident in autocracies and anocracies that exploit it as a means of societal control.

The exercise of societal control in anocracies and autocracies springs from their regime type's need to intensely regulate their population and the narratives. The internet provides a uniquely designed environment that facilitates traceability and, depending on the regime type (a.k.a., level of democracy or polity score), a panoptic surveillance of who is talking about what to whom. Thus, this digital panopticon enables anocracies and autocracies to squelch certain narratives, while promoting others, further fortifying their societal control (Gunitsky, 2015; MacKinnon, 2012; Manokha, 2018; Pinkaew, 2016). Figure 2 provides a world map where each country's level of democracy is coded and color from autocracy (–10 / red) through democracy (+10 / green), which corresponds to the polity scores in Appendix G (Marshall & Cole, 2014; Marshall & Elzinga-Marshall, 2017; Polity IV, 2018).

In this case, this pervasive means of societal control appears to be the method by which anocratic and autocratic state leaders control their civil society through the elites to expand their negotiation and compromise space during level-one (international level) discussions with the US.[16] To lay this out plainly, first, the regime leadership

[16] Civil Society – the self-generating and self-supporting communities of people who share a normative order and volunteer to organize political, economic, or cultural activities that are independent from the state or state functions (Diamond, 1994, p. 5; Hussain M. M., 2016, p. 7).

communicates the level-two (domestic level) narrative to their elites via media outlets. Second, the regime leverages the digital panopticon to cement their control of that narrative. Third, following the two-step information flow, elites and opinion leaders digest the narrative and signal a wait and see position on the given issue being discussed at level-one.

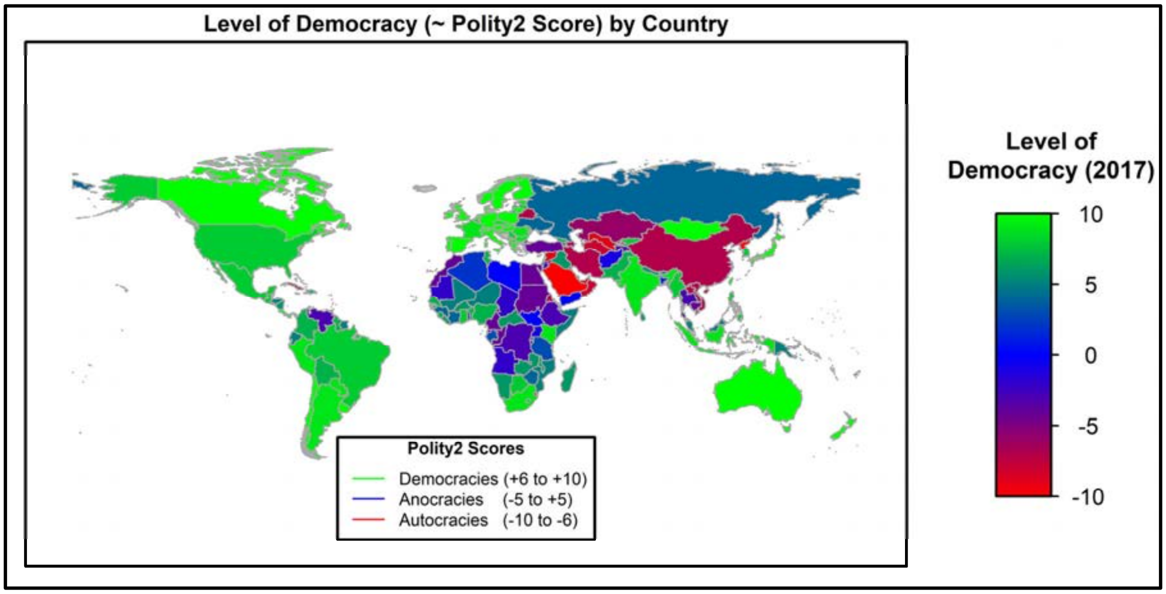


Figure 2. World Map Depicting Levels of Democracy by Color.

This activity provides the anocratic or autocratic leader with wide rhetorical space in which to operate, while *verbally* scuffling with the U.S. As the elites' signal to the population to decrease their activities, the level-one discussion remains verbal, leading to a conjectured *decrease* in intrusion activity. However, once this verbal tussling comes to an end and the *material* outcome becomes a reality, elites telegraph to the populace that they may resume or increase their activities to include network intrusions. Both causal inferences are the focus of this research. This is not to suggest that these are the only effects. Nor does the posited process necessarily proceed in the discrete order in which it is described here, beyond the *verbal* or *material* signaling leading to *decreased* or *increased* intrusion activity, respectively.

The transition from *verbal* rhetoric to *material* action may occur in several different ways, particularly when the narrative remains negative because the opposing side of the dyad, dispensing the conflictual rhetoric, did not achieve the change of U.S. policy originally sought. This leads to the media reporting physically real *material* events, either by the *verbal* bantering devolving into a negative *material* result or by simply escalating from *verbal* to *material* interactions between these states and the U.S. Alternatively, the media reported narratives could flow from material to verbal, as well.

Democracies on the other hand, may manifest the opposite effect, perhaps because they exercise very little societal control over the digital medium beyond the illegal (Goodman, 2015). Control of the media and internet modalities within democracies resides mostly in the private sector (Goodman, 2015; MacKinnon, 2012; Morozov, 2011). Beyond the threshold of clearly unlawful acts as defined by a democracy's laws, control of the media and internet is largely driven by a profit motive (Chesterman, 2011; Freedom House, 2017; Goodman, 2015; MacKinnon, 2012; McHugh & Ramirez, 2018; Morozov, 2011; Shahin & Zheng, 2020). Further, the elites within a democratic civil society span many different points of view on a given subject (Best & Higley, 2018; Higley & Burton, 2006). In democracies, while the two-level process may exist, it is far from consistent, controlled, or discrete (Putnam, 1988). Contrary to other regime types, democracies produce a multiplicity of level-two narratives that their leadership can only manage at best and may, on rare occasion, appear to control (Best & Higley, 2018; Bjola & Manor, 2018, Conceição-Heldt & Mello, 2017; Higley & Burton, 2006; Putnam, 1988; Strong, 2017; Trumbore, Boyer, Gibson, Harvey, & Wilkenfeld, 2000). As such, in democracies as the dyadic tone becomes increasingly negative for both *material* and *verbal* narratives, it would be expected that intrusion attempts will increase.

C. RESEARCH DESIGN

The final hypotheses, offered at the end of the literature review, will be tested using data derived from a representative U.S. Government server that provided cyber intrusion information in two date ranges. The first spans from 02 January 2015 to 06 May 2015 (~ 124 days) and the second from 12 September 2016 to 18 March 2017 (~ 178 days). The data sources will remain anonymous per their request. Data derived from intrusion detection software provided the means to assess the hacktivist or intrusion activity on a given network. The SNORT intrusion detection software (IDS) will be used to gather the intrusion activity data from servers running within these anonymous sources (Beale, Foster, Posluns, & Caswell, 2003; Cavusoglu, Mishra, & Raghunathan, 2005; Rehman, 2003). First, the researcher created an intrusion activity response variable by aggregating the intrusion data to derive a per country, per day or *country-day* variable. Per country-day will be the unit of analysis used throughout this research. Second, this data does not possess the level of fidelity necessary to discern specifically what trigger or catalyst (i.e., elite, social movement, or state-sponsored organization) led the hacktivist or group to intrude. Nor does it provide the capability to distinguish between hacktivists mobilized by elites, social movements, or government-sponsored groups.

Next, dyadic events data will be utilized to create a set of independent variables in the same unit of analysis, drawn from the Phoenix Data Project. The Phoenix Data Project establishes a set of nominal and ordinal codes from 386 worldwide, English language, international, local, and wire media news sources generating news articles on a daily basis. These scraped articles are coded and stored in electronically queryable databases (Goldstein, 1992; Howell, 1983; Schrodt P. A., 2012). Each line in the events coding data provides nominal dyad information between two countries and an ordinal score, the *Goldstein score*, ranging from cooperation +10 to conflict –10. This *media events data* is an electronic record of the dyadic narratives between international actors as reported by open media sources and electronically scraped from the given news outlet (Caerus, 2015; Schrodt P. A., 2012). As the use of [*media*] *events data* has become increasingly reliable, researchers have begun to use it to measure the level of cooperation or conflict between states (Bi, 2015; Colaresi, 2004; Goldstein, 1992; Goldstein & Pevehouse, 1997; Monroe & Schrodt, 2008; Monroe, Pan, Roberts, Sen & et al., 2015; Schrodt & Gerner, 1997). Further, the *Goldstein score* within the media events data closely estimates the level of *tone* of on-going narratives, as reported by open source media, describing the tenor of discourse or dialogue between sovereign states.

In addition to gauging the tone of narratives, the event coders delineate the narratives as either verbal or material, cooperative or conflictual in content.[17] Verbal narratives might include political rhetoric, verbal posturing, or political dialog. Essentially, a country's leadership may use these verbal narratives to telegraph potential threats, coerce, or cajole their opponents in the dyadic dialogue to come around to a position favorable to their country. Whereas, material narratives describe events characterized by physical acts (massing forces on another nation's borders, providing aid, conducting armed attacks, etc.).

Human event coders established rules to parse these verbal and material / cooperative and conflictual narratives into typological quadrants that will be useful in creating per country day count independent variables. Thus, the research uses the Conflict and Mediation Events Observations (CAMEO), two-digit, media event root codes, as shown in Table 1, as an indication of the characterization of the types of narratives about the U.S. used by other countries. There are 20 ordinal codes in the CAMEO construct using the terminology of the scraped article to categorize each narrative into *actor-action-actor* characterizations, within the bounded range from cooperative to conflictual (Caerus, 2015, pp. 3–4; Schrodt P. A., 2017). For example, the code for *engage in diplomatic cooperation* is 05 while *reduce relations* is 16, as depicted in the first and second columns of Table 1 (Schrodt P. A., 2012, pp. 131–138). The CAMEO defined actor-action-actor construct sorts the content of the media articles into cooperative-coded events 01–05 for verbal events and 06–09 for material events shown in black (i.e., cooperative or positive) in Table 1, with the conflictual or negative event codes depicted below them in red 10–14 describing verbal events while 15–20 define material events (Schrodt P. A., 2012, p. 3). Since each scraped

[17] Verbal Cooperative (Positive) – narratives describing dialog-based meeting, such as negotiations or peace talks or statements that express a desire to cooperate or appeal for assistance (other than material aid) for other states (Schrodt P. A., 2017, p. 20).

Verbal Conflictual (Negative) – a spoken criticism, threat, or accusation, innately rhetorical and normally related to past or future potential acts of conflict (Schrodt P. A., 2017, p. 20).

Material Cooperative (Positive) – physical acts of collaboration or assistance, including receiving or sending aid, reduce bans, reduce sanctions, etc (Schrodt P. A., 2017, p. 20).

Material Conflictual (Negative) – physical acts of a conflictual nature, including armed attacks, destruction of property, assassination, embargos, naval blockades, etc (Schrodt P. A., 2017, p. 20).

media narrative fits into one of the four quadrants of the typology, per country-day count variables will be easy to derive.

Finally, the daily *tone* variation (i.e., standard deviation) can be derived from these scraped narratives to determine the level of media polarization on a given day. Thus, a calculated media polarization variable could discern how increasing or decreasing divergence in daily media narratives impacts intrusions.

The focus of this research will cover the extent to which negative material and verbal narratives, tone and variation *today* affect intrusions on U.S. networks *tomorrow*; however, the development of the statistical model will require applying it to all-narratives (i.e., positive or negative / cooperative or conflictual) first. This application of the model to all-narratives will assist in testing the validity and reliability before proceeding to the negative narratives research. Further, the initial model will need to be exposed to multiple theoretical distribution types (i.e., Gaussian ~ normal, Poisson, negative binomial, and geometric) to discern which distributions best fit the observed data. Thus, the macro model will assist us in deciding which theoretical distribution fits best and provides the most illuminating output to enable the understanding of the theorized relationships.

Table 1. Cameo Media Event Root Codes. Adapted from Caerus (2015).

Media Event Root Code	**Description**
01	Make a Public Statement
02	Appeal
03	Express Intent to Cooperate
04	Consult (with dyad partner)
05	Engage in Diplomatic Cooperation
06	Engage in Material Cooperation
07	Provide Aid
08	Yield
09	Investigate
10	**Demand**
11	**Disapprove**
12	**Reject**
13	**Threaten**
14	**Protest**
15	**Exhibit Force Posture**
16	**Reduce Relations**
17	**Coerce**
18	**Assault**
19	**Fight**
20	**Use of Unconventional Mass Violence**

Once chosen, this initial model and statistical distribution structure, will be used to focus the model on the effects of negative narratives across all regime-types. This model will form the basis for the negative narratives research used throughout the remainder of this dissertation. Next, the analysis will examine the model to differentiate between the effects on regime-types (e.g., democracies, anocracies, and autocracies) before turning to focus on explicit countries falling within their type designations..[18] The research will

[18] *Anocracy* is defined as a form of government that is neither a full democracy nor an autocracy; often times referred to as a mixed democracy or hybrid regime (Marshall & Cole, 2014, p. 21).

Autocracy is a form of government where a citizens' participation is severely curtailed, restricted, or suppressed; chief executives are selected according to clearly defined (usually hereditary) rules of succession from within the established political elites; and, once in office, chief executives exercise power over the executive, legislative, and judicial branches of government, most of civil society (Marshall & Cole, 2014, pp. 20-21).

proceed as discussed here, as described in Table 2 and as described in detail in Chapter III, Model Design: Media Effects in Cyberspace.

Table 2. Research Design Steps

Research Step	Short Description
1	Develop a macro statistical model to test the effects of all-narrative types on subsequent levels of intrusions.
2	Test the macro model across multiple theoretical distribution types to discern which best fits the data and provides the most illustrative output describing the relationship between the media narrative – *yesterday* generated by other countries about the U.S. and intrusions on U.S. networks—*today*.
3	Focus the model chosen on *negative* narratives, about the U.S., originating from first all democracies, then anocracies, and then autocracies to test the hypotheses.
4	Focus the model on negative narratives, about the U.S., originating from these regime types and compare the results to a set of autocratic, anocratic, and democratic countries, using a case study format, to test if proffered hypotheses hold for the examined countries within each type.

D. DISSERTATION ORGANIZATION

This introduction began with a description of the cyber intrusion phenomenon, delved into the theoretical underpinnings of what may drive this behavior, and concluded with the intent to incorporate the various data and its sources into the research design to test the hypotheses that will be offered at the end of the literature review chapter. Subsequently, the following chapter will introduce the design of the quantitative (i.e., statistical regression) model in much greater detail and discuss the results derived from the macro regression model. Then, the chapter will present the All-Regime narratives regression model, followed by the different regime types and explore how stories, originating from other sovereign states, about the U.S. published *today* effect cyber intrusions on U.S. networks *tomorrow*. Next, in the case study chapters will aim to explore how the model responds to the shifting contexts of different regime types, and then down to particular countries. Across these levels of analysis, the evidence consistently shows that media narratives originating from other states about the U.S. generate substantial impacts on the succeeding levels of cyber intrusions observed on U.S. networks. Ultimately, the dissertation will wrap up with conclusions and recommendations for further research in this area.

THIS PAGE INTENTIONALLY LEFT BLANK

II. LITERATURE REVIEW

A. INTRODUCTION

This review will begin by surveying the literature to provide context for, assist in refining the explanation of, and focus this research covering the implied relationship between media events and cyber intrusions. First, a brief discussion of the cyber intrusion phenomenon provides clarification of why this is an important area of study, describes a cyber narrative, and defines the layers of the internet. Second, the review seeks to explore the theories underpinning international conflict and rivalry, including the development of a typology to describe cyber-intrusion behavior and its motivations. Third, the review will survey the *two-level* theory of international relations covering its linkages to state elites and media outlets and how it functions across different regime types. Fourth, the author will describe the theoretical placement of the *two-step flow* theory of communication inside of the two-level model and the applicability of this integrated construct across multiple regime types, which will assist in explaining the theoretical relationship between media events and cyber intrusions. This review will then address the media events data community and how these scraped, scored, and categorized media narratives provide a rich data set for use in developing a quantitative model to describe how media narratives on a given day may affect cyber intrusions on the following day. Next, the review will cover aspects of digital panopticon, narrative, and sharp power, teasing out certain elements that will buttress the explanation of the research. Finally, this chapter will discuss how the research intends to derive observable implications from the available data, ending with the proffering of hypotheses to test through the use of the developed model.

B. CYBER INTRUSION PHENOMENON

Media reports describing cyber intrusions—most often referred to in the ongoing media narrative as *Cyber Attacks*—seem to proliferate daily (Andriotis & Minaya, 2017; BBC, 2017; Kroft, 2015; Gandhi, et al., 2011; Koh, 2012; Kugler, 2009; Mims, 2017; Owens, Dam, & Lin, 2009; Paletta & Yadron, 2015; Stavridis, 2015). Over the past decade, the number of notable attacks, breaches, or intrusions seem to have increased exponentially from the Sony Online Entertainment in 2011 and the Sony Pictures Entertainment in 2014 to Equifax and WannaCry in 2017, to the Solar Winds hack of 2021. *Cyber Attacks*, or more precisely intrusions, appear to be growing in frequency and cost.[19] Further, as each individuals' connection to the internet becomes a perceived human necessity, the term *cyber-attack* takes on a meaning that both misleads the public and creates a fear of some exogenous menace, which seems too often be misplaced (Deibert R. J., 2013; Goodman, 2015; Lindsay, 2013; MacKinnon, 2012; Maness & Valeriano, 2016; Morozov, 2011; Rid, 2012; Valeriano & Maness, 2015).

Further, the ongoing narrative does not help. The media's use of the term cyber-attack, however ill-defined, has been adopted as the term of reference to describe any type of cyber event. The media comes by this naturally, they are simply trying to tell a story that

[19] The spear phishing intrusion at *Sony Online Entertainment* in 2011 compromised over 77 million consumer accounts in the company's PlayStation network, which constituted the largest data breach at the time and cost Sony over $171 million (M) to contain the breach (Hoffman, 2011; Richwine, 2014). Subsequently, *Sony Pictures Entertainment* was hacked again in 2014. U.S. Cyber Officials attributed the hack to North Korea, although they emphatically denied responsibility (Carter, 2015). To contain the 2014 intrusion, Sony had to completely disconnect from the internet, forcing their over 6000 employees to communicate the old-fashion way via land line telephone or hand delivered message, until the magnitude of the *cyber-attack* was contained (Kroft, 2015; Paletta D. , 2015). Sony lost over 3,000 computers and 800 servers, and all of the intellectual capital that was ex-filtrated out of their network before their hardware was damaged or *destroyed* – as described in the media narrative (Carter, 2015; Kroft, 2015).

A group, known as "Guardians of Peace," orchestrated the 2014 cyber intrusion (Whyte, 2016). Subsequently, an investigative team from Sony in cooperation with the U.S. Federal Bureau of Investigation (FBI) discovered the "Guardians" operated out of North Korea. Apparently, the intrusion was an attempt by North Korea to coerce Sony Pictures into halting the release of the *The Interview* a movie that depicted the assassination of Kim Jong-Un, the Supreme Leader of North Korea by a trio of popular comedians (Sharp, 2017; Whyte, 2016).

The initial estimated cost of the 2014 Sony Pictures intrusion was close to $100M, later revised to $35M (Hornyak, 2015; Kroft, 2015; Richwine, 2014). This figure is less than the 2011 breach because this hack was focused on their internal employees and not the records of their customers – the former, as discussed earlier, was much more expensive (Paletta D. , 2015; Richwine, 2014). Interesting how the $100 million in lost content and in *destroyed* IT equipment received wide media exposure; however, when Sony Picture revised the estimated loss to $35M and described the loss as immaterial – the media did not seem interested providing only meagre coverage (Hornyak, 2015). Nevertheless, from that point, the state of North Korea began to refine its tactics.

The *Equifax* data breach, hackers exfiltrated over 143 million records containing Americans' personal and financial information (i.e., name, address, Social Security number, and date of birth) (Andriotis, Rapoport, & McMillian, 2017).

In May 2017, the *WannaCry* ransomware virus spread throughout the world (Harris, 2017; Rivero, 2017). The ransomware infected information systems by initially locking users out of their computers and then demanding a payment in BitCoin, an electronic digital currency, to unlock the computer.[19] *WannaCry* operated in two stages one to infect, the other to spread the infection across other information systems, hitting Russia and China the hardest with 24,000+ and 15,000+ respectively (Rivero, 2017).

adds a bit of flair to the bland zeros and ones of cyberspace. These would be cyber reporters cast their stories (i.e., narratives) as possessing verisimilitude or the appearance of truth, whereas, the authors of these tales may only possess a modest degree of understanding on the subject.

The media attempts to create a narrative around the experience of others, in what narrative theorists call a descriptive structure to make sense of a cyber event (Barbatsis, 2004). But, Barbatsis (2004) offers a caution, by quoting narrative theory scholars, that narrative's descriptive structure merely reflects real-world events and does *not* record them.[20] In their defense, these media outlets using cyber narratives are attempting to describe incredibly complex cyber incidents, reducing them to narratives that allow the average person to make sense of and understand the story. If these narrators follow the time-honored media refrain, if it bleeds, it leads, they label these cyber events as attacks, which implies someone is bound to bleed as a result (Arango-Kure, Garz, & Rott, 2014; Miller & Albert 2015; Sherry, 2004; Shoemaker & Reese, 1996;). These cyber narratives create fascinating stories around what are frequently banal cyber incidents, structurally transforming them into the far more compelling and dramatic cyber-attack.

1. Cyber Attacks: The Narrative

Thus, the term *cyber-attack* feeds into this already electric atmosphere, conflating the meaning of it with *all* lesser cyber intrusions or incidents (BBC, 2017; Kroft, 2015; Czosseck, Ottis, & Taliharm, 2013; FireEye, M-Trends, 2016; Gandhi, et al., 2011; Harris, 2017; Stavridis, 2015; Valeriano & Maness, 2015). Some scholars liken cyberspace to the land, sea, air, and space (i.e., physical) domains, which are, at best, imprecise analogies for this man-made, synthetic domain (Arquilla & Ronfeldt, 1993; Clarke & Knake, 2010; Clarke & Knake, 2019; Lynn III, 2010; Valeriano & Maness, 2015; Valeriano, Jensen, &

[20] Narrative Theory – a. the institutionalized use of semiotic structures or codes to allow narrators (i.e., authors), and readers to communicate through texts; thereby, allowing the reader to understand and make sense of a given situation described in the story (Barbatsis, 2004; Kearns, 2005). b. information that actively engages the senses using language to create structure that draws in the reader or listener, intentionally, leaving out pieces of information, or the other side of the story, in an effort to engage the reader or listener by inviting them to us their imagination to fill in the missing information and discern what really happened (Wake, 2009, p. 674).

Maness, 2018). The media narrative and the scholarly conjectures meld together to create the impression that Cyber Attacks and their effects parallel those seen in the terrestrial world.

By the definition herein, *Cyber Attacks* must cause physical harm to persons or destroy systems, see page 1 or Appendix A (Schmitt, 2013, p. 106). While these incidents may have caused financial harm to the targets causing physical damage to objects of these media labeled *attacks*, none to date cross the threshold meeting *all* aspects (i.e., injury or death to a person) of the *cyber-attack* definition used in this research. Thus, the number of actual documented *Cyber Attacks* causing physical harm to human beings has *not* occurred as of yet, despite the relentless media and scholarly hyperbole predicting its imminent occurrence (BBC, 2017; Goodman, 2015; Lindsay, 2013; Maness & Valeriano, 2016; Rid, 2012; Valeriano & Maness, 2014; Valeriano & Maness, 2015).[21] For instance, while

[21] Four of the foremost, documented, examples of cyber-attacks on the physical layer via the syntactic substrate by a state or non-state actor include Bronze Soldier (Estonia 2007), Stuxnet (Iran 2009-2010), Shamoon-Saudi Aramco Corporation (Saudi Arabia 2012), and Sony Pictures Entertainment (US 2014). While surveying each of these cyber-attacks lies well beyond the scope of this research, we need to clarity to the level of damage or destruction caused by these attacks.

First, none of these *cyber-attacks*, as we have defined them, caused physical injury or death to any human beings, as stated earlier (Goodman, 2015; Lindsay, 2013; Maness & Valeriano, 2016; Rid, 2012; Valeriano & Maness, 2014; Valeriano & Maness, 2015). In only one case, *Stuxnet*, some do suggest, at least anecdotally, that physical damage and/or destruction of objects did occur (i.e., computers, servers, routers, IT Systems, centrifuges) may have occurred (Goodman, 2015; Lindsay, 2013; McGraw, 2013; Maness & Valeriano, 2016; Rid, 2012; Valeriano & Maness, 2014; Valeriano & Maness, 2015). However, in this *Stuxnet* case, recent evidence points to damage, but *destruction* of the centrifuges remains a conjecture (Gartzke & Lindsay, 2015; Lindsay, 2013; Rid, 2012; Sanger, 2012; Valeriano & Maness, 2015).

Second, two of the four, Bronze Soldier and *Stuxnet*, were state on state cyber incidents, with the other two, Shamoon and Sony Pictures, being state on non-state (Carter, 2015; Choo, 2011; Goodman, 2015; Lindsay, 2013; Maness & Valeriano, 2016; Paletta D. , 2015; Rid, 2012; Valeriano & Maness, 2015). Thus, these cyber incidents can and do transcend territorial and geographic boundaries with little regard for state sovereignty, borders, or governance (Choucri, 2012; Clarke & Knake, Cyberwar, 2010; Gartzke & Lindsay, Weaving Tangled Webs: Offense, Defense, and Deception in Cyberspace, 2015; Lindsay J. , Stuxnet and the Limits of Cyber Warfare, 2013; Nye J. S., 2011; Rid, 2012; Valeriano & Maness, 2015; Whyte, 2016). Further, these incidences can come from state or non-state actors (Maness & Valeriano, 2016; Nye J. S., 2011; Valeriano & Maness, 2014; Valeriano & Maness, 2015; Whyte, 2016).

Maness and Valeriano (2016) provide empirical evidence that cyber incidents have occurred, they carefully avoid referring to them as *Cyber Attacks*.[22] The type of research done by these and other authors tend to refute much of the apocryphal *cyber-attack* theoretic terminology proffered by some scholars and media sources (Gartzke & Lindsay, 2015; Lindsay, 2013; Maness & Valeriano, 2016; Rid, 2012; Valeriano & Maness, 2014; Valeriano & Maness, 2015). Therefore, at this point in time, only the *damage to objects* portion of our *cyber-attack* definitions holds up to the scrutiny of empirical research.

2. Cyber Attacks: The Narrative's Effect

Certainly, the wanton fear of the unknown in cyberspace appears to infect the public, the elites, the politicians, and the media with a quasi-phobic viewpoint-colonizing each individual's lifeworld, driven by the imprecise terminology consistent in today's

Finally, in all cases, the target of the *cyber-attack* incurred financial costs due to loss of reputation or due to the damage and subsequent repair of infected systems. Thus, when *cyber-attacks* occur, and they do, targeted state or non-state actors have incurred in the past and will incur in the future economic costs associated with the incident (Goodman, 2015; Gartzke & Lindsay, Weaving Tangled Webs: Offense, Defense, and Deception in Cyberspace, 2015; Kroft, 2015; Lindsay J. , Stuxnet and the Limits of Cyber Warfare, 2013; Maness & Valeriano, 2016; Nye J. S., 2011; Rid, 2012; Singer & Friedman, 2013; Valeriano & Maness, 2015). Still, to reiterate – no quantifiable evidence exists that a *cyber-attack* caused physical harm, death, or injury to human being nor evidence of actual *destruction* of an object, computer, server, router, or IT system. Certainly, *cyber-attacks* have caused economic harm to individuals or their organizations and damage to IT systems.

Yet, while the initial media reports described these cyber incidents as massive or colossal in scope, the long-term observable results do not. Estonia remains one of the most cyber-connected countries in the world, hosts the North Atlantic Treaty Organization's (NATO), Cooperative Cyber Defense Center of Excellence in Tallinn, and hosts the annual International Cyber Conflict Conference (CyCon) (Clarke & Knake, 2010; Valeriano & Maness, 2015). Iran continues to develop its nuclear capability; in fact, the Stuxnet incident may have strengthened their resolve (Valeriano & Maness, 2015). Saudi Aramco remains the world's largest energy producer, generating daily revenues of over $1B per day and an estimated net worth of $2T (Gregory, 2017; Valeriano & Maness, 2015). Sony Pictures continues to churn out new movies, with an estimated net worth of $30B in 2017, equivalent to 857 times greater than the 2014 estimated loss of $35M (Hornyak, 2015; Lee, 2017).[21] A loss described by Sony Pictures as not material to its overall financial results for the year ending March 2015 (Hornyak, 2015). However, since no incidence of injury or death to a person or destruction of an object has transpired to date, points to a deep flaw in the scholarship surrounding the qualitative cyber-attack inference.

[22] Cyber Incident – a. an occurrence or set of occurrences that result in an actual or potentially adverse effect on an information system, network, and/or the information residing therein (Committee on National Security Systems, 2015, p. 40). b. an individual action or cyber-operation launched against a state, by another state or non-state actor as part of an ongoing cyber dispute or conflict (Valeriano & Maness, 2014, p. 349; Valeriano & Maness, 2015).

cyber narrative.[23] A quick Google News query of the word, *cyber-attack*, returns over 11M results in a little under half a second. So, regardless of whether an individual appreciates the media's use of imprecise language to describe these cyberspace events, better described as intrusions or even incidents, this lexicon has crept into society's collective cyber reality creating an uninformed fear of some exogenous threat.

This palpable fear, across civil society, leads many policy makers to rely on the advice of private sector cybersecurity companies to attain, gain, or maintain their cyberspace capabilities in defense of their national interests (Valeriano & Maness, 2015).[24] Thus, the general lack of cyber fluency, the imprecise use of cyber terms—particularly in media narratives, the scholarly comparison of cyberspace to other conflictual domains, and the growing commercial interests in cybersecurity fuse together to create a distorted, apocryphal representation of cyberspace threats (Clarke & Knake, 2010; Singer & Friedman, 2013; Valeriano & Maness, 2015). The basis of this fear comes from the lack of cyber fluency within civil society in general.

More precisely, civil society lacks a deep knowledge of the internet and how it works. Coupled with the daily media *cyber-attack* narrative, colonizing what Jürgen Habermas (1987) would describe as an individual's *lifeworld*, this causes many to internalize their fears of what might happen to them, their family, or their country due to these seemingly relentless *Cyber Attacks (Valeriano & Maness, 2015)*. Yet, existing research has only unearthed implied damage or destruction of objects. Cyber-attack as defined in this volume falls well short of the deadly or destructive connotations the word

[23] Lifeworld – best describes a human's socially constructed reality, where the individual hears from and speaks to the world around them, interacting with their day-to-day world system. Habermas (1987) clarifies that a person's communications (i.e., speaking and hearing) in the modern world system is semantically laced with propositional, illocutionary, and expressive components that in effect can do harm or "violence" to a person's lifeworld; thereby, constraining clear communication and hampering the ability to achieve societal consensus on given issues. This harm or violence to the lifeworld of individuals causes pathologies and crises that lead to serious social problems (Habermas, 1987; Ryan, 2005).

[24] The private sector can provide us with evidence of the magnitude of this growing societal trend, according to Steve Morgan – a well-known cyber expert, investors pumped $3.5B into cybersecurity start-up companies in 2016 (Morgan, 2016; OilPrice.com, 2017). Morgan estimates that by 2020 that number will increase to $170B (Morgan, 2016; OilPrice.com, 2017). A whopping 4857% percent increase over the next four years. Or $170B divided by $3.5B equals 48.571, which if multiplied by 100% that equals 4857%.

attack enjoys in the non-synthetic land, sea, and air domains. Thus, the author chooses to defenestrate the imprecise term *cyber-attack* once and for all, in favor of cyber intrusion, which more precisely describes the topic. Next, a review of the internet's origins, how it works, and an introduction to some key terms, will provide the conversant knowledge of cyberspace necessary for use in this ongoing discussion.

3. Internet: The Evolution

The internet, cyberspace, or Worldwide Web (WWW) of today began as a research project, in the mid-1960s, executed by a U.S. government agency known as the Advance Research Projects Agency (ARPA) (Barabasi, 2003). Originally, the ARPA net project envisioned the connection of scientific researchers and academicians by interlinking their computers, as a means through which these intellectuals could collaborate and share information. Eventually, the network became more sophisticated leveraging emerging technology connecting computers to optical cables, servers, and routers causing information between these individuals to move even faster.[25] From that point, the ARPA net began to grow at a rapid pace. Eventually growing into the internet. In 1989, the invention of web pages, and their incumbent commercial applications, enabled the internet to grow into today's WWW. Nevertheless, even with its exponential growth, the WWW's protocols and design management remained under the purview of the U.S. National Science Foundation (NSF) (Barabasi, 2003, pp. 143–148).

In early 1995, NSF relinquished control of the internet, as it continued to grow exponentially, ultimately, expanding globally and across the private sector. Over the intervening years, a set of international committees coalesced around the a US–based, international, non-profit corporation, Internet Corporation for Assigned Names and Numbers (ICANN), which now sells domain names, promulgates policy standards, and nominally manages data routing across internet's system of systems (Barabasi, 2003; ICANN, 2018; Nye, 2014; Shackelford, 2012). At best, ICANN and this coterie of committees provide stewardship and the collection of policies that keep the WWW

[25] Router – a device that mediates the transmission routes of data packets over an electronic communications network (i.e., the Internet) (Webster, 2017, sec. "router").

functioning; however, the realization of an effective governance structure for this new domain remains illusive (Barabasi, 2003; ICANN, 2018; Nye, 2014; Shackelford, 2012).

Today, cyberspace has emerged as a collective of servers owned by multinational corporations and governments connected together by routers and optical cables that reside in states across the globe and serve as a backbone for information transported across the internet (Barabasi, 2003). Technically, any state or non-state actor with a computer and access to an internet connection may use this domain for their own purposes. For example, a person or group could use the internet to communicate or coordinate efforts, to conduct business, to collect information or gain knowledge, to conduct acts of malice or subversion, to hack into an unwitting server, etc. (Rid, 2012; Valeriano & Manness, 2015). Essentially, the internet is a quasi-governed, borderless domain that spans the globe (Choucri, 2012; Goldsmith & Wu, 2006). Any internet user, who places any of their information on the WWW; ostensibly, has placed it there for all the world to see (Goodman, 2015).

4. Internet: The Layers

Current theory breaks the internet down into discrete layers: the physical and the synthetic, with the later broken down into the syntactic and the semantic substrates (Libicki, 2007). These substrates describe and comprise the multiple layers that operate together and allow the internet to function (Choucri, 2012; Clarke & Knake, 2010; Libicki, 2007; Valeriano & Maness, 2015).[26] The physical layer, the backbone of the internet, contains all of the manifold computers, routers, servers, technical control devices, telecommunications controllers, and IT systems that allow the internet to operate (Choucri,

[26] Clark and Knake (2010) stratified cyberspace into the physical, logical, informational, and actor layers. Choucri (2012) chose to follow this construct. Libicki (2007) broke the layers of the internet into the physical, syntactic, and semantic. Libicki's stratification of cyberspace collapses Clarke and Knake's logical and informational stratum into the synthetic using more precise language by using syntactic (i.e., logical) and semantic (i.e., informational) substrata. Valeriano and Maness (2015) seem to adopt Libicki's construct, which will be used throughout this volume.

2012; Clarke & Knake, 2010; Comer, 2015; Libicki, 2007, p. 8; Valeriano & Maness, 2015).[27]

The *synthetic* layers consist of the *syntactic* and *semantic* substrates, as Libicki (2007) described. The computer language, instructions, and syntax reside within the *syntactic* substrate, which enables the internet to function, as the operator intends (Libicki, 2007, pp. 1–14).[28] The *syntactic* substrate provides access to the *semantic* layer, where the information and knowledge, created by humans, resides in cyberspace (Choucri, 2012; Clarke & Knake, 2010; Libicki, 2007; Valeriano & Maness, 2015).[29] The *syntactic* layer provides the medium to access the physical layer. *Cyber-intrusions* come through this substrate. Thus, to hack or to intrude into a network entails the use of the physical layer to gain access to the *synthetic* layer through the manipulation of the *syntactic* to access, damage, or exfiltrate the information residing in the *semantic* substrate (Choucri, 2012; Clarke & Knake, 2010; Libicki, 2007; Valeriano & Maness, 2015). Any cyber intrusion would proceed in this manner. Yet, attribution of these intrusions remains elusive due to the ubiquitous use of Internet protocol (IP) anonymizers and other surreptitious methods not discussed here.

[27] Information Technology (IT) Systems – Includes all categories of ubiquitous technology used for the gathering, storing, transmitting, retrieving, or processing of information (e.g., microelectronics, printed circuit boards, computing systems, software, signal processors, mobile telephony, satellite communications, and networks). Synonymous with Information and Communications Technology (Committee on National Security Systems, 2015, p. 62).

Further, using the International Organization for Standardization (ISO) internet 7-layer reference, in this context the physical layer would incorporate ISO layers 1 through 4 (i.e. 1. Physical, 2. Data Link, 3. Network, and 4. Transport) (Comer D. , 2015). Comer (2015) points out that modern protocols may not fit into this structure; yet, the use of the ISO layering terminology persists, largely for descriptive purposes.

[28] Using the ISO layering protocol this syntactic layer would encompass layer 5 and 7 (i.e., 5. Session (login in procedures) and 7. Application) (Comer D. , 2015).

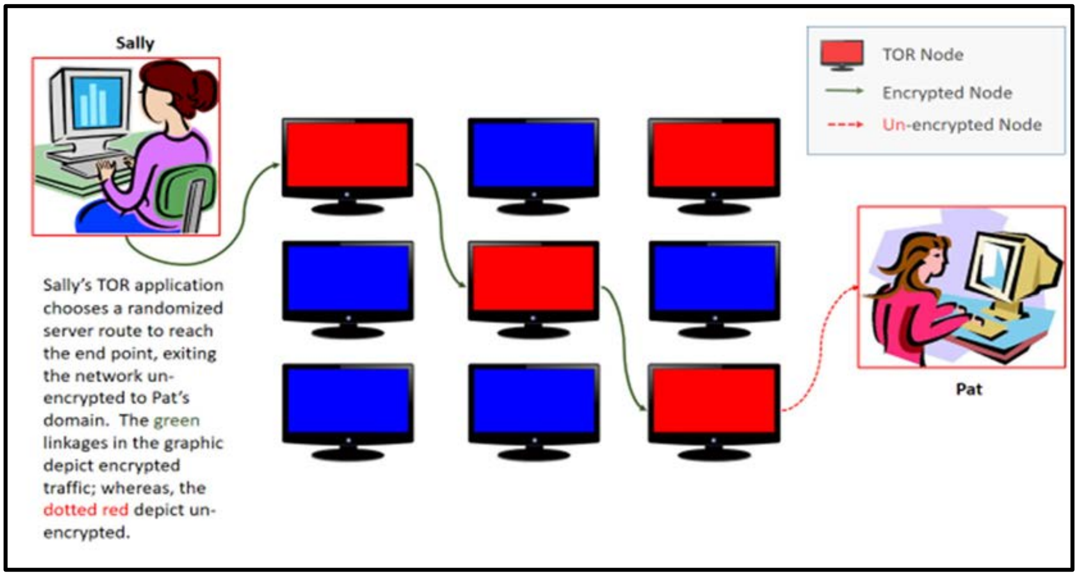
[29] Syntactic substrate – a substratum of the synthetic layer that contains the computer language, instructions, and syntax, which enables the internet to function. The physical layer, of cyberspace, enables access to the semantic substrate, through the syntactic substrate where the hacking occurs to gain access to the information in the semantic (Libicki, 2007, pp. 8-10; Valeriano & Maness, 2015, pp. 22-24).

Semantic substrate – a substratum of the synthetic layer that contains the information and knowledge created, manipulated, and utilized by humans in our day-to-day life. Access to this substrate comes through the physical through the syntactic. Information that is exfiltrated, manipulated, or stolen resides in the semantic substrate (Libicki, 2007, pp. 8-10; Valeriano & Maness, 2015, pp. 22-24).

Using the ISO Layering Protocol this semantic layer would be synonymous with Layer 6 (i.e., 6. Presentation) (Comer D. , 2015).

5. Internet: The Anonymity

IP anonymizers, such as The Onion Router (TOR), a common freeware application, essentially encrypt the user’s network traffic from point of origin until exiting the anonymizer network of servers.[30] As shown in Figure 3, it is not until the last link to the final destination that information proceeds *un*-encrypted. This makes attribution of the intrusion’s origin, as in the examples below, exceedingly difficult for individuals, but possible by leveraging government or state-level resources.



Sally’s TOR application chooses a randomized server route to reach the end point, exiting the network un-encrypted to Pat’s domain. The green linkages in the graphic depict encrypted traffic; whereas, the dotted red depict un-encrypted.

Figure 3. The Onion Router (TOR) Encryption Process.

[30] Internet Protocol (IP) – Standard protocol for transmission of data from source to destinations in packet-switched communications networks and interconnected systems of such networks (Committee on National Security Systems, 2015, p. 70).

Freeware – (a.k.a. Public Domain Software) Software not protected by copyright laws of any nation that may be freely used without permission of or payment to the creator, and that carries no warranties from or liabilities to the creator (Committee on National Security Systems, 2015, p. 99).

Thus, using an IP anonymizer, like TOR, an internet user or would-be hacker gains a certain amount of anonymity when using the internet. Indeed, intrusions and hacks have become an instrument of statecraft to use in conflict or rivalry situations between states or non-state actors (i.e., Sony Pictures) (Arquilla & Ronfeldt, 1993; Choo, 2011; Denning, 2007; Gandhi et al., 2011; Harris, 2008; Maness & Valeriano, 2016; Murphy, 2014; Shackelford, 2012). In reality, most of this cyber activity seems to fall into the realm of a low-level cyber incidence at best or more appropriately as cyber intrusions. In this way, cyberspace is both similar and different from the other conflictual domains, where crime, coercion, espionage, and sabotage (i.e., with the intent to damage only) do occur, frequently. As such, it is prudent to explore the existing literature surveying the extent to which conflict and rivalry between any manifold combination of state or non-state actors unfolds in the internet domain. So, what does conflict and rivalry look like in cyberspace?

C. INTERNATIONAL CONFLICT AND RIVALRY

Since humans began to make historical records, the state has acted as a system around which groups of people organized. Granted the state concept was nascent at first but grew in its importance over time. The Treaty of Westphalia (1648), which ended the Thirty Years' War in Europe, set the foundational cornerstone establishing the territorial sovereignty of the state as the premier form of organization in the international system and its concomitant elite underpinnings (Bull, 2012, p. 39; Higley & Burton, 2006, p. 24; Nye J. S., 2007, p. 3). People throughout the world have and continue to organize around the state paradigm.[31]

The state construct has led to much conflict and rivalry over the centuries in the various domains expanding from the land and sea to air and space in the most recent era. The rivalry normally revolves around competition for resources, frequently territorial with pre-existent cultural, ethnic, or religious overtones contributing to the contentious atmosphere (Diehl & Goertz, 2001; Klein, Goertz, & Diehl, 2006; Thompson, 2001;

[31] Presently, there are approximately 196 sovereign states in the World (Polity IV, 2018).

Vasquez & Leskiw, 2001).[32] In some cases, over time, these rivalries lead to conflicts ranging from simple disagreements with cyber overtones, to arms races, to armed skirmishes, and even to all-out war (Diehl & Goertz, 2001; Klein, Goertz, & Diehl, 2006; Maoz & San-Akca, 2012; Toft, 2014; Thompson, 2001; Valeriano & Maness, 2014).[33] What Alvin and Heidi Toffler (1994) described as the Third Wave or the information age engulfed modern society—cyberspace became the next contentious domain.[34]

1. Conflict in Cyberspace

Early on, as the information age began to take its form and supplant the industrial age, many conflict and rivalry scholars conjectured that the Third Wave would similarly impact inter-state affairs and tactics of warfare, just as the Second Wave had so utterly transformed First Wave's feudal, agrarian-based society. (Arquilla & Ronfeldt, 1993; Clarke & Knake, 2010; De Tocqueville, 1955; Lynn III, 2010; Toffler, 1980; Toffler & Toffler, 1993; Valeriano & Maness, 2015).[35] Various aspiring cyber-intellectuals and

[32] Rivalry – is a relationship between two states whereby through a series of connected disputes both sides use, with some regularity, their instruments of national power (i.e., diplomatic, informational, military, or economic [DIME]) to telegraph threats, to employ coercion or intimidation tactics in order to gain some competitive advantage over the other (Chairman of the Joint Chiefs of Staff, 2016; Diehl & Goertz, 2001; Farlin, 2014; Porter, 1991; Valeriano, Jensen, & Maness, 2018; Vasquez & Leskiw, 2001). Rivalries take on psychological manifestations of their enmity towards each other, which include suspicion, mistrust, hatred, and demonization (Maoz & Mor, 2002). This psychosis seems to permeate all level of civil societies (i.e., masses to elites) engaged in a rivalrous behavior (Maoz & Mor, 2002). Further, opponents view accommodations, made by their rival, in actions, deeds, or statements with bias suspicion, whereas, hostility consistently defines the true essence of a rival's intentions or attitudes (Jervis, 1976; Heradstveit, 1979; Maoz, 1990; Maoz & Mor, 2002, p. 7).

[33] Conflict – is a disagreement on preferred outcomes (Valeriano & Maness, 2015, p. 32).

[34] Toffler uses "social wave-front analysis" as a theoretical construct or metaphor to explain the often turbulent, unpredictable, and often destructive fluctuations in societal patterns that emerge as a result of changes in technology, brought about by necessity or cycles of innovation (i.e., First Wave – Agricultural Revolution, Second Wave – Industrial Revolution, Third Wave – Information Revolution) (Nye J. S., 2011; Toffler, 1980; Toffler & Toffler, 1993).

[35] The First Wave – Agricultural Revolution (i.e., age); the age of the three estates, 1st Estate or the Clergy, 2d Estate or the Nobility, 3d Estate or the Serfs, Peasants, or Commoners. Social and Political power resides with the owners of the land, usually nobility. Society revolved around the cultivation of arable land and the security of it. Hence, conflict generally revolved around the protection or acquisition of land or territory (Connolly, 1979; De Tocqueville, 1955; Toffler, 1980; Toffler & Toffler, 1993). Information circulated from person to person by word of mouth. Agrarian Age spanned from 8000–9000 BC or BCE (Saharan Africans begin to farm and raise cattle for subsistence) to 1770s (Toffler, 1980).

cyber-luminaries surmised that cyberspace would become the next contested domain, comparable to the land, sea, air, and space domains (Arquilla & Ronfeldt, 1993; Clarke & Knake, 2010; Valeriano & Maness, 2015). As a matter of their own national security, states seek to master, if not dominate, each domain in an effort to minimize threats from other states (Choucri, 2012, p. 38; Valeriano & Maness, 2015, p. 37). Yet, due to the internet's complexity, most policy makers and state leaders rely on cyber security professionals and scholars to gain insights and assist them in clarifying their policies and initiatives in this realm (Clarke & Knake, 2010; Clarke & Knake, 2019).

Certainly, many cyber professionals and scholars using qualitative research methods, and its requisite inductive reasoning, have done their best to inform the ongoing cyber debate amongst policy makers and elites. Indeed, qualitative research remains the time-honored, central pillar of comparative politics and the basis for most research in the cyber arena. The growth of the internet and the veritable explosion of available data creates an estimated 2.5 quintillion bytes per day and the computational means to analyze them.

Second Wave – Industrial Age (i.e., Revolution), the age of mechanization of textiles, transportation, communications, warfare, etc., which created the requisite mass production, mass merchandising, mass distribution of goods and services, and mass media (Toffler, 1980; Toffler & Toffler, 1993) a. social and political power resides with those leading, managing, or investing in major industries (i.e., gas, oil, steel, automobile, etc.). Society became dependent on industrial production and the security of materials and means of production. Information begins to accelerate beyond person-to-person communication to print media and transmission via telegraph, telephone, and/or wireless radio. Agriculture still necessary to sustain the population became increasingly industrialized and more efficient (i.e., Eli Whitney's Cotton Gin, steam engine, steam locomotive). Conflict between the industrial and agrarian age societies culminated in the U.S. Civil War (1861–1864), with the industrial society firmly supplanting the agrarian (Toffler, 1980). The Industrial Age spanned from approximately 1800 to 1960.

Third Wave – Information Revolution (current age), the age of digitization and computerization of information through use of interconnected networks spanning the globe (i.e., the internet, World Wide Web, Cyberspace), enabling the nearly instantaneous transfer of information and knowledge, leading to the demassification of society (Nye J. , 2014; Toffler, 1980; Toffler & Toffler, 1993). Social and political power resides with those creating, innovating, controlling, managing, harnessing information to improve or innovate the use of existing legacy or newly developed systems (Nye J. , 2014; Toffler, 1980; Toffler & Toffler, 1993). By using information, agriculture and industrial products have become commodities (Toffler, 1980; Toffler & Toffler, 1993). The Information Revolution began in the 1960s and continues in the present era.

Thus, human understanding of the internet, in its entirety, remains elusive.[36] Nevertheless, this increase in data availability and computational power has combined to enable political and social scientist to leverage statistical tools and to quantitatively test these conjectured qualitative *cyber* mechanisms (Baum & Zhukov, 2015; IBM, 2018; Maness & Valeriano, 2016; Rid, 2012; Toft, 2014; Valeriano & Maness, 2014; Valeriano & Maness, 2015; Warren, 2015). These political scientists have uncovered some interesting results as they pertain to conflict and rivalry in cyberspace.

To begin with, inside cyberspace empirically, a lot of rivalry and some conflict exists, but very few cyber disputes or conflicts ever spill over into the terrestrial realm or cause any real world destruction *(Schmitt, 2013; Valeriano & Maness, 2014; Valeriano & Maness, 2015)*.[37] In fact, Valeriano and Maness (2015) demonstrated in their research that roughly 16% (i.e., 20) of rival dyads actually devolved into cyber conflict between 2001 and 2011.[38] Thus, relatively few cyber rivalries have blossomed into cyber conflicts (Lindsay, 2013; Maness & Valeriano, 2016; Valeriano & Maness, 2014; Valeriano & Maness, 2015). Further, evidence exists that these conflicts initially resulted in financial loss due to damage of IT systems, exfiltration of intellectual property, destruction of information, etc., leading to the loss of reputation of the target state or non-state actor. In

[36] In 2017, it was estimated that daily humans create 2.5 quintillion bytes of data, the equivalent to approximately of 47 million Blu-Ray ©, high capacity, storage discs (IBM, 2018). Each Blu-Ray © disc holds 50 gigabytes of data. If one placed each of the 47 million discs atop the other starting at sea level, the stack of discs would tower to the height 56 kilometers or approximately ~ 35 miles – just beyond the Earth's stratosphere (Layers of Earth's Atmosphere, 2018). That figure is calculated by equating 2.5 quintillion bytes to 2.33 billion gigabytes. One Blu-Ray disc holds 50 gigabytes. By dividing the 2.33 billion gigabytes by 50 equals 46.6 million discs. A single Blu-Ray disc has a width of 1.2 millimeters or 0.00394 of a foot. By multiplying 46.6 million by the width of the disk, one derives the height in feet spanned by stacking each disk atop or 183,604 feet, which equates to 56 kilometers or 35 miles once converted. It is estimated that only about 0.5% of this data is used or analyzed by humankind per day (Regalado, 2013).

[37] Cyber dispute – specific campaigns between two states using cyber tactics during a particular time-period and contains one to several incidents, often including an initial engagement and responses (Valeriano & Maness, 2014, p. 349).

Cyber conflict – the use of computational technologies in cyberspace for malevolent and destructive purposes in order to impact, change, modify diplomatic, economic, and military interactions between entities [state or non-state] short of war and non-contiguous to a battlefield (Valeriano & Maness, 2014, pp. 348-351; Valeriano & Maness, 2015, p. 5).

[38] 20 (rival dyads with observed cyber conflicts between 2001 and 2011) divided by 126 (known rival dyads existing over the 2001 to 2011 period) = 0.15873 ~ 16% (Valeriano & Maness, 2015, pp. 88-96).

fact, Maness and Valeriano (2016) provided empirical evidence that cyber incidents have little or no impact on foreign policy relationships between states involved in cyber conflicts with one exception—Distributed Denial of Service (DDOS) incidents.[39]

Further, it appears that full-scale cyber conflict in observable numbers, falls astonishingly short of what one might expect. This surprisingly low number appears to indicate that Valeriano and Maness' (2015) theory of cyber restraint may be in operation. State or non-state antagonists may constrain their tactics in cyberspace to avoid miscalculation or misinterpretation of intentions, thereby, intentionally preventing a conflict (Maness & Valeriano, 2016; Valeriano & Maness, 2014). Indeed, most of the cyber activities observed fall well short of conflicts; instead, fall into the realm of a low-level cyber incidence or intrusions at best. Since rivalries seem to exist as precursors to conflicts, as discussed above, an exploration of the literature describing international rivalry in cyberspace would logically follow. So, what does rivalry look like in cyberspace?

2. Rivalry in Cyberspace

First, most enduring rivalries stem from some longstanding territorial disputes and the resources that exist within the territory in question, usually amplified by cultural, ethnic, or religious issues and are largely regional (Diehl & Goertz, 2001; Klein, Goertz, & Diehl, 2006; Thompson, 2001; Toft, 2014; Valeriano & Maness, 2014; Valeriano & Maness, 2015; Vasquez & Leskiw, 2001; Weidmann, 2015). Rivalries encompass the ongoing process of interaction and the psychological baggage surrounding the issue under dispute, leading to low-level cyber intrusions (Maoz & Mor, 2002; Valeriano & Maness, 2015). Cyber antagonists conduct intrusions, as discussed in the previous section, through

[39] Cyber Incident – a. an occurrence or set of occurrences that result in an actual or potentially adverse effect on an information system, network, and/or the information residing therein (Committee on National Security Systems, 2015, p. 40). b. an individual action or cyber-operation launched against a state, by another state or non-state actor as part of an ongoing cyber dispute or conflict (Valeriano & Maness, 2014, p. 349; Valeriano & Maness, 2015).

Distributed Denial of Service (DDOS) – a tactic in which multiple compromised computer systems target a server [s], website [s], or other network resource [s], and cause a denial of service for users of the targeted resource. The flood of incoming messages, connection requests or malformed packets to the target system forces it to slow down or even crash and shut down, thereby, denying service to legitimate users or systems (Beaver, 2018, sec."DDOS").

the *syntactic* substrate of cyberspace's *synthetic* layer (Choucri, 2012; Clarke & Knake, 2010; Libicki, 2007; Valeriano & Maness, 2015). These intruding actors intend to gain access to and through the *synthetic* layer to execute any number of various cyber tactics driven by malice, subversion, or simply seeking information. The *semantic* and *syntactic* substrata, within the *synthetic* layer, will remain the focus of the rest of this volume, because this is where manifest, low-level rivalrous behavior or intrusions regularly occur (Valeriano & Maness, 2015).[40]

Since most internet users do not have the technical skills necessary nor the time to attempt an intrusion, the next probable suspects are botnets.[41] Botnets (i.e., robot networks) consist of a host of networked computers forced or clandestinely compromised by a remote user or hacker to perform an array of functions (Clarke & Knake, 2010; Gandhi, et al., 2011; Kello, 2013; Rid, 2012; Shackelford, 2012; Singer & Friedman, 2013; Valeriano & Maness, 2015, p. 34).[42] The hackers often execute the common DDOS cyber

[40] In the ISO layering construct, the syntactic layer encompasses layers 5 (i.e., session or login procedures) and 7 (i.e., applications) (Comer, 2015). Whereas, the semantic layer, as defined in the ISO construct, would consist of layer 6 or the data presentation layer (Comer, 2015).

[41] As of 2016, an estimated 75 million servers globally undergird internet operations (Jones, 2016). Types of servers include cloud, database, file, print, web, game, and applications servers (Comer & Stevens, 1993, p. 11). In our initial cyber intrusion data set collected intrusions made on a single application server for approximately 124 days in early 2015. Over that time, this physical server accounted for over 1.048M cyber intrusions. These cyber intrusions are monitored by the information resources branch of the organization and measured in the level of intrusion severity from 1 (high risk) to 5 (low risk). If we were to use this total number of intrusions as a benchmark to calculate the level of cyber intrusion activity across all of the servers plugged into the internet the number would be approximately 634 billion intrusions per day (Internet Users by Country, 2017; Jones, 2016). [1,048,000 (Intrusions) / 124 (days) = 8,452 (intrusions per day) | 8,452 X 75,000,000 (estimated # of servers on the internet) = 633,870,967,742 ~ 634 billion cyber intrusions per day across all internet servers (Internet Users by Country, 2017; Jones, 2016).] Meaning that every human connected to the internet would need to execute 188 cyber intrusion attempts per day. [633,870,967,742 (per day intrusions) / 3,366,542,060 (# of internet users in 2016) = 188 (intrusions per internet user, per day) (Internet Users by Country, 2017).]

[42] Botnet(s) – host of networked computers forced or clandestinely compromised and controlled by a remote user or hacker to perform an array of functions. Botnets constitute free (stolen) computational or network resources leveraged to conduct malicious activity on the internet, such as denial of service, defraud internet advertisers, etc., while masking the identity of the remote operator (Singer & Friedman, 2013, p. 44). Hackers use tailored malware to clandestinely take over and exploit a computer or networks resources for their own purposes (Singer & Friedman, 2013). Hackers use various methods to propagate their customized malware via automated or non-automated means (Shin, Lin, & Guofei, 2011).

tactic by leveraging their botnets (Clarke & Knake, 2010; Gandhi, et al., 2011; Kello, 2013; Rid, 2012; Shackelford, 2012; Singer & Friedman, 2013; Valeriano & Maness, 2015, p. 34). Further, the vast number of internet users who own these compromised computers never realize their system is part of a botnet (Kello, 2013; Singer & Friedman, 2013; Valeriano & Maness, 2015).

Regardless of whether these intrusions originate with a group of hackers with or without botnets, the global level of activity estimated at 634 billion intrusions per day (see footnote 42), even if it is off by a factor of ten, seems worthy of investigation. Certainly, a lot more activity in cyberspace is happening around the lower end of the spectrum where cyber intrusions reside and well within the realm of rivalry behavior, especially when one considers the small number of cyber incidents or conflicts, previously discussed. Further, this back of the envelope analysis of these state or non-state cyber interactions provides some evidence of the operation of cyber restraint theory at the synthetic level (Valeriano & Maness, 2015).

While qualitative and, more recently, quantitative scholars have exhaustively analyzed the conflictual end of cyber interactions, qualitative academics have generated many insightful conjectures and theories. A few quantitative scholars have provided empirical evidence equating to 111 incidents and 45 disputes between 20 rivals over an 11–year period (Valeriano & Maness, 2015, p. 89). This research begets cyber restraint theory backed up by empirical evidence that only 20 of those 126 rivalries (~ 16%) escalated into cyber conflict (Valeriano & Maness, 2015, p. 89). Nevertheless, while this research is quite valuable, it relies on a relatively small number of documented cyber conflicts, disputes, or incidents that occurred in the real world.

Malware – software or firmware intended to perform an unauthorized process that will have adverse impact on the confidentiality, integrity, or availability of an information system. A virus, worm, Trojan horse, or other code-based entity that infects a host. Spyware and some forms of adware are also examples of malicious code, hardware, firmware, or software that is intentionally included or inserted in a system for a harmful purpose (Cichonski, Millar, Grance, & Scarfone, 2012, p. 60; Committee on National Security Systems, 2015, p. 79).

However, based on the extrapolation using real-world cyber intrusion data to derive an albeit rough approximation of 634B intrusion attempts per day across cyberspace (see footnote 42 above for the calculation), this area seems ripe for analysis because the preponderance of cyber activity appears to fall into the intrusion or the intrusion attempt realm. This cyber intrusion activity seems to be indicative of low-level rivalrous behavior, regardless of whether the intrusion originated from state or non-state actors. Within this construct, players seek to gain the attention of their rival, perhaps to modify their behavior, policy, or intention, but do so in a restrained manner. Presently, no research has leveraged real-world cyber intrusion data to explore what drives this behavior using quantitative statistical techniques. This volume seeks to add to the body of knowledge by next conjecturing a typology of what motivates cyber intrusion behavior in rivalry dyads, regardless of whether a state or non-state actor(s) executed the intrusions or attempts.

D. TYPOLOGY IN CYBERSPACE

Cyber intrusion behavior at this less harmful end of the rivalry spectrum revolves around two categories or intents: 1) Subversive Intent or 2) Information Seeking Intent. Each result in different kinds of observed behavior, pursuing often-divergent goals. On one end of the typology, is a malevolence driven by the desire to harm a rival, even if the antagonists hurt themselves in the process, they view their actions as just (Maness & Valeriano, 2016; Valeriano & Maness, 2015). The main thrust of this observed behavior appears to focus on questioning the existence or the legitimacy of a given rival’s authority (i.e., government, President, Congress, Parliament, etc.) (Rid, 2012).

The opposite end encompasses actions set upon deliberately gathering information to satisfy some conscious or unconscious need, want, or desire (Case & Given, 2016; Valeriano & Maness, 2014; Valeriano & Maness, 2015; Valeriano, Jensen, & Maness, 2018). This type can span from simple curiosity, to espionage, or to the nefarious—seeking to harm an individual or country's reputation. Nevertheless, regardless of type, the vector of these intrusions are predominately malicious.[43]

The research parses this arena of cyber intrusion behaviors into these types to provide granularity of understanding. The intent is not to force these would-be hacktivist or intruders, manifesting cyber intrusion behavior, into one of these discrete bins; rather, the research's aim is to use these categories in a discursive manner. Meaning that an intruder could begin the process by initially conducting intelligence, surveillance, or reconnaissance (i.e., information-seeking) of a given server to achieve the subversive goal by defacing the organizations website each of which begins along a malicious vector appearing as a cybercrime.[44] The intent of this typology is to provide the spectrum and the boundaries of these evident intrusive behaviors to draw upon in the exploration of motivations driving cyber intrusion activity. The succeeding paragraphs will precisely define the parameters of such cyber intrusions.

1. Subversive Intent

The Distributed Denial of Service (DDOS) (a.k.a. virtual sit-in or blockade) of a targeted network; the degradation or disruption of a given internet target; the spreading of propaganda or disinformation aspiring to deceive; or the defacement of a target's website by a large group of hacktivists or a group of hacktivists wielding their subjugated botnets describes the cyber activities that bound subversive intent (Clarke & Knake, 2010; Gandhi, et al., 2011; Kello, 2013; Maness & Valeriano, 2016; Rid, 2012; Shackelford, 2012; Singer & Friedman, 2013; Valeriano & Maness, 2015). These cyber acts intend to challenge the integrity, veracity, power, and authority of established institutions or positions (i.e.,

[43] Intrusion, infiltration, or exploitation of IT systems to steal intellectual property, a person's identity, or execute a *cybercrime* comprise the lattice of cyber actions and goals that form the boundaries of malicious vector (Choo, 2011; Goodman, 2015; Valeriano & Maness, 2015). These observable actions seem intent on causing financial, psychological, or reputational harm to the target (i.e., individual or government), regardless of whether the hacktivist achieves their goal. Therefore, the desire to commit an unlawful act to cause financial, psychological, or reputational harm or distress to a rival defines the *malicious vector* (Goodman, 2015; Sharp, 2017; Valeriano & Maness, 2015).

[44] Cybercrime – any crime that is facilitated or committed using a computer, network, or hardware device (Gordon & Ford, 2006, p. 14). Examples include but are not limited to phishing, identity theft, cyber stalking, theft of intellectual property, exfiltration of data, etc.

governments, agencies, corporations, presidents, prime ministers, parliaments, etc.). Hacktivist use these tactics to imply that the state, entity, or organization lacks the ability to control their operations in cyberspace; therefore, by extension, the target cannot influence or control their real-world operations (Valeriano & Maness, 2015, pp. 33–34). Their approach is to erode each individual's social bonds, beliefs, and trust in the state or non-state entity and in doing so possibly recruit or coerce followers to their cause (Rid, 2012, pp. 22–23; Valeriano, Jensen, & Maness, 2018). Again, regardless of whether the hacktivists realize their goal; it is the execution of the cyber subversive act that counts (Rid, 2012). Thus, the desire to undermine the constitution, the integrity, or the authority embodied in a rival's ability to exercise control over their established institutions or entities defines *subversive intent* (Rid, 2012, p. 22; Valeriano & Maness, 2015, pp. 33–37).

2. Information Seeking Intent

The conduct of cyber espionage (i.e., intelligence, surveillance, or reconnaissance), or the theft of information specifically by gathering, exfiltrating, or stealing information on or about an opponent delineates the parameters of information seeking intent (Carter, 2015; Clarke & Knake, Cyberwar, 2010; Denning & Denning, 2010; Gandhi et al., 2011; Gartzke & Lindsay, 2015; Kello, 2013; Samuel, 2004b; Valeriano & Maness, 2015). This cyber behavior makes up right at 50% of all cyber incidents cataloged by Valeriano, Jensen, and Maness (2018) in their longitudinal study spanning from 2000 to 2014.

Needs, wants, sense-making, or desires of the state or non-state actors seem to drive these observable deeds (Case & Given, 2016; Dervin & Naumer, 2009; Turcotte, York, Irving, Scholl, & Pingree, 2015). Usually wants or sense-making manifest themselves in an individual's observable behavior patterns; whereas, needs or desires do not normally reveal themselves in actions or deeds (Case & Given, 2016; Dervin & Naumer, 2009). In fact, individuals often find it quite difficult to verbalize a need or desire (Case & Given, 2016). Thus, in cyberspace, the research mainly deals with the state or non-state intruder's or hacker's *want* of information to discover patterns, fill gaps, or answer specific questions seeking information manifesting active or intentional behavior (Case & Given, 2016, p. 93; Dervin & Naumer, 2009). Doxing would also fall into this category. Doxing involves a hacker seeking to infiltrate a target’s network to extract personal or governmental information that the target may find embarrassing, if or when made public (Singer & Friedman, 2013).[45] As such, the active and intentional actions in cyberspace, set upon executing acts of cyber espionage (i.e., intelligence, surveillance, reconnaissance) to exfiltrate or gather information specifically from or out of a target’s IT networks defines *information seeking intent (Case & Given, 2016; Clarke & Knake, 2010; Denning D. E., 2011; Dervin & Naumer, 2009; Gandhi, et al., 2011; Gartzke & Lindsay, 2015; Kello, 2013)*.

Therefore, subversive intent or information seeking intent enabled by a malicious vector make up the typology bounding this research space. These acts define those behaviors and observable actions that seem to manifest themselves in the available data set. Analysis of real-world cyber data to provide evidence to buttress conjectured theories through the use of statistical models remains the focus of this research, intent on exploring these relationships in the third wave.

3. Third Wave Implications

Valeriano and Maness (2014; 2015; 2016) and many others through numerous scholarly contributions refined the understanding of cyber conflicts, disputes, and incidences (Gartzke & Lindsay, 2015; Lindsay, 2013; Rid, 2012). Their research and that of others enabled this research to move from a broad understanding of international conflict and rivalry in cyberspace to ultimately arrive at the discrete portion of rivalry that will be explored in the following chapters. In this last section of the typology, the researcher will explore the impact of information age on regime types and how state rivals interact in cyberspace.

[45] Doxing – revealing personal documents publicly, as part of a protest, prank, or vigilante action. Often doxing requires minimal network penetration, relying more on careful research to link hidden personal or embarrassing data to the victim (Singer & Friedman, 2013, p. 46).

Again, leveraging much of the current scholarly material about state on state rivalry, these studies provide a foundation of evidence indicating how regime types have acted or will act in this domain in the past, present, or future. This research will survey this space by reviewing actions of two autocracies, two anocracies, and two democracies, noting their differences in the case study chapters. Given this scope, broad generalizations can be challenging; nevertheless, these will provide a set of indicators showing how these regime types compete in this space. Although this is not a direct match with the categories used by Valeriano, Jensen, and Maness (2018), the research will leverage the explanatory value of the defined typology, as shown in Table 2. In doing so, the research seeks to classify each regime type, to understand how they seem to leverage cyberspace in order to achieve some *competitive advantage* (Choucri, 2012; Diehl & Goertz, 2001; Porter, 1991; Valeriano, Jensen, & Maness, 2018; Vasquez & Leskiw, 2001).

Table 3. Frequency Counts for Vector and Intent of Cyber Incidents 2000–2014. Adapted from Valeriano, Jensen, and Maness (2018).

Regime Type	**Cyber Vector**	**Cyber *Intent / in order of Priority**	**Total Cyber Incidents**
Autocracies	Malicious** (80/95 = **84%**)	#1 Information Seek (62/95 = **65%**) #2 Subversive (33/95 = **35%**)	**95**
Anocracies	Malicious (32/45 = **71%**)	#1 Subversive (25/45 = **56%**) #2 Information Seek (20/45 = **44%**)	**45**
Democracies	Malicious (44/52 = **85%**)	#1 Subversive (33/52 = **63%**) #2 Information Seek (19/52 = **37%**)	**52**

*Valeriano, Jensen, and Maness (2018) use the term Cyber Objective, which in this paper is synonymous with Cyber intent.
** The majority of the non-malicious vector consists of DDOS attacks, which fall under subversive intent.

4. Rivalry in the Third Wave

Thus, states of differing regime types, with the commensurate level of sophistication, participate in this domain. While their motivations may be different, the intent to gain the necessary level of capability to protect a state's national interest in cyberspace seems apparent (Choucri, 2012; Valeriano & Maness, 2015). All of our antagonists noted in this realm employ malicious methods (i.e., intrusion, infiltration, exploitation) to penetrate through the syntactic layer in order to gain access to the semantic layer where the information they seek to find or manipulate for subversive intent exists. Regardless of whether the target is a state or non-state actor, this method of access remains consistent (Choucri, 2012; Clarke & Knake, 2010; Libicki, 2007; Valeriano & Maness, 2015; Valeriano, Jensen, & Maness, 2018).

Certainly, hacktivist cyber-intrusion attempts begin the process that either leads to information seeking or subversive intent. Thus, studying the cyber intrusion phenomenon and trying to determine its causal determinants appears ripe for exploration. The research intends to use the quantitative methods used by scholars in this arena to empirically test whether the tone, variance, and types (i.e., material and verbal) of continuing media narratives have an impact on cyber intrusions. However, before testing that correlative linkage, theoretical refinement of several other theories is necessary to flesh out the impending explanations.

E. TWO-LEVEL INTERNATIONAL RELATIONS THEORY

As discussed briefly in the Introduction, Putnam posited that two levels of negotiations occur simultaneously as one state engages another in formal discussions over some issue of mutual interest (Conceição-Heldt & Mello, 2017; Putnam, 1988; Trumbore, Boyer, Gibson, Harvey, & Wilkenfeld, 2000; Walton & McKersie, 1965). Leveraging the descriptive value of this theory, one can envision a dyadic negotiation between two states. One in which both nations use the *information* instrument of national power seeking to ensure that the negotiation culminates in an outcome favorable to their state (Farlin, 2014; Mattis, 2018). Putnam (1988) describes this as level-one, international messaging or communication between the leaders or negotiators of these states, pursuing a *win-set* satisfactory to their side of the negotiation. Parallel to these level-one negotiations resides the level-two domestic dialog, where bargaining and consultation with elites or opinion leaders occurs, seeking to influence or control the narrative conveyed to the country's population to cultivate support of the chosen level-one win-set. In this process, elites set out to assist or inhibit their nation's leaders efforts to either ensure the chosen win-set's ratification or prevent its rejection (Bjola & Manor, 2018; Conceição-Heldt & Mello, 2017; Putnam, 1988; Strong, 2017; Trumbore, Boyer, Gibson, Harvey, & Wilkenfeld, 2000).

1. Theory Linkage

Further, although Putnam (1988) makes no distinction between regime types in discussion of the two-level process, he does imply that *no* state leader is totally immune from domestic pressures surrounding a given issue (Putnam, 1988; Trumbore, Boyer, Gibson, Harvey, & Wilkenfeld, 2000). Yet, intuitively and within the body of knowledge on this subject, evidence exists that democracies encounter more difficulties managing the domestic narrative of the issue at hand versus other regime types such as anocracies and autocracies (Trumbore, Boyer, Gibson, Harvey, & Wilkenfeld, 2000, p. 693).

Further, as Trumbore et al. (2000, pp. 687–688) discovered the constellation of proximate leaders (i.e., elites, opinion leaders) advising a state's decision maker on given conflictual issues decreases markedly across the continuum from democracies to anocracies to autocracies. Or simply, this research indicates that the *number* of elite voices who have access to a state's leadership during negotiations decreases across regime types from democracies to autocracies. This decrease enables elites in anocracies and autocracies to enjoy greater influence over their country's leaders and the chosen narrative. Therefore, the real power to control the domestic narrative rests in the hands of fewer elites across the spectrum of regime types discussed here.

a. Media Indexing

Media journalists use indexing in writing their stories in an attempt to reach their professional standard of balanced, fair, and objective reporting. Indexing will cause the media to report the narratives of those elites who are perceived to have the ability to influence events, at a higher rate or in greater proportion than other voices (Bennett, 1990; Strong, 2017, pp. 293-294).[46] In effect, enabling these fewer elites in autocracies, and less so in anocracies, to have an outsized ability to control their state's side of the ongoing narrative particularly at the domestic level or level-two. The impact of this outsized influence may manifest itself in the amount of cyber intrusions coming from these regime types by magnifying the narratives of fewer indexed elites projecting an influence over large portions of their intrusive populations. As Bennett (1990) posited and Strong (2017) validated, *indexing* operates in the journalistic community and may become a factor in the conduct of this research. Finally, as implied above, Strong (2017) states that indexing can *amplify* the influence of elites. Especially, when a country has fewer elites in position to advise their leaders that discrete set of proximate leaders enjoy an enormous amount of influence. Further, each regime, depending on type, may exercise an amount of control over media content in cyberspace. This control of content provides regime leadership with the capability to cement their control of the domestic narrative and enhance their ability to exercise social control at level-two.

Lastly, the indexing of foreign leaders by another states domestic media, depending upon the dyadic relationship between two states, can lead to reverberation (Putnam, 1988; Strong, 2017).[47] Putnam (1988) rightly played down this effect on the U.S., because

[46] Indexing – the way in which journalists write their narratives (i.e., stories) by reporting the voices or viewpoints of prominent officials who, because of their influence, may affect the outcome of the situation (Bennett, 1990; Strong, 2017). Journalists perform the function of indexing to ensure they adhere to professional standards of balanced, fair, and objective reporting, which is reinforced by normative editorial standards (Bennett, 1990; Strong, 2017).

[47] Reverberation – how statements and actions of foreign actors (i.e., elites) reported by media sources can affect the domestic politics of another state, thereby, influencing the foreign policy decisions of that state (Putnam R. D., 1988; Strong, 2017).

foreign actors statements and actions have only limited significance in the U.S. (Hayes & Guardino, 2013; Murray, 2014; Strong, 2017). However, Putnam did point out that weaker states should and do greater attention to stronger states (Putnam, 1988; Strong, 2017). Subsequently, Strong (2017) showed how non-rivalrous states like the U.S. and the United Kingdom (UK), who enjoy an unusual, often harmonious relationship, may enable the UK's media to index certain U.S. elites statements or actions resulting in reverberation within level-one of the UK's policy arena (Conceição-Heldt & Mello, 2017). This conjecture will be explored in the Democracies case study to follow.

b. Content Controls

In addition, to these fewer elite voices, depending on regime type and country, controls placed on content in cyberspace may be vastly different. Deibert and Rohozinski (2010) created a typology describing the generations of cyberspace content controls. Deibert (2015) extended this typology from three generations to four as shown in Table 4. The forms of internet content controls as described exist within and are employed in various degrees by all countries and regime types. Further, all generations are *not* mutually exclusive and can exist simultaneously in a given country (Deibert & Rohozinski, 2010, pp. 28-29).

Democracies may use certain aspects of Second or Third-Generation controls to address child pornography, cybercrime, or terrorism, but usually follows strict legal parameters with incumbent checks and balances to prevent abuse by state authorities (Choo, 2011; Deibert & Rohozinski, 2010; Deibert, 2015; Goodman, 2015; Kriesi et al., 2013; Mackinnon, 2011, 2012; Morozov, 2011; Stier, 2015). While autocracies tend to rely on the first three applying exhaustive information controls and perhaps, may dabble a bit in the fourth (Akgül & Kırlıdoğ, 2015; Aryan, Aryan, & Halderman, 2013; Deibert & Rohozinski, 2010; Deibert, 2015; Greitens, 2013; Mackinnon, 2011, 2012; Morozov, 2011; Pinkaew, 2016; Ruijgrok, 2017). Anocracies appear to have vaulted over the first in favor of employing the second and third in tandem (Deibert & Rohozinski, 2010).

Anocracies, appear to enjoy the benefits of plausible deniability by accepting pro-regime supporter's use of extra-judicial tactics to intimidate any opposition, thereby squelching any alternative narrative, while simultaneously accepting *no* responsibility for these partisan actions (Calamur, 2017; Deibert & Rohozinski, 2010; Deibert, 2015; Maréchal, 2017; Nocetti, 2015; Ognyanova, 2018). Finally, this typology will become beneficial later in this chapter's discussion, becoming discretely helpful during analysis of regime types and countries in the case studies.

But for now, this generational typology describes the unique aspects of internet content controls that can be used by a regime to enable them to effectively manage or control the domestic narrative at level-two. This level of control would be quite beneficial as a country's leader attempts to gain some advantage during negotiations with the U.S. The ability to control the domestic narrative through both the elites and via the internet's synthetic controls could be quite valuable—particularly when considering the nature and the positive or negative content of narratives.

Table 4. Range of Cyberspace Information Content Controls

Descriptions of the Generations of Internet Content Controls
First-Generation (Gen):[1] Covers the denial of access to specific internet resources through the use of blocking, filtering, or deep packet inspection (DPI) techniques, active policing of cyber cafés, and/or the creation country, state, language, or domain specific internet (i.e. Great Firewall of China, Halal Internet, RUNET, etc.).[1] First Generation (Gen) controls are inherently *defensive* in nature and are employed domestically.
Second-Gen:[2] Encompasses the creation of legal governance frameworks buttressed by technical capabilities establishing a normative environment, whereby, state-enabled actors can deny access to or modify selected information resources in real time. Thus, the legal, normative part forms the *overt* aspect, which provides the legitimacy for the *covert* aspect to monitor and censor all content—as necessary. Overtly, this legal basis grants these state-enabled actors the authority to covertly monitor what the citizen user reads, posts, or attempts to use prohibited content. Thereby, this covertly gathered information can be used to support overt or coercive tactics such as arrests, detainment, fines or other forms of intimidation as a means to maintain control of social discourse and the dominant narrative. The combination of the overt and covert aspects places the citizen user in a catch-22, where meeting the requirements for compliance sets the conditions for prosecution and non-compliance forms the legal basis for punishment. Covert content controls include informal removal of information or censorship, technical shutdowns, computer network attack techniques. Overt illegal content infractions can be anything the state deems a threat to their national security, which can include anything from criticism of religious or state officials, to the use of The Onion Router (TOR), or to the use of social media to coordinate a civil protest.
Third-Gen:[3] Covers the set of controls that intends to compete in the information space in a sophisticated, multi-dimensional way carrying the state's narrative to the population, while undermining the opposition's narrative through the use of an utterly devastating counterinformation campaign with the intent to demoralize, discredit, and overwhelm any opponent. Third Gen controls include warrantless surveillance, state-sanction cyberzones, and information campaigns, data mining targeted systems, and direct action.[4] Surveillance and data mining of targeted computer systems are specifically meant to confuse, entrap, and disgrace opponents. Third-Gen controls are inherently *offensive* in nature and span from domestic controls to international campaigns attempting to expand their country's narrative to influence other states. Elements of Third-Gen controls can be executed by regime recruited, crowdsourced citizens who may feel compelled to direct action methods to squelch opposing voices. These crowdsourced legions provide the regime with the ability to use plausible deniability to distance themselves, as necessary, from the more rash actions (i.e., extra-judicial) undertaken by their partisans. Examples include China's fifty-centers and Russia's Patriotic Hackers.
Fourth-Gen:[5] Encompasses the expansion of authoritarian controls from the tactical or operational realm into the strategic; whereby, autocratic states argue for greater expansive, state-led controls and democratic states advocate for greater openness and transparency in cyberspace. The differences between the two could not be more stark. With the autocracies viewing the internet residing within their borders as their sovereign, albeit synthetic, territory that must be controlled, policed, and secured. Further, any incursion upon that synthetic territory is regarded as an attack on their state's sovereignty. While the democracies see the internet as an international domain useful to exchange ideas, to foster innovation, and to execute global commerce. The internet is a synthetic construct to be exploited, shared, and leveraged for the greater good. These bipolar debates occur in both regional and international forums where cyberspace policy is being crafted. This is precisely where these strategic struggles about cyberspace governance occur. This is also where the strategic struggle against the expansion of authoritarian controls in cyberspace occur.
[1] Deibert, 2010, 2015 [2] Akgül & Kirlidoğ, 2015; Deibert & Rohozinski, 2010, 2015; Ensafi, Winter, Mueen, & Crandall, 2015; MacKinnon, 2011; Morozov, 2011 [3] Deibert, 2015; Deibert & Rohozinski, 2010 [4] A cyberzone consist of state sanction electronic spaces (i.e., state sponsored—intranet), which only can access authorized state provided information (Deibert & Rohozinski, 2010). Direct action is defined as any action that achieves its desired goal (i.e., civil disorder, civil strife, civil disorder, civil violence, or any state sponsor variations thereof) and spans from cyber to kinetic measures (Deibert & Rohozinski, 2010; Deibert, 2015; King M. L., 1963; Keck & Sikkink, 1998; MacKinnon, 2012; McAdam, McCarthy, & Zald, 1999) [5] Deibert, 2015; Maréchal, 2017; Nocetti, 2018

2. Theory Application

To begin with a country's leadership will choose a type of storyline in order to maneuver into a position of advantage during a negotiation, possibly selecting a negative narrative. To that point, as discussed in the Introduction, that leader might prefer a negative verbal or material narrative, believing it will optimize their negotiation space allowing them to achieve a win-set for their country. For example, say a given state is locked in a dyadic negotiation with the U.S. that state might use negative *verbal* narratives attempting to coerce, cajole, or influence the U.S. into agreeing to their chosen win-set. Depending on the regime type, a nation's hackers or intruders may react differently to this negative *verbal* rhetoric. Whereas, the research expects the hacktivist or intruder's reaction to be consistent across regimes, particularly when other nations create negative *material* narratives directed at the U.S. and its interests.

In democracies, the multiplicity of elite voices produce a cacophony of media reported narratives, which leads to a lack of clarity. This lack of clarity may lead to different levels of intrusions resulting from the material or verbal narratives used by the country opposite the U.S. in dyadic discussions. While anocracies and autocracies possess fewer elite voices and higher levels of internet content controls than democracies. The combination of the two enables fewer proximate leaders to project their outsized opinions on their state's leaders and the state's use of generations (i.e., levels) of content controls can produce a decidedly focused narrative.

Additionally, autocracies enjoy a definitive level of clarity and unanimity of viewpoints, and by extension a certain clarity of media messaging (i.e., narratives) when communicating with their domestic populations on a given issue. This progressing unanimity of narrative, which is not as coherent and oftentimes incomprehensible in democracies, becomes clearer and more precise in the progression through anocracies to autocracies. Thus, an increasing level of narrative clarity may imply a growing degree of societal control across these regime types. This posited increasing level of societal control may reveal itself in the level of cyber intrusions occurring the day following the media event and may differ across regime types as the hypotheses offered later will indicate.

But before departing this exploration, this research needs to close a few gaps in the explanation thus far. First, the research looks to a branch of communication theory to explain how elites interpret media events and influence civil society's view of the media narrative. Second, a quick exploration of the media events coding community will follow leading into the final piece of this review: the digital panopticon, narrative, and sharp power theories and how they relate to this research. So, how does Lazarsfeld's posited two-step flow of media information assist in this explanation?

F. TWO-STEP FLOW OF COMMUNICATION THEORY

This theory resides within the Media Effects branch of Communication Theory, specifically within the Minimal Effects theoretical structure (Ball-RoKeach & DeFleur, 1976; Katz, 2001; Neuman & Guggenheim, 2011; Postelnicu, 2008; Werder, 2009).[48] Throughout the 1950s and 1960s at Columbia University, a group of scholars led by Paul Lazarsfeld ostensibly rejected once dominant significant effects theoretic in favor of the minimal effects paradigm (DeFleur & Dennis, 1981; Lazarsfeld, Berelson, & Gaudet, 1944; Neuman & Guggenheim, 2011; Postelnicu, 2008).[49] One of Lazarsfeld's students,

[48] Media-Effects Theory – a. the deliberate and non-deliberate short and long-term within-person changes in cognitions (including beliefs), emotions, attitudes, and behavior that result from media use (Valkenburg, Peter, & Walther, 2016, p. 316). b. Elements of media effects include timing (immediate vs. long-term), duration (temporary vs. permanent), valence (negative or positive), change (difference vs. no difference), intention (or non-intentional), level of effect (macro vs. micro), direct (or indirect), and manifestation (observable vs. latent) (Potter, 2012, pp. 35-36). Media Effects falls under the larger umbrella of Communications Theory (Ball-RoKeach & DeFleur, 1976; Neuman & Guggenheim, 2011; Werder, 2009). Generally, the constituency of Media Effects Theory fit into three camps: the Significant Effects, Minimal Effects, and Cumulative Effects, also referred to as Interpretive Effects (Neuman & Guggenheim, 2011; Werder, 2009).

[49] In the early 1930s, it appeared that propagandists such as Hitler, Mussolini, or Tojo were quite adroit in the use media to influence their populations (Lasswell, 1935). As such, there seemed to be ample real-world evidence that media could indeed be the magic bullet to influence large passive or homogeneous populations (Ball-RoKeach & DeFleur, 1976; Lasswell, 1935; Neuman & Guggenheim, 2011; Werder, 2009). Subsequently, Claude Shannon (1948) discovered a formula that governed the amount of information or data broadcasted over a single channel, commonly referred to as Shannon's Law (Aftab, Cheung, Kim, Thakkar, & Yeddanapudi, 2002; Shannon C. , 1948; Shannon & Weaver, 1964). Weaver goes further to describe how Shannon's Mathematical Theory of Communication governs the rate at which semantic information aired to large audiences using a single channel can be transmitted and received; thereby, constraining the effect of media communication based on the audience and venue size (Shannon & Weaver, 1964, pp. 24-28). Further, very little evidence emerged, beyond the observed, revealing that those engaged in the propaganda campaigns of the 1930s and 1940s actually considered the magic bullet theoretic as viable

Joseph Klapper wrote an influential review of the premises underpinning the minimal effects view of the theory (Klapper, 1960; Neuman & Guggenheim, 2011).

Building on the research previously completed by Lazarsfeld et.al (1944), Klapper (1960) continued the investigation of the media's ability to influence voters during an election cycle. A critical finding of his research lies in the fact that media coverage only swayed a small fraction of voters (Klapper, 1960; Lazarsfeld, Berelson, & Gaudet, 1944; Neuman & Guggenheim, 2011; Postelnicu, 2008). He found that the perceptive viewpoints of opinion leaders (i.e., elites, politicians, and policy makers), conveyed through their social interactions with friends and acquaintances, had greater influence on the voting population. He also observed that these opinion leaders actively and shrewdly digested media narratives to form their opinions, which they in turn shared through their social interactions as described in the two-step flow model (Klapper, 1960; Lazarsfeld, Berelson, & Gaudet, 1944; Neuman & Guggenheim, 2011; Postelnicu, 2008).[50]

1. Theory Linkage

Thus, the mediated two-step flow begins with opinion leaders (i.e., elites or proximate leaders) collecting, interpreting, and untwining the media narrative to form their own positions on the subject of the day—step-one. Second, these opinion leaders pass on their views to the voting population via social interaction; thus, reinforcing a key component of minimal effects—step-two (Klapper, 1960; Neuman & Guggenheim, 2011, p. 172; Postelnicu, 2008; Werder, 2009). Thus, Lazarsfeld, Berelson, and Gaudet (1944) concluded that information transmitted, at the time via word of mouth, played a greater role in the influence of civil society then mass media narratives. Certainly, the velocity of that information transfer has continued to increase in the current era. But, on the cusp of

(Neuman & Guggenheim, 2011). As such, social scientist studying media effects began to question the foundation paradigms upon which the theory rested (Werder, 2009).

[50] Coincidentally, Klapper, at the time an employee of CBS News, testified before the U.S. Congress regarding media effects. At the time, Congress was considering regulating the television industry because of its perceived supporting *effect* on some of the transgressive societal mores emerging at the time. This fact only served to add to the folklore surrounding Klapper and buttress the pre-eminence of the minimal effects premise at the beginning of the information age (Neuman & Guggenheim, 2011).

the information age, another scholar discovered step-one of Lazarsfeld’s information flow operating in British society.

In the late 1990s, Kenneth Newton (1999) conducted a quantitative review of the impact of media, specifically television and print media, on a sample of the British population. In his findings, he noted that those participants who read a paper daily manifested a greater level of interest, working knowledge, and understanding of the current political issues (Newton, 1999). To a lesser degree, habitual television news viewers did as well. Further, Newton labeled these British daily paper readers as sophisticated consumers of media, particularly newsprint, and were cognitively mobilized[51] (Newton, 1999). Thus, certain elites consume media narratives and form opinions about that news. More recently, other scholars have found evidence that both step one and two operate in the information age.

The Turcotte et al. (2015) study found evidence of the two-step operating across modern social media platforms. First, their research found trust of the news media’s reporting guides individual behavior, with opinion leaders figuring prominently in lending credibility to media narratives (Ladd, 2013; Turcotte, York, Irving, Scholl, & Pingree, 2015). Second, opinion leaders, in step-two of the process, perform the necessary function of informing and educating civil society in the information age and may assist in forestalling the news media deteriorating credibility (Turcotte, York, Irving, Scholl, & Pingree, 2015, pp. 530-531). Thirdly, this study validates that the interpersonal nature of the two-step flow still matters in relation to news credibility and to information-seeking behavior. As a reminder, the later makes up 50% of all cyber incidents and is mentioned in section D of this chapter as one of the typological intents used to explain cyber intrusion behavior. Thus, it appears that the two-step flow of communication is relevant, operant, and useful for explanation—even today. Next, these theories will be fit into the existing theoretical structure.

[51] Cognitively mobilized – describes people or groups of people who manifest higher levels of political participation, who have deeper political discussions, who have comprehensive political information, who possess heightened political awareness, and have an ideologically refined set of political skills, as compared to the general population in western countries (Newton, 1999, pp. 581-582).

2. Theory Integration

As discussed in the Introduction and described graphically in Appendix C, it appears that the two-step flow operates within level-two or domestic political messaging during a given state's negotiations with the U.S. or other nations. This linkage rest on the body of knowledge associating the two theories, which can be tied closely together contingent on the level of domestic controls of internet content employed by a particular country (Bjola & Manor, 2018; Conceição-Heldt & Mello, 2017; Deibert & Rohozinski, 2010; Deibert, 2015; Katz, 2001; Lazarsfeld, Berelson, & Gaudet, 1944; Neuman & Guggenheim, 2011; Maréchal, 2017; Nocetti, 2015; Ognyanova, 2018; Putnam, 1988; Strong, 2017; Trumbore, Boyer, Gibson, Harvey, & Wilkenfeld, 2000; Turcotte, York, Irving, Scholl, & Pingree, 2015).

First, regardless of whether elites are creating or digesting the generated narrative this piece of the puzzle firmly resides in or is connected to step-one of the two-step flow and at domestic level-two. Second, elites communicate and affirm the veracity of the narrative to the population, at step-two and again well within the level-two domestic narrative, where a country's leadership manages the national messaging. Thus, the author conjectures theoretically that the two-step flow operates and reinforces the level-two domestic narratives in international relations between sovereign states, as depicted in Appendix C's logic map. The strength of this interaction may be constrained or reinforced by the level of domestic content controls used within a given country.

To varying degrees, this theoretical linkage operates within states attempting to manage that domestic narrative during level-one negotiations. For leaders and elites of democratic states, this process appears to be more of an attempt at managing the narrative due to the plurality of differing elite viewpoints that exist in democracies. As these competitive elites positionally jockey within civil society to create and sustain the dominate narrative seeking ratification of the current administration's chosen win-set (Hoffman-Lange, 2018; Putnam, 1976, pp. 115–121). This cacophony and plurality of narratives in democracies may lead to *increases* in tomorrow's intrusions resulting from the type of today's narrative, irrespective of type (i.e., material or verbal).

Within anocracies and autocracies, as the hypotheses will indicate, today's narrative, depending upon type (i.e., verbal or material) may manifest itself in the amount of intrusions tomorrow; thereby, indicating certain regimes possess a greater degree of societal control. This higher level of societal control rests on a traditional ruling class of consensual elites relying on a hierarchical structure linking elites to citizens (Hoffman-Lange, 2018; Putnam, 1976, pp. 115–121).

As discussed earlier, other scholars continue to expand this arena of study, particularly in the international relations arena. Conceição-Heldt and Mello (2017) named these elites gatekeepers or central actors in international negotiations. They and other scholars conjectured that these actors, now enabled by technology, can manage both the international (i.e., level-one) and domestic narratives (i.e., level-two), where the two-step flow operates, simultaneously (Bjola & Manor, 2018; Conceição-Heldt & Mello, 2017; Strong, 2017; Turcotte, York, Irving, Scholl, & Pingree, 2015).

Indeed, the number of channels or linkages connecting each elite to their domestic or international diaspora only continue to multiply (Barabasi, 2003). Twitter, Instagram, Snapchat, Facebook, Telegram, text message, cell phone, etc., are all constitute channels/ linkages connecting each individual, acting as a node for more and more information. Thus, opinion leaders / policymakers are connecting with more and more individual nodes, passing their views on a given issue. Therefore, in the past what could have taken days for an opinion leader to opine at next Saturday's cocktail party, is now passed in a matter of seconds—making the two-step flow nearly instantaneous. Indeed several scholars, using quantitative methods, discovered that the half-life of a given day's news narrative,[52] indicating its ability to cognitively mobilize elites lasts for less than 24 hours or 1 day (Castillo, El-Haddad, Pfeffer, & Stempeck, 2014). Hence, the hypotheses posited later in this study seek to gauge the impact of yesterday's narratives on today's cyber intrusions. Next, the research turns to the media events coding literature for assistance in deriving

[52] Half-life – the time required to realize half of the value or impact of event, element or substance undergoing a process, usually of decay or lose of effectiveness, transitioning from a period of usefulness and popularity to a period of decline or obsolescence (Webster, 2017).

explanatory variables for use in a statistical model to measure the influence today's narratives may have on tomorrow's intrusions.

3. Media Events Coding

Beginning in the mid-1960s, a group of political science scholars began manually coding daily news reports to ascertain whether the latent linguistic patterns correlated with the tenor of state-to-state relations (Goldstein, 1992). Anyone who has done qualitative research using methods described by Glaser and Strauss (1977) can attest to the laborious and tedious nature of a manual coding process. Fortunately, machine coding of media events has significantly improved with advances in computing power. Today, machine coding of media events *scrape* a billion sentences a day from over 100,000 news articles across the globe (Schrodt, 2017).[53] These scraped articles are machine-coded and stored in digital query-able databases (Goldstein, 1992; Howell, 1983; Schrodt, 2012). The data derived from this process, commonly referred to as [*media] events data*, has become increasingly reliable for measuring the level of cooperation or conflict between states (Bi, 2015; Colaresi, 2004; Goldstein, 1992; Goldstein & Pevehouse, 1997; Maness & Valeriano, 2016; Monroe & Schrodt, 2008; Monroe, Pan, Roberts, Sen, & et al., 2015; Schrodt & Gerner, 1997).

Each *scraped* article defines a dyad capturing its directionality, for example, an article describing an Iranian viewpoint (i.e., narrative) on a given issue in reference to the United States, or vice versa, forms a single dyad (Vincent, 1979, p. 47).[54] First, these articles are categorized as verbal cooperative (i.e., positive), verbal conflictual (i.e., negative), material cooperative, or material conflictual, as defined on page 11. Separately within the CAMEO coding construct, each article scraped and collected daily by the given political events database is scored on an ordinal scale of cooperation (+10) to conflict

[53] Scrape or Scrapping refers to a discrete form of machine learning or [electronic] statistical learning techniques, whereby, electronic text on a given website or set of websites is scanned for a predefined set of words or phrases; once discovered the information is extracted from the sources website and placed into a database for various uses such as, in this case, political discourse analysis (Monroe & Schrodt, 2008, p. 353; Monroe, Pan, Roberts, Sen, & et al., 2015, p. 71; Schrenk, 2012, pp. 227-237).

[54] Dyad – an interaction between two elements or parts, in this case two states or countries (Oxford Dictionary, 2015).

(–10). Essentially, the political narrative captured in each media article is measured for its tone,[55] depicting the directional tenor of narrative from cooperative to conflictual between two states. This scale of cooperative or conflictual is known as the *Goldstein score* and is commonly accepted by political scientists (Bi, 2015; Brandt, Colaresi, & Freeman, 2008; Colaresi, 2004; Goldstein, 1992; Goldstein & Pevehouse, 1997; Schrodt & Gerner, 1997; Shellman, Clare Hatfield, & Mills, 2010; Yonamine, 2001).

To date neither the number of *verbal* or *material* articles nor the *Goldstein score* or its variation have been used to develop independent variables to discern their influence on intrusion activity using a statistical regression model. This proposed model would use these explanatory variables as proxies for the gravitas or tone of media narratives generated by other states directed at the U.S. and its interests, on a given day, and their impact or influence cyber intrusion activity the following day. Thus, the model would examine the correlation relationship between the digitally recorded in the *Goldstein score* or tone, its derived variation or polarization, and the number of a state's verbal and material media narratives about the U.S. *today* and their effect on intrusion activity on U.S. networks *tomorrow*. Next, the research will explore segments of several different theories that will complete the explanation of this cyber intrusion phenomenon.

G. OTHER USEFUL THEORIES

These theories add certain elements intended to buttress and expand the overall generality of this research. Further, parts of each will be integral to regime type explorations and explanations contained in the case study chapters.

1. Digital Panopticon

As presented in the introduction, Jeremy Bentham, a 19th century social theorist, developed a prison architectural design based on a hub and spoke principle placing the guard(s) at the hub and the prisoner's cells on the spokes (Bentham, 2012; Loadenthal,

[55] Tone – a construct meant to apply a objective scale (i.e.,+10 to -10) to media narratives from cooperative (i.e.,, positive, +10) to conflictual (i.e.,, negative, -10) (Bi, 2015; Brandt, Colaresi, & Freeman, 2008; Colaresi, 2004; Goldstein, 1992; Goldstein & Pevehouse, 1997; Schrodt & Gerner, 1997; Shellman, Clare Hatfield, & Mills, 2010; Yonamine, 2001).

2018). In effect, this design subsequently created the panopticon effect describing how the individual prisoner modified their behavior, in effect self-policing, because they were never certain whether they were or were not under surveillance by the guard(s) (Bentham, 2012; Galič, Timan, & Koops, 2017; Loadenthal, 2018; MacKinnon, 2012, pp. 75-86; Manokha, 2018). In the recent era, scholars extended theory of the panoptic effect to apply to private citizens, where depending on regime type, may find themselves under varying levels (i.e., generations) of digital surveillance (Chesterman, 2011; Deibert & Rohozinski, 2010; Deibert, 2015; Foucault, 1977; Goodman, 2015; MacKinnon, 2012; Manokha, 2018). Every citizen's digital footprint regardless of device, program, or application could be under surveillance by the state or some nefarious character at any time (Chesterman, 2011; Deibert & Rohozinski, 2010; Deibert, 2015; Duffy, 2015; Gabdulhakov, 2020; Goodman 2015; Mackinnon, 2012; Morozov, 2011; Manokha, 2018; Nocetti, 2015; Ognyanova, 2018). Even the closed-circuit television (CCTV) networks ubiquitous in most large cities can, as a result of facial recognition technology, place most of their citizens under observation (Galič, Timan, & Koops, 2017; Goodman, 2015; Morozov, 2011; Manokha, 2018). Subsequently, scholars metaphorically named this omnipresent, latent, surveillance infrastructure the digital panopticon (Chesterman, 2011; Foucault, 1977; Galič, Timan, & Koops, 2017; MacKinnon, 2012; Manokha, 2018).

Most of the scholarly discussion in this arena revolve around terminology in the search for qualitative definitions to flesh out surveillance theory attempting to move beyond the metaphoric panopticon (Galič, Timan, & Koops, 2017). This research intends to focus on the surveillance or dataveillance aspects of the digital panopticon, more specifically a given regime's purpose in leveraging the digital footprints of their citizens as a means of control or power over them (Chesterman, 2011).[56] Certainly, the narrative chosen by the more repressive regimes, espousing the benefits of the digital panopticon,

[56] Surveillance – a. to watch from above; to keep a close watch over someone, b. 'sur' to watch from above, 'veillance' from above (Galič, Timan, & Koops, 2017; Webster, 2017).

Dataveillance – a. surveilling individual behavior through the intensive data trails their digital behavior generates. b. surveilling individuals through computational means and digital information, which has become easier for government entities to trace individuals or groups than was possible in the past because of the historical on heavier forms of architectural or institutional surveillance means (Clarke, 1988; Galič, Timan, & Koops, 2017, p. 29).

revolves around the protection, the safety and the security of the population or, of course, *national security* (Gabdulhakov, 2020; Galič, Timan, & Koops, 2017; Goodman, 2015; MacKinnon, 2012; Morozov, 2011; Wallace, 2008). However, this research seeks to focus on the more Orwellian side of the metaphoric digital panopticon and its use as a means of societal control (Akgül & Kirlidoğ, 2015; Chesterman, 2011; Foucault, 1977; Galič, Timan, & Koops, 2017; Goodman, 2015; MacKinnon, 2012; Morozov, 2011; Pinkaew, 2016).

2. Narrative Theory

While, the hypotheses of this research hinge on directed verbal or material narratives, narrative theory and the exploration of it is not the focus. Yet, a brief review of the pertinent parts of narrative theory for use in the explanation of this phenomenon remains useful. Specifically, the author intends to cover these few specific aspects of this theory. First, what is a narrative? Second, who and how are narratives created? Finally, how can one gauge the truthfulness or veracity of a given narrative?

Most dictionaries define narratives as stories (Webster, 2017). Stories as Hesiod observed, in the ancient Greek poem *Theogony*, by stating these narratives consist of a combination of elements of truth and *lies* that resemble truth (Herman, Jahn, & Ryan, 2005). In effect, these specifically written narratives or stories, created by humans, as interpretations of events that they themselves witnessed or they themselves recorded based on another person's interpretation of a given event, which in either case implies a unique point of view (Herman, Jahn, & Ryan, 2005; Nerone, 2015; Wake, 2009). That unique viewpoint indicates a certain *polyvocality*, a key concept of narratology, which in part means a given narrative is a story reduced from many different viewpoints on a given issue to only a few or to what fits on a page.[57] Consequently, during the reduction or synthesis process that creates a narrative, differing points of view within the story simply go unobserved, untold, or unrecorded. So, the other part of polyvocality means that any given

[57] Polyvocality – means there is *no* objective truth, *no* single official version of a story, *no* preferred interpretation or reading of the events, rather, the story is derived from many voices and multiple differing points of view from which the single narrative is created (Wake, 2009, pp. 673-677).

narrative or storyline does not inherently embody objective truth, officiality of version, or preferred understanding of the event or situation described in the narrative (Wake, 2009). Fundamentally, narratives simultaneously *reveal* and *conceal* elements of what actually occurred. Certainly, this may be due to time and space constraints in writing and constructively creating the narrative to fit into news print or a web page (Herman, Jahn, & Ryan, 2005). However, some regime types may use their influence or content control capabilities to clandestinely manipulate the information within the story attempting to control the narrative on a given issue. In the 1960s, the Soviet Union began developing doctrine to describe this form of information warfare, naming it-*reflexive control*.[58]

Reflexive control bears a significant resemblance to perception management, except that its terminology (i.e., control) and intent are acutely focused on influencing an opponent through information exploitation (Thomas, 2004). One of the means of exploitation is through use of media narratives (Inkster, 2016; Snegovaya, 2015; Valeriano, Jensen, & Maness, 2018). While many regimes do not embrace the doctrine or use the term reflexive control, their use of media manipulation and the narratives therein seems apparent and operant today (Bilgiç, 2018; Jaitner & Mattsson, 2015; Pinkaew, 2016; Snegovaya, 2015; Valeriano, Jensen, & Maness, 2018). Further, several of the regime types and countries covered in the case studies chapters use this type of tactic to control the narrative domestically and to influence the narrative internationally in their discourse directed at the U.S. Both the narrative and reflexive control theoretics fit nicely into an emergent theory, which ties them together and provides a useful term to use in explanations within this research—*Sharp Power*.

3. Sharp Power

The term sharp power springs out of the hard power and soft power lexicon, originally coined by Joseph Nye (Nye, 2007; Walker & Ludwig, 2017). A state using hard

[58] Reflexive Control – explains the use of tailored information (i.e., media narratives) that would influence an opponent or rival to voluntarily make the pre-determined decision created, framed, and preferred by the preparer or originator (a.k.a., opposing state in a conflictual dyad) (Thomas, 2004, pp. 237-238; Valeriano, Jensen, & Maness, 2018, pp. 113-114). While similar to perception management, reflexive control focuses on *control* of the subject – in this case public opinion of a state or the civil society within a target country (Thomas, 2004, p. 237).

power relies upon the military or economic instruments of national power to coerce other nations to act in their state's national interest (Walker & Ludwig, 2017). Whereas, soft power uses attraction and persuasion to obtain the desired behavior or outcome (Nye, 2007; Walker, Kalathil, & Ludwig, 2020; Walker & Ludwig, 2017). Soft power leverages the diplomatic and informational instruments of national power. While sharp power appears to rely solely on the *informational* instrument intent on bending the narrative to tell their chosen story (Walker, Kalathil, & Ludwig, 2020; Walker & Ludwig, 2017).

A nation wielding sharp power relentlessly uses their influence across multiple domains including academia, media, politics, think tanks, and civil society to tell their narrative and paint their intentions as just and true. Drawing out and highlighting the positive, while censoring or neutralizing the negative story.[59] The country employing sharp power intends to pierce, penetrate, or puncture any competing narrative that does not align with their own and may leverage third and fourth generation internet content controls to ensure their storyline dominates all others (Custer, Prakash, Solis, Knight, & Lin, 2019; Deibert, 2015; Deibert & Rohozinski, 2010; Maréchal, 2017; Nocetti, 2015; Ognyanova, 2018; Walker & Ludwig, 2017; Zittrain et al., 2017). Finally, achieving the goal of general acceptance of their chosen narrative, which is not time based—it takes as long as it takes (Walker & Ludwig, 2017). Generally, the use of sharp power falls to autocratic or autocratic leaning countries, who tend to prefer it as a means to prey upon and to take advantage of the open cyberspace, media, and political structures that epitomize democracies (Custer et al., 2019; Deibert, 2015; Marcellino, Marcinek, Pezard, & Matthews, 2020; Maréchal, 2017; Nathan, 2017; Nocetti, 2015; Paul & Matthews, 2017; Strovsky, 2015; Walker, Kalathil, & Ludwig, 2020; Walker & Ludwig, 2017).

[59] For example, in October 2019 when Wikipedia, the crowdsourced and edited online encyclopedia, received thousands of edits from Mandarin language sources editing the 1989 Tiananmen Square massacre webpage, changing the description to an "incident" to "quell counter-revolutionary riots." Similarly, the description of Taiwan was redefined to "a province in the People's Republic of China (PRC) (Miller, 2019; Walker, Kalathil, & Ludwig, 2020). Or in the same month, when Daryl Morey, general manager of the Houston Rockets basketball team, sent out a tweet in support of the protestors in Hong Kong. Morey drew the ire of the PRC sponsored netizens effectively condemning his statement, eventually leading the Chinese basketball association, state and online media to cut sponsorship of the Houston Rockets (Cook, 2019; Walker, Kalathil, & Ludwig, 2020).

Accordingly, sharp power and its tendrils into reflexive control and narrative theory make it useful in the explanation of the two-level process as well as the two-step process nested within it. First, reflexive control and sharp power may operate at level-one by state X attempting to ensure the resilience of their chosen win-set narrative while engaged in *verbal* negotiations with the U.S. Second, the ability of an anocracy or autocracy to wield sharp power, perhaps using reflexive control, to manipulate the narrative implies that state X exercises enough societal control via the digital panopticon, enabled by generational controls, to ensure their citizen's support the win-set narrative during the verbal phase of the negotiations. Finally, this indicates that state X may exercise some level of internet content control over the domestic storyline and that state elites have communicated the need to support the win-set narrative to their citizens during the verbal phase. Again, this suggests that the two-step process operates within level-two supported by strong content controls, thereby controlling the domestic narrative in state X. Thus, the digital panopticon, narrative theory, and sharp power may prove useful when explaining how media narratives may impact cyber intruders residing in different countries and ruled by different regime structures.

H. DERIVING OBSERVABLE IMPLICATIONS

When taking this literature review in its entirety, one might question how could this research be scoped to derive some observable implications to either accept or reject postulated hypotheses concerning how media events influence cyberspace activity? First, the research must consider the data available, which consists of 302 days of cyber intrusions cataloged by SNORT intrusion detection software and scraped media events captured in the Phoenix data set. Second, by exposing this available data to a statistical model, the research could discern if yesterday's media events have an observable impact on today's cyber intrusion activity on U.S. servers. Finally, if a relationship did exist, this could provide evidence of the operation of the two-step process functioning within level-two—domestic media narratives. Wherein, a given society's elites monitor and digest the domestic narrative, derive a position on the varying issues, and communicate it to the population.

The two-step process implies that the population is cued by the elites and may adopt their position; however, it does not describe how the triggered hacker's position or their associations within society may on one end of the spectrum *mobilize* them to engage in hacktivist behavior manifesting either subversive or information-seeking intent (Aelst, 2017; Newton, 1999). While, on the other end of the spectrum these signals from elites, social movements, or state-sponsors may lead to *malaise* behavior amongst hacktivists leading to on-line disengagement (Aelst, 2017; Newton, 1999). As discussed in the introductory chapter based on the existing literature, these hacktivists would fall into three distinct bins within society, the elite triggered or non-triggered citizen, the hacktivist affiliated with a social movement led by an elite cabal, or the state-sponsored intruder (Aelst, 2017; Anderson & Sadjadpour, 2018; Best & Higley, 2018; Biçakci, Doruk, & Mitat, 2015; Calamur, 2017; Deibert & Rohozinski, 2010; Denning D. E., 2011; Goodman, 2015; Keck & Sikkink, 1998; Kello, 2013; Lindsay, 2014; McAdam, McCarthy, & Zald, 1999; MacKinnon, 2012; Newton, 1999; Nye, 2011; Pinkaew, 2016; Singer & Friedman, 2013; Sinpeng, 2013; Snegovaya, 2015; Thorton & Miron, 2019; Valeriano & Maness, 2015; Valeriano, Jensen, & Maness, 2018).[60] Further, hacktivists may reside or receive signals within each or any combination of these bins. While the triggering elites may be

[60] Social Movement Theory seeks to explain how political opportunities arise, how they are framed, and how resources are mobilized resulting in some form of collective action to achieve the movement's goal – to challenge government policies, to change civil societies behavior, attitudes, or value systems, or to draw attention to a social injustice. This paper utilizes a broad definition of Social Movement Theory based on analysis and synthesis of the extant related literature. See (McAdams, McCarthy, & Zald, 1999; McAdams, Tarrow, & Tilly, 2001) for an overall review of Social Movement Theory and its associated elements of political opportunities, mobilizing structures, and framing processes. See (De Tocqueville, 1856; Tarrow, 1996) for political opportunities. For political framing, see (Benford & Snow, 2000; Gamson & Meyer, 1999; McAdams, 1999). See (Carroll & Hackett, 2006; McCarthy & Zald, 1977).for resource mobilization. See (De Tocqueville, 1955; De Tocqueville, 2002) for challenges to government policies. See (Bayat, 2005; Keck & Sikkink, 1998) for changes in civil society. See (De Tocqueville, 1955; De Tocqueville, 2002; Keck & Sikkink, 1998) for drawing attention to a social injustice.

An example of a social movement would be the virtual sit-in by a group of hacktivists. In 1998 a group of social movement activists wanted to draw attention to the plight of the indigenous Zapatista population of Chiapas, Mexico. The Zapatista's are subsistence farmers whose culture rested upon their access to their ancestral lands. The Mexican Government was attempting to comply with the requirements of the North American Free Trade Agreement (NAFTA) began forcibly removing the Zapatista's from their land, which led to an armed uprising by the Zapatistas. Approximately, 10,000 hacktivists who viewed this as a human rights violation by the Mexican government conducted a virtual sit-in of the websites of the President of Mexico, the President of the United States (US), the U.S. Pentagon, the Mexican Stock Exchange, and the Frankfurt Stock Exchange delivering 600,000 queries per minute on each website (Denning, 2001, pp. 12 & 73). Although, the virtual sit-in did not permanently damage the servers involved, it did garner media and drew global attention to the Zapatista cause.

affiliated or unaffiliated with these distinct groupings, their impact on hackers, residing in or amongst these bins, may be a product of the conjectured two-step flow operating as a result of the domestic narrative as depicted in Appendix C (Best & Higley, 2018; Conceição-Heldt & Mello, 2017; Higley & Burton, 2006; Higley, 2018; Lazarsfeld, Berelson, & Gaudet, 1944; Putnam, 1988; Strong, 2017).

Therefore, the statistical model explanatory variables will specifically focus on the daily counts of negative material and verbal narratives, the negative narrative tone, and the tone variation. The research intends to gauge today's media events in relation to the following day's intrusions, which provides an excellent construct to test the proffered hypotheses to engender a better understanding of this phenomenon. The hypotheses offered in Figure 4 will be tested using statistical methods to discern if they operate in the real world. Finally, if the statistical evidence does not support the acceptance of a given hypothesis, this demonstrates a failure to reject the null hypothesis. The statistical evidence provided fails to rise to the level necessary to reject the null, meaning the evidence provided does not support the existence of the hypothesized relationship.

Hypothesis #1 (H1): *Increases* in the number of conflictual *material* interactions reported in the media narratives of other sovereign states directed at the United States (US) and its interests—yesterday, regardless of regime type, results in *increased* cyber intrusion activity on U.S. networks—today.

Hypothesis #2 (H2): *Increases* in the number of conflictual *verbal* interactions reported in the media narratives of **democratic** states directed at the United States (US) and its interests—yesterday, results in *increased* cyber intrusion activity on U.S. networks—today.

Hypothesis #3 (H3): *Increases* in the number of conflictual *verbal* interactions reported in the media narratives of **anocratic** states directed at the United States (US) and its interests—yesterday, results in *no change* in cyber intrusion activity on U.S. networks—today.

Hypothesis #4 (H4): *Increases* in the number of conflictual *verbal* interactions reported in the media narratives of **autocratic** states directed at the United States (US) and its interests—yesterday, results in *decreased* cyber intrusion activity on U.S. networks—today.

Hypothesis #5 (H5): *Increases* in the variation of negative narrative tone, indicating an increased level of media polarization, across media stories originating from **democratic** and **anocratic** states directed at the U.S. and its interests—yesterday, results in *decreased* in cyber intrusion activity on U.S. networks—today.

Hypothesis #6 (H6): *Increases* in the variation of negative narrative tone, indicating an increased level of media polarization, across media stories originating from **autocratic** states directed at the U.S. and its interest—yesterday, results in *increased* cyber intrusion activity on U.S. networks—today.

Hypothesis #7 (H7): *Increases* in the accumulated conflictual or negative *tone* of interactions reported in media narratives from other countries directed towards the United States (US) and its interests—yesterday, results in *decreased* cyber intrusion activity on U.S. networks—today, with the effect becoming stronger as the level of democracy of the originating country *increases*.

Figure 4. Main and Conditional Hypotheses

Further, the researcher seeks to proffer a conditional hypothesis to be tested through the use of a first-order interactive term. The author suspects that there is interaction between the negative narrative *tone* variable or Goldstein Mean and the Level of Democracy (i.e. Polity score) or H7. As such, Figure 4 above provides a listing of the hypotheses to be tested in this study.

Therefore, the statistical model explanatory variables will specifically focus on the daily counts of negative material and verbal narratives, the average daily negative narrative (NN) tone and variation, and the interaction between average NN tone and levels of democracy. The research will gauge today's media events in relation to the following day's intrusions, which provides an excellent construct to test the proffered hypotheses ultimately to engender a better understanding of this phenomenon.

I. CONCLUSION

This literature review began with a discussion of the cyber intrusion phenomenon, discussing the efficacy of the cyber-attack narrative and its effect. Ultimately concluding that the media label of cyber-attack, while apocryphal and sensational intent on capturing the public's attention, entirely misses the mark in its description of the actual cyber-event best described as an intrusion. Next, the review covered the origin of the internet, how it operates, and how its various layers interact, concluding with an understanding of how it functions. The goal here was to introduce the layering terminology for future use. Finally, the section concluded with how IP anonymizers and TOR make anonymity on the internet a reality, which makes identification of an intrusion's origin suspect at best and something that should be kept in mind throughout the execution of the research.

Next, the review covered much of the extant conflict and rivalry literature and its consistent causes, meaning these situations usually begin as territorial, but then progress or are reinforced by significant cultural, ethnic, or religious overtones and normally persist as regional issues. Meanwhile, conflict observed in cyberspace remains quite restrained; simultaneously, a lot of rivalrous activity permeates this space where gaining the attention of the state opposite the cyber antagonist or rival in the dyad is the intent. Further, these antagonists use this rivalrous cyber jostling to coerce, compel, or pressure the target state into making some policy or behavioral change. Finally, these cyber antagonists appear to gain access to the physical or semantic layers of cyberspace via the syntactic. The syntactic is the layer of computer language, code, instruction, and syntax, which enables the internet to function properly.

Subsequently, a typology was created, based on the work of Valeriano, Jensen, and Maness (2018), to describe this rivalrous behavior in cyberspace as either subversive or information seeking intent via a malicious vector. This malicious vector comprises approximately 82% of the cyber incidents identified between 2000 and 2014; additionally, this vector appears to be the catalyst or gateway into the execution of information seeking or subversive intent. Thus, it appears appropriate to place cyber intrusion activity within this duo of types.

Next, the research delved further into the theoretical realms seeking to create an explanation of why these cyber intrusions occur. First, the author reviewed Putnam’s Two-level International Relations Theory covering how a state’s decision makers must manage both the international (i.e., Level-one) and domestic narratives (i.e., Level-two), simultaneously, when engaged in negotiations with another state. Second, the researcher discussed how the power of elites varies within these and how the influence of their voices varies across regime types. While democracies contain a multiplicity of elitist voices, autocracies accommodate far less. Thus, within autocracies those *few* elites have an inordinate amount of power and influence; while, in democracies elites’ power and influence is diffuse. Further, the review covered the generational level of cyberspace content controls, with anocracies bypassing the first preferring to focus on second and third generation controls, while autocracies tend to employ all three in tandem.

Subsequently, the research surveyed the two-step flow theory of communications and posited its operation inside of two-level theory of international relations. The two-step flow surmises that elites read the daily narrative, espouse an interpretation of the veracity of the storyline, and ultimately, relay their view of the narrative to surrogates in the state’s population. This research intends to test this conjectured operation of the two-step process within level-two by using negative material, verbal, tone, and variation of media events captured on a given day to gauge their impact on cyber intrusions on the following day.

Next, the research introduced the digital panopticon, narrative, and sharp power theories for possible use in explaining the nuances of the two-step process operating in domestic (i.e., level-two) narratives as it pertains to differing regime types and countries.

Some portions of each of these theories will facilitate the case study explanations based on the results of the statistical model, introduced in the next chapter.

Finally, this chapter provided a set of classifications within which the hacktivist might reside. Specifically, establishing the categories of the elite triggered hacktivist, who could be an average citizen, a member of a social movement group, or a state-sponsored intruder. Ultimately, arriving at a set of hypotheses to be tested, using the model described in the next chapter. The conjectured difference between verbal rhetoric and material action may possesses a certain gravitas within negative narratives. Further, increases in negative narrative tone variance may lead to a dampening effect on the following day’s intrusions activity. While, the interaction between tone and regime type (i.e., level of democracy or polity score) may result in decreasing levels of intrusions as the set of countries becomes more democratic. In short, this review covered the literature germane to cyber intrusion phenomenon seeking to create the framework to explain and to better understand if today’s negative media events, directed at the U.S. by other countries, affect tomorrow’s cyber intrusions on U.S. networks.

THIS PAGE INTENTIONALLY LEFT BLANK

III. MODEL DESIGN: MEDIA EFFECTS IN CYBERSPACE

A. INTRODUCTION

As stated in the design section of the introductory chapter, the first few explanatory variables chosen to test against the response variable of intrusions per country, per day were intuitive given the hypotheses proposed. Initially, this chapter shall develop the explanatory variables using the events coding data drawn from in the Phoenix Data set, which uses the CAMEO coding ontology for scraped articles. All of the variables used in the model will conform to a per country, per day or *per* country-day unit of analysis; however, most control variables used do not exist in this format (i.e., per capita Gross Domestic Product, population size, internet penetration rate), and as such will remain constant for each day of the year.

First, this chapter reviews how the cyber intrusion data was captured and discuss the derivation of the cyber-intrusions per country-day dependent variable. Second, a brief summary is given of how the media events and control variables were derived and how they will be used to create the country-day unit of analysis for each model, when possible. Third, this chapter formulates the macro models encompassing all negative and positive tone narratives originating from countries opposite the U.S. in dyadic dialog to choose the best fitting probability distribution model (i.e., Gaussian, Poisson, negative binomial, etc.). Then, the model refocuses on negative narratives and particular regime-types and countries. This refocusing will include the modification of the *tone* variable to incorporate only conflictual or negative narratives and the development of an interactive variable to gain a better understanding of what relationships that may assist in gaining better insights for explanation. Next, the research applies the model to specific regime types (i.e., democracies, anocracies, autocracies) that project negative narratives toward the U.S. Finally, the chapter tests the posited hypotheses using the evidence provided by each model to discern whether the evidence supports or does not support each given hypothesis by regime type using the All-Regime’s NN model.

Per their request, the cyber-intrusion data source shall remain anonymous. The source drew the data set from a single representative, internet facing, U.S. Government server equipped with SNORT intrusion detection software. Properly configured, SNORT intrusion detection software catalogs the last IP address or IP node from which the intrusion originated (Beale, Foster, Posluns, & Caswell, 2003; Cavusoglu, Mishra, & Raghunathan, 2005; Rehman, 2003). Again, with the advent of TOR, or The ONION Router, and IP anonymizers the actual origin may remain suspect.

The data set contained two unbroken date ranges. The first from 02 January 2015 to 06 May 2015 (124 days) and the second 12 September 2016 to 18 March 2017 (178 days); thus, providing 302 days of intrusion data in two separate sets. Explicitly, this research focuses on the date, the country of origin, the intrusion risk indicator, and the day of the week that the intrusion occurred. This SNORT data was used to derive an intrusions per day dependent variable using the R programming language. Though the same process and language, all of the independent variables were derived and *lagged* by a day to gauge their impact on the following day's intrusion activity.

In addition, day of the week control variables were derived from the intrusions data set. The researcher enumerated the days of the week (e.g. 1 = Monday, 2 = Tuesday, etc.), based on the date provided in the data set, and then convert these to dichotomous indicators. This allowed for the control of differences across days of the week. Further, a control variable for the month of the intrusion was created to take account of monthly fluctuations in intrusion attempts, as well.

B. MEDIA-EVENTS VARIABLES

Initially, the proxy for the average daily media narrative *tone* using the Goldstein mean (**Gold_Mean**) and its daily standard deviation, or level of narrative *polarization*, were computed. This enabled the derivation and measurement of the daily media tone mean value and variation *yesterday* relate to cyber intrusion attempts—*today*. Or to state it another way, to gauge the effect of today's media events on tomorrow's intrusions.[61]

[61] Both of these ways of describing the relationship between the response and explanatory variables will be used throughout this text.

Next, a control variable summing up the total narratives count (**Total Narratives**) was created, summing up all narratives negative or positive across all narrative categories in the unit of analysis, as described in the control variables section below. This control variable captures all the narratives, regardless of whether positive or negative, material or verbal. As with the other control variables, the research intends to account for the effects of other narratives on the dependent variable. Thus, allowing the research to focus specifically on the negative *material* and *verbal* narratives—yesterday to gauge their impact on the total intrusions—today. As many of these daily narratives and types are skewed toward zero with some significant statistical outliers, each will be logarithmically transformed as is common practice to reduce the impact on the model validity. Next the Gold_Mean variable was multiplied by the given country's polity score to create the first-order interactive term **Gold_Mean *x* Polity**.

Thus, by using these five explanatory variables (i.e., negative *material* and *verbal* narrative, *Gold_Mean* (narrative tone), *Gold_SD* (narrative polarization), and Gold_Mean *x* Polity, while controlling for day and month of the intrusions and narratives, lays the foundational work to develop the statistical inference model required to test the hypotheses.

C. CONTROL VARIABLES

The remaining balance of the control variables is collected and included in the model, by country. These variables include total narratives, total intrusions, internet and media freedom, media self-censorship, regime type (i.e., polity score and polity squared), internet penetration rate, population, gross domestic product (GDP), day of the week and month of intrusions. Thus, the regression model takes shape as shown in Equation 1, with the explanatory variables in **bold** and the control variables shown in plain type.

$$
\begin{aligned}
&\textbf{TotalIntrusion}_{\textbf{Today}\ (\textbf{Lead})}\\
&\quad = \ \textbf{Log}\ (\textbf{Negative Material Narratives})_{\textbf{country-day}}\ (\text{NmN})\\
&\quad + \textbf{Log}(\textbf{Negative Verbal Narratives})_{\textbf{country-day}}\ (\text{NVN})\\
&\quad + \textbf{Gold}_{\textbf{Mean}\ \text{country-day}}\ (\text{Narrative Tone})\\
&\quad + \textbf{Gold}_{\textbf{SD}\ \text{country-day}}(\text{Narrative Polarization or NNp})\\
&\quad + \left(\textbf{Gold}_{\textbf{Mean}\ \text{country-day}}\ x\ \textbf{Polity}_{\ \textbf{country-year}}\right)\ (\text{Tone Interaction})\\
&\quad + \text{Log}(\text{TotalNarratives} + 1)_{\ \text{country-day}}\\
&\quad + \text{Log}(\text{TotalIntrusions}_{\text{Yesterday}} + 1)_{\ \text{country-day}}\\
&\quad + \text{Polity}_{\ \text{country-year}}\ (\text{level of democracy}) + \text{Polity squared}\\
&\quad + \text{InternetNotFree}_{\ \text{country-year}} + \text{MediaNotFree}_{\ \text{country-year}}\\
&\quad + \ \text{MediaSelfCensor}_{\ \text{country-year}} + \ \text{InternetPenetrationRate}_{\ \text{country-year}}\\
&\quad + \text{Log}(\text{Population} + 1)_{\ \text{country-year}} \ + \text{Log}(\text{GDP}_{\text{inUSdollars}} + 1)_{\text{country-year}}\\
&\quad + \ \text{Day of Week} + \text{Month} + \ \text{Constant}
\end{aligned}
$$

Equation 1: Macro Statistical Model

First, total narrative—yesterday, regardless of whether they were negative or positive, material or verbal and total intrusions, were captured to account for their impact. The control of these should be straight forward because the aim is to ascertain and then quantify the relationship between today's narratives and tomorrow's intrusions. Second, the research sought to control for a host of country specific parameters beginning with polity or regime type (i.e., democracy, anocracy, or autocracy) capturing both its raw score and its potential polynomial effect.[62] Third, internet and media freedom, media self-censorship, internet penetration rate, population, gross domestic product (GDP), and finally

[62] Polity – the design or constitution of a politically formed state or country; in this context it means to describe the form of governing institutions spanning from Democracies, to mixed governments such as Anocracies, through to totalitarian regimes or Autocracies (Polity IV, 2018; Webster, 2017).

the day of the week and month in which both the narrative and intrusion took place.[63] The polity variable leverages the Polity IV (2018) data, which ascribes yearly scores to countries between +10 and +6 as democracies, +5 through –5 as anocracies, and –6 through –10 as autocracies.[64]

Finally, the research sought to control for each country's level of internet and media freedom. These control variables were drawn from the V–Dem database that contained country variables for both internet and media freedom and for media self-censorship (V-Dem Institute, 2019, pp. 185-188). The V–Dem assigns a scaled variable for each, which was modified to derive a binary (i.e., dichotomous) variable denoting free or no self-censorship as a zero (0) and not free or media self-censorship as a one (1).

Next, the model will be exposed to different statistical regression model types (i.e., normal, Poisson, negative binomial, hurdle, and zero-inflated) to ascertain which model provides the best inferential value. Then, the author intends to use the model at different levels of analysis to test the hypotheses offered throughout the remainder of this dissertation.

D. MEDIA EFFECTS MODEL

In the previous sections, the dependent, various independent, and control variables necessary to test the hypotheses were described. Using R, the data was broken into the country-day unit of analysis deriving some 44,545 *macro-level* observations across the period of analysis. As one might imagine the data varies greatly not only between countries, but also across regime types with lots of country-days where zero intrusions and/or media

[63] The internet and media freedom, media self-censorship, population, and gross domestic product (GDP) were drawn from the V-Dem data set (V-Dem Institute, 2019). Further, since scholarly evidence exists that implies media sources in some regime types and countries – self-censor, the media self-censorship control variable was added from the V-Dem source, as well (Asmolov, 2016; Baarda, 2017; Deibert & Rohozinski, 2010; Gabdulhakov, 2020; Galič, Timan, & Koops, 2017; Manokha, 2018; Maréchal, 2017; Nocetti, 2015; Ognyanova, 2018; , V-Dem Institute, 2019, Zhukov & Baum, 2016).

Gross domestic product is a measure the output of all labor and capital within the geographical boundaries of a country, regardless of the residence of that labor or owner of the capital (Anderson, 1993). Current dollars – in this context reflects the dollar value of GDP in the year generated. The internet penetration rate was drawn from the World Bank, World Development Indicators data set (The World Bank, 2019).

[64] Democracies range from +10 to +6, Anocracies from +5 to -5, and Autocracies from -6 to -10.

events were recorded in the data. It seemed best to begin the testing of this macro-level data set with a baseline (Gaussian) normal distribution, even though its main use is for modeling continuous measurements and does not necessarily fit the discrete data set. Subsequently, the research focused on the discrete models from basic Poisson and negative binomial to hurdle and zero-inflated models.[65] Appendix D, provides the statistical output for all *eleven* models in tabular format for comparison purposes. Through review of the models arrayed, the original Poisson distribution represents the regression variables accurately and delivers the lowest mean average and root mean square error score (MAE & RMSE) from the 20% test sample held out from the observations used to estimate the models.[66] Taken together these statistical tests signify that the Poisson distribution model provides the highest out-of-sample predictive accuracy, and therefore the most useful information for testing the hypotheses. Further, since the observed intrusion data follows a discrete (count) unit of measurement, it made sense to use the best fitting discrete model.

[65] Hurdle models fit the count variables into a Poisson, negative binomial, or geometric distribution, while fitting the zero counts into a binomial or censored count distribution (Zeileis, Kleiber, & Jackman, 2015). This allows all the data to be considered vice the abnormal amount of zeroes skewing the data; thereby, inhibiting proper analysis. Econometric models originally employed the hurdle concept; however, other areas of study look to employ this statistical structure to buttress their scientific endeavors.

Zero-inflated models provide, yet, another option for handling excess zeroes. The zero-inflated model structure breaks the data into a two-component mixture structure. Modeling the zeroes as a point mass using a binary or Bernoulli distribution, while modeling the count variables as a Poisson, a negative binomial, or a geometric (Zeileis, Kleiber, & Jackman, 2015).

[66] Mean Absolute Error (MAE) – is the measure of the average absolute difference between the actual and model predicted values (Levine, Berenson, & Stephan, 1998, pp. 690-693). Root Mean Square Error (RMSE) – is the square root of the mean difference between the observed values of the data and the model’s predicted values. Both metrics provide an indication of how well the model predicts the response. The lower the MAE or RMSE the better the explanatory variables predict the response variable (Ludecke, 2019, p. 19).

p-value – the *observed level of significance* indicates the probability of obtaining a result or test statistic equal to or more extreme than the one obtained from the sample data, which may or may not support the null hypothesis or H_0 (Kerlinger & Lee, 2000; Levine, Berenson, & Stephan, 1998). For example, if the probability is high (i.e., p < 0.1), provides weak evidence *against* rejecting the null hypothesis, because the probability of drawing a test statistic or result equal to or more extreme than the current coefficient is 1 in 10 or 10%. While, if the probability was low (i.e., p < 0.01) offers stronger evidence for rejection of the null at a probability of 1% or 1 in 100. This observed level of significance indicates that the probability of deriving a coefficient value equal to or more extreme than the value derived is less than 1% under the null hypothesis; therefore, supporting rejection of the null and acceptance of the conjectured hypothesis. In general, a p-value of 0.05 (~5%) or less would allow for acceptance of the proffered hypothesis and rejection of the null. In this case, p-values shown in the bottom right hand corner of statistical output tables denotes the p-value in number of asterisks (i.e., *p < 0.1, **p < 0.05, or *** p < 0.01). These asterisk values lie to the right of each of the independent variables in the statistical tables indicating the probability discussed here (Levine, Berenson, & Stephan, 1998, pp. 348-349).

In other words, either an intrusion occurred and was counted today, which may or may not have coincided with a counted media event yesterday. This fact warrants using a discrete model structure (i.e., Poisson, negative binomial, geometric, etc.). Thus in this case, the Poisson provides the best fit as shown in the second column of Appendix D, with the tone, negative material, and verbal narratives described in Figure 5.

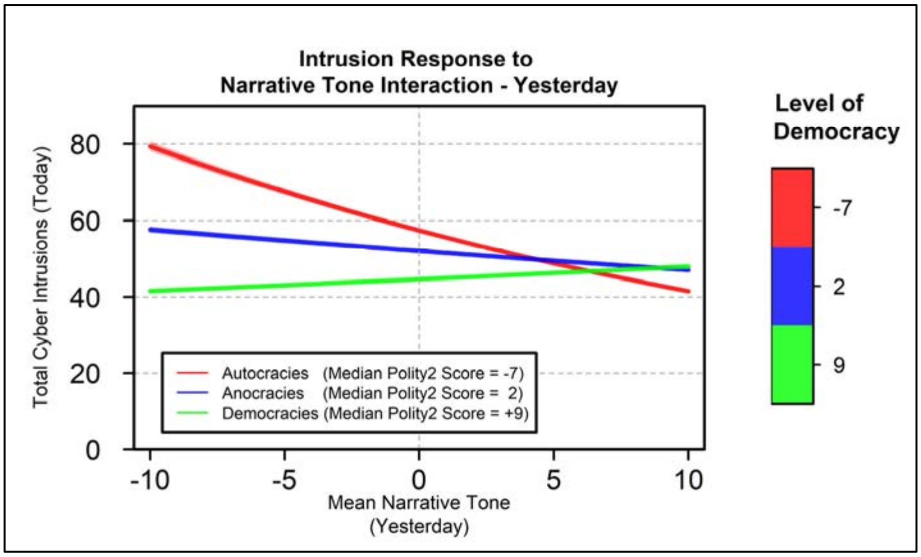


Figure 5. Narrative Tone Results

Both Figure 5 and the table in Appendix D reveal some interesting characteristics drawn out by analyzing this data set with the *macro* model. First, the *red* line compares the positive and negative *tone* of all media narratives reported by all countries with a polity score of –7 directed at the United States over the period of analysis.[67] Each line in Figure 5 represents the multiplicative interaction between narrative tone and each set of countries level of democracy (i.e., Polity score).[68] Notice how the *red* and *blue* lines pitch up when moving right to left from positive narrative tone to negative, while the *green* line decreases across the same range. Thus, as the *tone* of yesterday's narratives transitions from very

[67] These countries include Azerbaijan, Belarus, China, Cuba, Eritrea, Iran, Kuwait, Laos, and Vietnam as shown in Appendix G.

[68] This is because their product (i.e., narrative tone and polity) creates the first-order interactive term, which shows impact of yesterday's narrative tone on today's intrusions as the level of democracy changes.

positive (+10) on the right to negative (–10) on the left, intrusion attempts increase—*today* from autocracies and anocracies, while intrusions coming from democracies decrease as narrative tone becomes progressively negative.

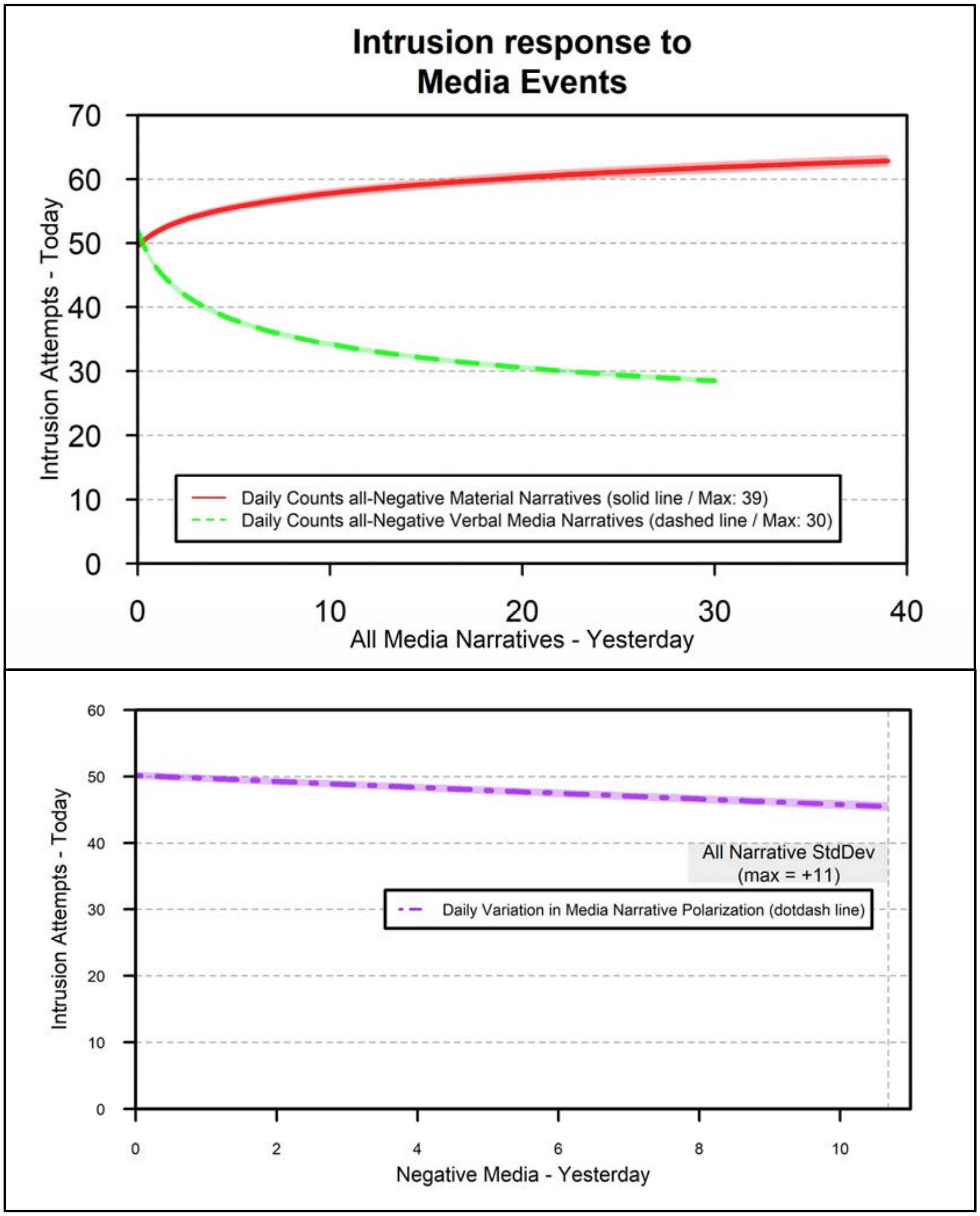


Figure 6. Media Results: Macro Model

The *red* (Negative *Material* Narratives) and *green* (Negative *Verbal* Narratives) appear to have an impact on intrusions attempts-*today*. As Figure 6 indicates as the number of yesterday's negative material narratives increases a corresponding increase in today's intrusions result, while negative verbal narratives record the opposite effect as their count increases. Finally, increases in yesterday's media tone variation, indicating narrative polarization depicted in the *purple* line, appears to score a negative impact on today's intrusions.

E. EVIDENCE OF MEDIA EFFECTS IN CYBERSPACE

Unlike the *macro* model above and in Appendix D, which was useful in deciding on the correct model to apply, the research now turns to focus on how the *negative* narratives (NN) types, tone, and polarization *yesterday* influence intrusion attempts *today*, as posited in the hypotheses. Simply, because the hypotheses focus on the negative narratives, the research going forward will emphasize the *negative* range of the narrative tone score, vice the entire range used in the all-narratives (i.e., macro) model that ranged from positive to negative discussed in the previous section. As such, the coefficients for narrative tone will focus on those days with dominant negative narratives emanating from the given set of countries. This change in research focus is highlighted by the change in narrative direction, specifically focusing on the NN tone, NN polarization, and the negative tone interaction term in Equation 2.

Equation 2 with the results shown in Table 5 encompasses the explanatory variables that comprise the focus of this research going forward from the All-Regimes negative narratives model to specific regime types across this period of analysis. Each column of Table 5 shows the *explanatory* variables of interest and their coefficient values in relation to the dependent variable. The numbers in parentheses below each of the coefficients describe the standard error over which, plus or minus, the derived coefficient varies. Thus, Table 5 provides information to explore the dyadic relationship between the negative narratives of a given country or set directed at the United States *yesterday* and its impact on intrusion attempts on U.S. networks *today*.

$$\begin{aligned}
&\mathbf{TotalIntrusion}_{\mathbf{Today\ (Lead)}} \\
&= \text{Log (Negative Material Narratives)}_{\text{country-day}}\ \text{(NmN)} \\
&+ \text{Log(Negative Verbal Narratives)}_{\text{country-day}}\ \text{(NVN)} \\
&+ \mathbf{Gold}_{\mathbf{Mean}\ \text{country-day}}\ \textbf{(Negative Narrative Tone)} \\
&+ \mathbf{Gold}_{\mathbf{SD}\ \text{country-day}}\textbf{(Negative Narrative Polarization or NNp)} \\
&+ \left(\mathbf{Gold}_{\mathbf{Mean}\ \text{country-day}}\ \boldsymbol{x}\ \mathbf{Polity}_{\text{country-year}}\right)\ \textbf{(Negative Tone Interaction)} \\
&+ \text{Log(TotalNarratives} + 1)_{\text{country-day}} + \text{Log(TotalIntrusions}_{\text{Yesterday}} + 1)_{\text{country-day}} \\
&+ \text{Polity}_{\text{country-year}}\ \text{(level of democracy)} + \text{Polity squared} \\
&+ \text{InternetNotFree}_{\text{country-year}} + \text{MediaNotFree}_{\text{country-year}} \\
&+ \text{MediaSelfCensor}_{\text{country-year}} + \text{InternetPenetrationRate}_{\text{country-year}} \\
&+ \text{Log(Population} + 1)_{\text{country-year}} + \text{Log(GDP}_{\text{inUSdollars}} + 1)_{\text{country-year}} + \text{Day of Week} \\
&+ \text{Month} + \text{Constant}
\end{aligned}$$

Equation 2: Statistical Model: Negative Narratives

This analysis of *yesterday's* negative narratives reveals that as the number of negative *material* narratives generated by other countries about the U.S. and its interests—increases, a corresponding increase in intrusion attempts *today* on U.S. networks from those countries will result. Therefore, at this level of analysis, it does appear that increasingly negative narratives describing *material* interactions between the U.S. and other sovereign states *today* results in greater cyber intrusion activity on U.S. networks *tomorrow.* As such, at this level of analysis and across these regime types, evidence exists to accept H1 and reject the null hypothesis across all regime types depicted in separate columns in Table 5.[69]

[69] **Hypothesis #1 (H1):** *Increases* in the number of conflictual *material* interactions reported in the media narratives of other sovereign states directed at the United States (U.S.) and its interests—yesterday, regardless of regime type, results in *increased* cyber intrusion activity on U.S. networks—today.

Table 5. Results of Negative Narratives Models, across Regime-Types

CYBER INTRUSION ATTEMPTS (Negative Narratives)				
	Dependent Variable			
	Total Intrusions – Today			
Independent	*Poisson Model*			
Variables (Yesterday)/Model	All- Regimes	Democracies	Anocracies	Autocracies
Negative Material Narratives	**0.03*****	**0.03*****	**0.10*****	**0.14*****
	(0.002)	**(0.004)**	**(0.005)**	**(0.002)**
Negative Verbal Narrative	–0.24***	0.08***	0.0000	–0.23***
	(0.002)	(0.004)	(0.005)	(0.002)
NN Gold_Mean (Tone)	**–0.003*****	**0.23*****	**–0.001**	**–0.21*****
	(0.001)	**(0.01)**	**(0.001)**	**(0.02)**
Gold_SD	–0.01***	–0.03***	–0.02***	0.04***
	(0.001)	(0.001)	(0.002)	(0.001)
Polity	**–0.01*****	**0.77*****	**–0.01*****	**–2.75*****
	(0.0001)	**(0.02)**	**(0.001)**	**(0.05)**
Polity squared	–0.001***	–0.04***	–0.01***	–0.21***
	(0.0000)	(0.001)	(0.001)	(0.003)
Internet Not Free	**0.12*****	**0.08*****	**–0.29*****	
	(0.003)	**(0.005)**	**(0.01)**	
Media Not Free	–0.21***	–0.12***		
	(0.003)	(0.003)		
Media Self-Censorship	**0.08*****	**0.04*****	**3.50*****	
	(0.003)	**(0.003)**	**(0.45)**	
Friday	0.22***	0.29***	0.56***	0.17***
	(0.002)	(0.003)	(0.01)	(0.004)
Saturday	**0.12*****	**0.07*****	**0.28*****	**0.19*****
	(0.002)	**(0.003)**	**(0.01)**	**(0.004)**
Sunday	–0.32***	–0.27***	–0.29***	–0.31***
	(0.003)	(0.004)	(0.01)	(0.005)
NN GoldMean *x* Polity	**0.002*****	**–0.03*****	**0.01*****	**–0.03*****
	(0.0001)	**(0.001)**	**(0.0004)**	**(0.003)**
Constant	–4.49***	–5.99***	–11.69***	–13.75***
	(0.03)	(0.10)	(0.47)	(0.20)
Observations	40,608	24,126	10,071	5,184
MAE	36.9	22.2	15.7	137.1
RMSE	581.0	202.8	118.9	1,309.9
AIC	2,512,547.6	767,059.7	192,375.2	1,174,295.0
Log Likelihood	–1,256,240.8	–383,496.8	–96,155.6	–587,117.5
				*p<0.1; **p<0.05; ***p<0.01

Further, negative verbal narratives yesterday, originating from autocracies, seem to dampen cyber intrusions *today*; whereas, they appear to have the opposite effect on intrusion attempts coming from democracies. However, anocratic negative verbal narratives yesterday appear to have no effect or no correlation with today's intrusions. Although, this provides indications of support for H2, H3, and H4 at the All-Regime level, it was necessary to delve into the regime-type level of analysis to accept or refute the relationships claimed in these hypotheses.[70]

Next, the research turns to the analysis of the negative narrative polarization coefficient (i.e., NN Gold_SD). All-Regimes, anocracies, and democracies track together recording negative coefficient values. While, autocracies tack in the opposite direction depicting that yesterday's negative narrative media polarization shows an amplifying effect on today's intrusion activity. Taken together this suggests support for H5 and H6; however, as in the hypotheses mentioned above, analysis at the regime-type level remains necessary for their refutation or acceptance.[71]

Further, notice the first-order interaction term combining yesterday's negative narrative tone (i.e., NN Gold_Mean) and the country's level of democracy (i.e., polity score) to derive the negative tone interaction coefficients. Figure 7 graphically represents their interaction across the range of NN tone shown between –10 and +5 on the x-axis, while the y-axis quantifies the resulting number of intrusions today resulting from yesterday's media tenor. The line coloration shown in the XY graphic and the z-axis represents the effect of NN tone ascribed to the median level of democracy for each regime type with *green* (+9) representing democracies, *blue* (2) representing anocracies, and *red*

[70] **Hypothesis #2 (H2):** *Increases* in the number of conflictual *verbal* interactions reported in the media narratives of democratic states directed at the United States (U.S.) and its interests—yesterday, results in *increased* cyber intrusion activity on U.S. networks—today.

Hypothesis #3 (H3): *Increases* in the number of conflictual *verbal* interactions reported in the media narratives of anocratic states directed at the United States (U.S.) and its interests—yesterday, results in *no change* in cyber intrusion activity on U.S. networks—today.

Hypothesis #4 (H4): *Increases* in the number of conflictual *verbal* interactions reported in the media narratives of autocratic states directed at the United States (U.S.) and its interests—yesterday, results in *decreased* cyber intrusion activity on U.S. networks—today.

[71] **Hypothesis #5 (H5)**: *Increases* in the variation of negative narrative tone, indicating an increased level of media polarization, across media stories originating from **democratic** and **anocratic** states directed at the U.S. and its interest—yesterday, results in *decreased* in cyber intrusion activity on U.S. networks—today.

Hypothesis #6 (H6): *Increases* in the variation of negative narrative tone, indicating an increased level of media polarization, across media stories originating from **autocratic** states directed at the U.S. and its interest—yesterday, results in *increased* cyber intrusion activity on U.S. networks—today.

(–7) representing autocracies.[72] The coloration of the z-axis corresponds to the change in levels of democracy for each discrete line described below.

Figure 7 displays that for those –7 autocracies, in *red*, ascribing an increase in yesterday's negative media tone results in an increase in intrusion attempts on U.S. networks today, with less intrusions resulting from anocracies shown in *blue*. While for +9 democracies, in *green*, cyber intrusions today actually decrease as a result of yesterday's increasingly negative media tone.

This finding may seem inconsistent with results of H1 and H2 described above; however, they measure two different things. Negative material and verbal narratives, the coefficients used to test H1 and H2, are measuring the daily sum of each negative narrative type. As the number of NNs both material and verbal about the U.S. on a given day increase, this results in increased intrusions the following day.

The negative tone interaction coefficient quantified in the first column of Table 5 (i.e., All-Regimes model) and graphed in Figure7 measures the interaction of the mean NN tone—yesterday, at a given level of democracy, and their combined effect on intrusions today. Because the range of the x-axis spans from +5.5 in the positive range the figure to –10, as one might expect even on NN days, positive narratives do exist; hence, those are captured in this analysis. Thus, as the average NN tone becomes more conflictual / negative yesterday the effect appears to dampen intrusion activity today for democracies. While, the effect of the interactive variable, visually appears to score a neutral impact from anocracies and an increasing effect for autocracies across the x-axis in Figure 7. As such, at this level of analysis the evidence provided in both column 1 of Table 5 and Figure 7 allows for the acceptance of H7.[73] However, by reviewing the coefficient values for negative tone interaction in the columns for autocracies, anocracies and democracies, denotes a change

[72] Argentina, Bulgaria, India, Kenya, and South Africa provide examples of some of the countries described in the median Level of Democracy scoring a +9. Algeria encompass the only anocracy scoring a 2 on the Polity scale. Finally, Azerbaijan, China, Iran, and Vietnam comprise some of the autocrats scoring -7 and included in that median value Level of Democracy shown in Figure 7.

[73] **Hypothesis #7 (H7)**: *Increases* in the accumulated conflictual or negative *tone* of interactions reported in media narratives from other countries directed towards the United States (U.S.) and its interests—yesterday, results in *decreased* cyber intrusion activity on U.S. networks—today, with the effect becoming stronger as the level of democracy of the originating country *increases*.

in direction or sign of these variables. Thus, the regime sections that follow will explore this coefficient fully and either accept or reject H7 at the regime type level of analysis.

Finally, as depicted by the red solid line in Figure 8, an increase in the daily sum of Negative Media (*Material*) narratives about the U.S.—yesterday, corresponds with an increase in cyber intrusion attempts on U.S. networks—today. The green dashed line shows a drop in intrusions on U.S. networks—today corresponding with an increase in negative media *verbal* narratives *yesterday*. Finally, the purple dot-dash line gauges yesterday's level of negative narrative (NN) polarization scoring a drop in today's intrusion activity as media polarization increases. The x-axis indicates the number or daily sum of negative media material or verbal narratives, and in the bottom frame of Figure 8, the degree of negative media polarization *yesterday* spanning from zero to eleven (~ +10.7). Whereas, the y-axis depicts the cyber intrusion attempts *today*. The shaded areas around each of the lines represents the 95% confidence interval predicting the resulting number of intrusion attempts today as yesterday's media narratives become progressively negative or more polarized.

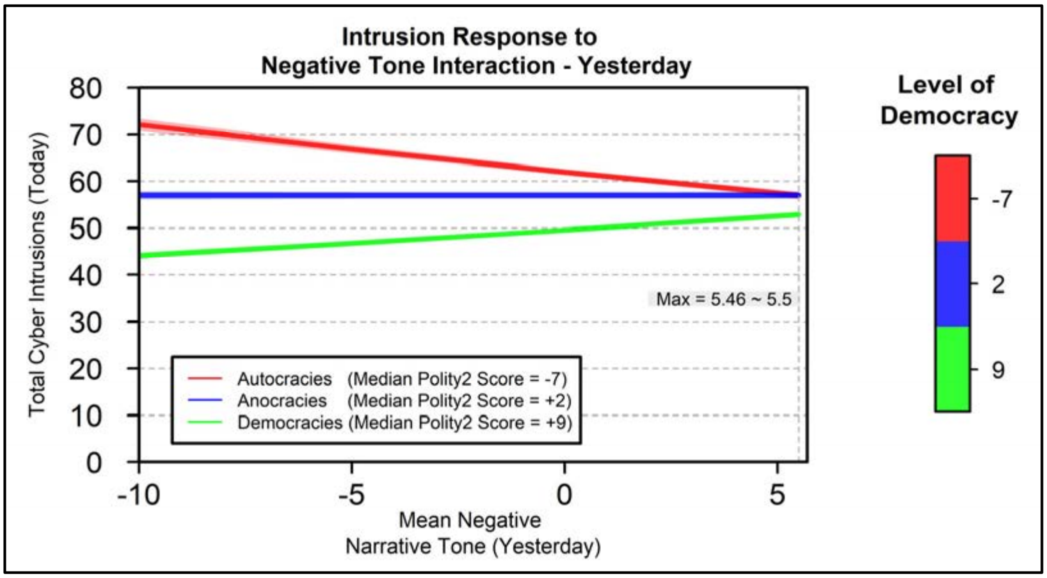


Figure 7. All-Regimes' Negative Narrative Tone Results

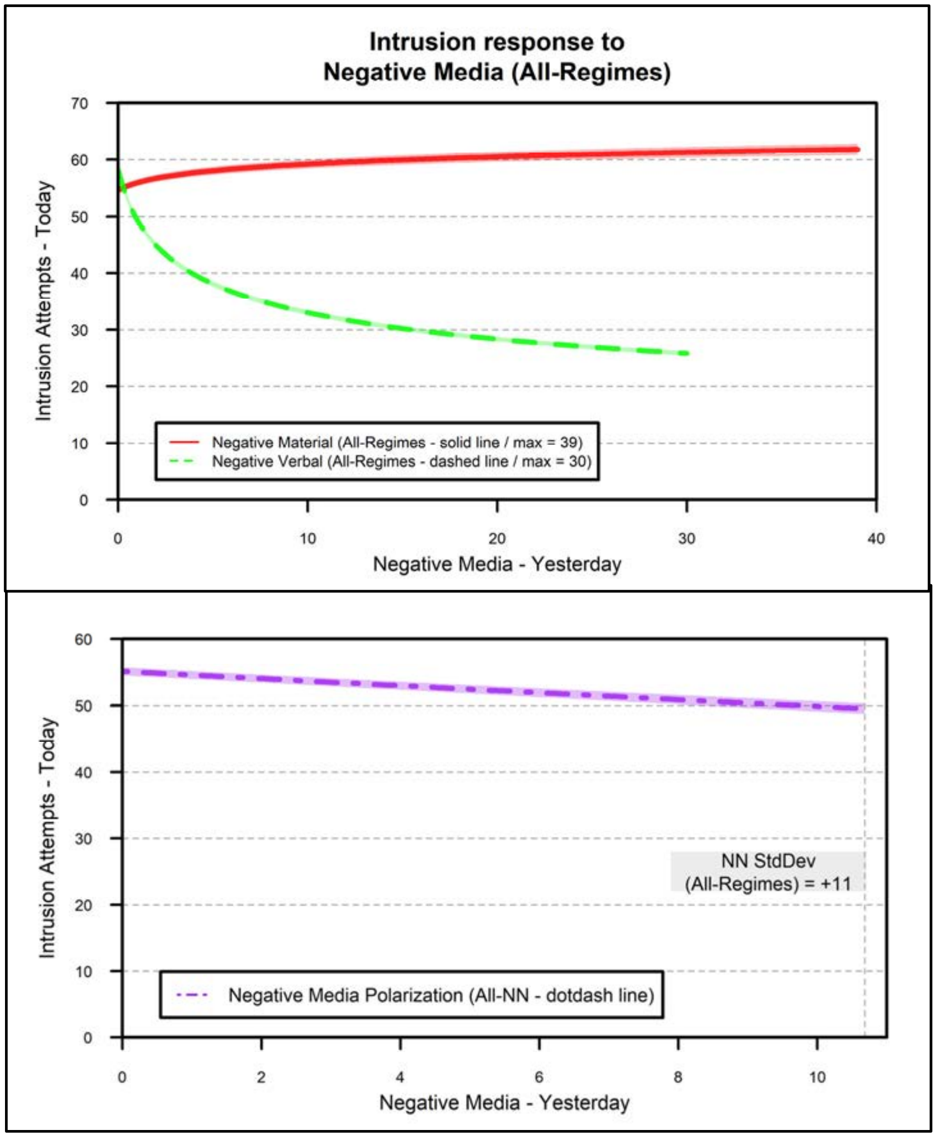


Figure 8. Media Results: All-Regimes' NN Model.

Thus, Figure 8 provides further evidence of the correlation between negative *material* media narratives—*yesterday* and cyber intrusions—*today* as H1 indicates. Further, the value of the negative material narratives (+0.03) and the low p-value further supports the rejection of the null hypothesis. Taken all together this evidence supports acceptance of H1, and evidence provided is consistent with that conclusion.

Further, the negative media verbal narrative depicted by the dashed *green* line seems to refute H2 and H3, while supporting H4. Finally, the negative narrative polarization coefficient shown in column 1 of Table 5 and represented by the purple line in Figure 8 describes a drop in intrusions as variability in media polarization increases supporting H5 but refuting H6. However, to refute or accept these hypotheses will require delving into the regime level of analysis. As such, subsequent sections will break down the data into the differing regime-types, beginning with democracies. So, how do cyber intrusion attempts on U.S. networks—*today* respond to yesterday's negative media narratives originating from other democratic countries dyadically opposite to the US?

1. Democracies in Cyberspace

While the research will cover democracies and their incumbent characteristics extensively in the case study chapter to follow, here the intent is to provide a brief overview of the more relevant aspects that make democracies different from other regime types. Democracies rank amongst the freest in most aspects of society. Democracies provide access to the political system through individual voting mechanisms, participation in and support for political parties, and open access to government institutions. Normally, a democracy's internet infrastructure does not promote government surveillance or censorship, but instead the free exchange of ideas; however, many allow big technology firms to manage their on-line content resulting from myopic policies authored by shortsighted politicians (Barabasi, 2003; Goodman, 2015; Lukasik, 2011; MacKinnon, 2012; Morozov, 2011). Yet, for the purposes of this research, democracies allow for a media environment free from censorship (Freedom House, 2017; MacKinnon, 2012). Thus, democracies do not appear to exercise the levers of societal control as much as other regime types (Freedom House, 2017; Gehlbach & Sonin, 2013; Stier, 2015).

Democracies usually possess thriving civil societies with their incumbent debates around contemporary issues. Certainly, elites exist in democratic societies; however, their gravitas or influence may or may not necessarily stem from their heritage, wealth, or class. In democracies, elites' influence may extend from their active participation and understanding of current political and cultural issues of the day, as opinion leaders (Higley

& Burton, 2006; Higley, 2018; Hoffman-Lange, 2018).[74] These opinion leaders gain and maintain a working knowledge of ongoing media narratives, which provides them an amount of influence in most of these societies (Habermas, 2006; Newton, 1999).

Within democratic societies, there exists a multiplicity of opinion leaders at various levels; thus, when political leaders or elites attempt to communicate discrete media messages to members of society, the message often comes off as chaotic, diffuse, or unclear (Bjola & Manor, 2018; Conceição-Heldt & Mello, 2017; Putnam, 1988; Strong, 2017; Trumbore, Boyer, Gibson, Harvey, & Wilkenfeld, 2000). This creates an amount of cognitive dissonance in the individuals within a democratic society, which may cause them to seek to resolve their dissonance through information-seeking behavior (Case & Given, 2016; Habermas, 1987; Turcotte, York, Irving, Scholl, & Pingree, 2015). This may lead some within these societies to resort to hacking behavior to assuage their dissonance (Valkenburg, Peter, & Walther, 2016, p. 321). Further, democratic regimes enforce very few prohibitions, except for criminal activity, on citizens' use of the internet (Goodman, 2015; Morozov, 2011). As such, the Democracies model focused on those democratic countries generating negative narratives regarding the US.

First, notice the increases in both negative *material* and *verbal* narratives *yesterday* manifest a positive correlation with cyber intrusions on the next day in Table 5. Material narratives track consistently with increases in cyber intrusions the following day in the All-Regimes model. While, the parallel negative *verbal* narratives mark a unique direction shift between the All-Regimes and the Democracies model, as shown in Table 5 above. As discussed earlier, this may indicate democracy's overall restrained use of societal control mechanisms.

Further, while a given democracy may engage the U.S. in negotiations over some issue, that democracy may relentlessly use verbally negative storylines about the U.S. attempting to influence or control the on-going narrative within level-one (international

[74] Elite – individuals and small, cohesive groups who wield a disproportionate level of power or influence affecting national and supranational political outcomes in a substantial way on a continuing basis (Best & Higley, 2018, p. 3; Higley & Burton, 2006, p. 14). Throughout this text, elite is synonymous with opinion or proximate leader, particularly when discussing democratic elites.

politics) of two-level process theory. Simultaneously, these democracies attempt to influence their domestic or level-two process using media messaging, over which they enjoy very little, if any, real control (Aelst, 2017; Habermas, 2006; Higley & Burton, 2006; Putnam, 1988; Turcotte, York, Irving, Scholl, & Pingree, 2015). Thus, beyond the negative or positive polarities resident in media narratives, intruders on U.S. networks from other democracies appear to remain tone-deaf to the *material-verbal* nuance. Or these democratic hackers may be indulging in information seeking behavior seeking to salve their inquisitive nature to find out the rest of the story. This may occur because they live in relatively free societies where the ramifications of their cyber intrusive proclivities may not incur harsh legal consequences, as in other societies. Nevertheless, unlike the All-Regimes model, democratic hackers (i.e., intruders) appear unphased by subtle differences in the media narratives.

Secondly, the negative narrative polarization (i.e., Gold_SD) remains consistent with the All-Regimes' model also scoring a dampening effect on intrusions the day following the media event recorded. Thus, the entirety of this evidence appears to support what many scholars posit about democracies that the sheer multiplicity and diversity of media narratives, media outlets, and opinion leaders, drowns out the subtle changes in media tone or variation, beyond the positive or negative polarities in material or verbal narratives (Aelst, 2017; Turcotte, York, Irving, Scholl, & Pingree, 2015).

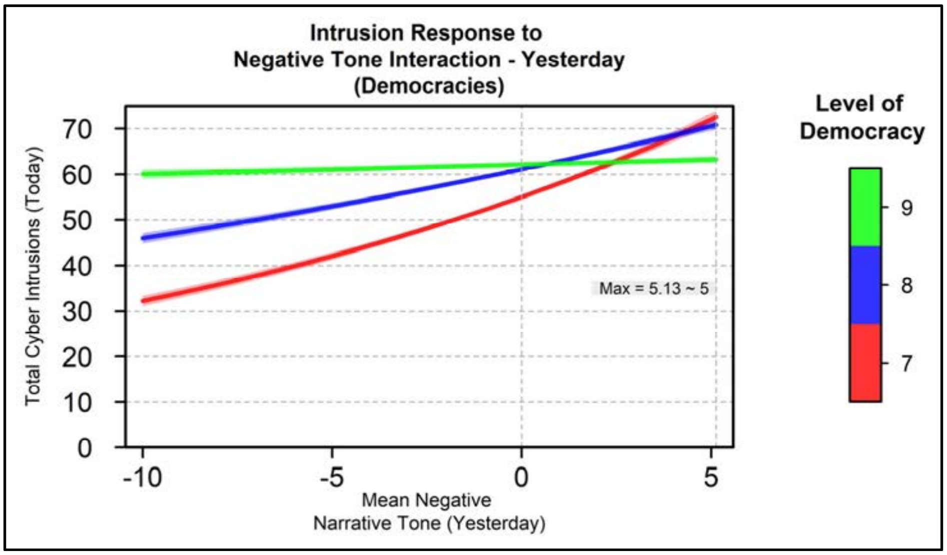


Figure 9. Negative Narrative Tone Results: Democracies.

Next, the negative tone interaction between yesterday's increase in negative media tone and the level of democracy results in more intrusions today. In Figure 9, notice how the *red* line depicting the interaction between increasing negative tone and the lower democratic level yesterday decreases the level of intrusions today at a faster rate with the intrusion attempts decreasing by –40 per day across the NN tone range.[75] The *red* line, equating to a polity score of –7, describes a mean value 50 intrusions per day. The higher level of democracy, the *green* line with a Polity Score of +9, records a mean value of 61 intrusions, approximately 22% higher than low democracy countries, decreasing at a rate of –3 intrusions per day, 93% less than the *red* line countries, across the NN tone range.[76] Notice that the *green* line predictions, from countries with a higher level of democracy, crosses above the red and blue lines at +3 and +1 in narrative tone, respectively, and

[75] The red line begins at 72.5 intrusions on the right dropping to 32.2 on the left (72.5 – 32.2 = 40.3 ~ -40), spanning from positive tone of 5.13 and -10 NN tone, respectively. Some of the countries represented in the red line include Columbia, Georgia, Nigeria, and Tunisia.

[76] The mean value of the line across the entire red line and green line were calculated using R deriving 62 and 51, respectively. By dividing the difference by 51 ((62-51) / 51 = 0.216) 22% is derived. Some of the countries represented in the green line include Argentina, Czech Republic, India, and South Africa. Further, by using R coding the predicted values for the given line were derived. At +5.13 on the NN tone x-axis the green line records 63.3 intrusions and at the end of the line at -10, 60 intrusions were estimated. As such, 63.3 – 60 = -3.3 ~ -3 drop in intrusions across the green line. Finally, the green line decreases across the x-axis by -40, while the red line records a decrease of -3; thus, -40-(-3) / -40 or -37/-40 equals 92.5 ~ 93% or a decrease 93% less than those countries captured in the green line.

remains above both of these lower level democracies across the remainder of the negative range. The differences in mean value and slope drop per day over the NN tone range indicate that today's increasingly NN tone has a greater dampening effect on tomorrow's intrusions coming from low-level democracies. This is a phenomenon this research intends to explore in the Democracies' case study. Further, this finding is inconsistent with that of the All-Regime's NN model and provides evidence for rejection of H7 for democracies.[77]

Finally, Figure 10 graphically and numerically completes the analysis of the negative material and verbal and NN media polarization coefficients. As the number of each of these storylines, regardless of type, originating from democracies about the U.S., increase *yesterday*, this leads to cyber intrusion increases *today*. Observe the negative verbal narratives value and how it shifts opposite in sign and magnitude swinging to a positive marginal rate *1.3 times* above the All-Regimes' predictions.[78] In democracies both material and verbal effects begin and remain at a level above the same values in the All-Regimes model, as depicted in the graphic and table at the bottom of Figure 10. Material negative narratives, depicted by the red long dash line in Figure 10, clock in at an average of +68 intrusions 13% above All-Regimes at +60 but show an average marginal effect (AME) 35% *lower* impact on intrusions across the x-axis.[79] The NN polarization forecast value shows a precipitous drop, scoring an average marginal effect *87% below* that of the All-Regimes model across the x-axis media polarization range.[80] Further, the All-

[77] **Hypothesis #7 (H7)**: *Increases* in the accumulated conflictual or negative *tone* of interactions reported in media narratives from other countries directed towards the United States (U.S.) and its interests—yesterday, results in *decreased* cyber intrusion activity on U.S. networks—today, with the effect becoming stronger as the level of democracy of the originating country *increases*.

[78] The model used to derive the average marginal effect (AME) for both the All-Regimes and the democracies are the same. The predicted values of NmN, NvN, and NNP were derived by holding all of the other variables' constant at their mean values. Thus, the AME values for the NmN, NvN, and NNp variables predicts the marginal change (effect) on intrusions, shown on the y-axis, per unit change in each of these independent variables across the x-axis. As such, the AME in the table at the bottom of Figure 10 was derived through the use of the same model; thus, the All-Regimes negative verbal marginal change across the x-axis range clocks in at -2.1, with democracies scoring a +0.7, as such (-2.1 – 0.7)) / -2.1 = +1.33 ~ 1.3.

[79] Calculated as follows: 0.354 – 0. 2286) / 0.354 = 0.35 ~ 35% drop below the All-Regimes model.

[80] Calculated as follows: -1.82-(-0.97) / -0.97 = 0.867 ~ 87% drop below the All-Regimes' prediction.

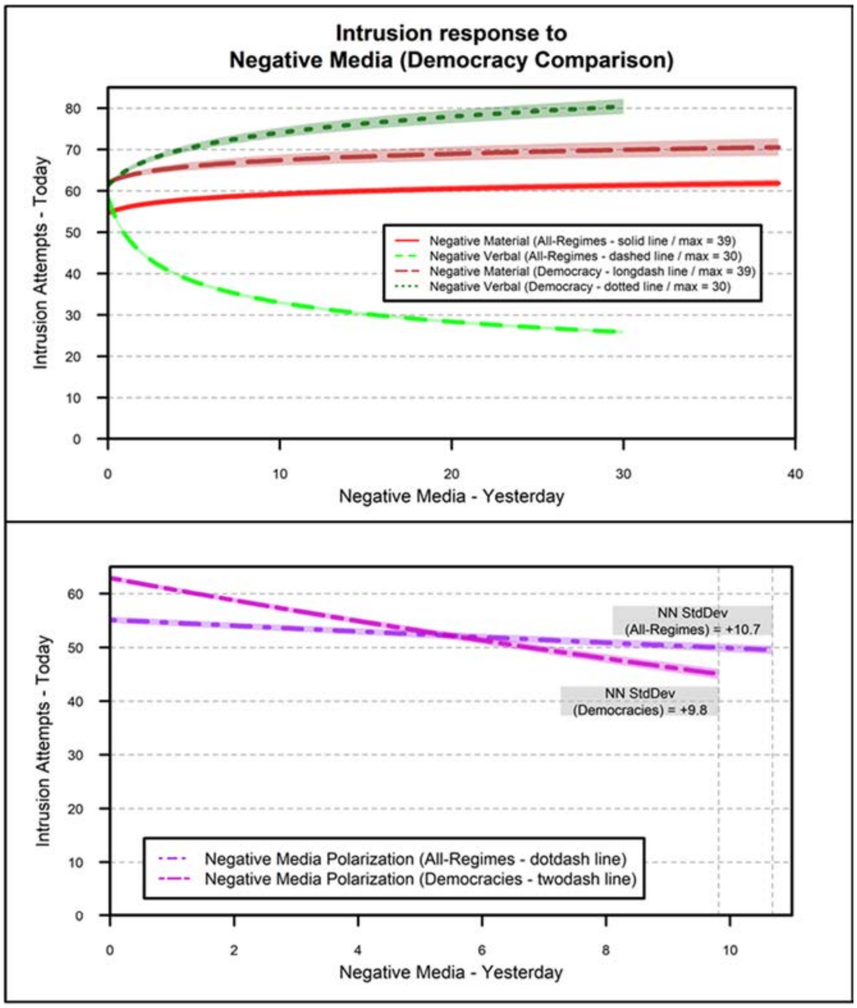
Regimes model records a slightly higher maximum NN polarization value recording a daily variation of 10.7 over democracies at 9.8 at 8% less, as shown in the bottom frame.

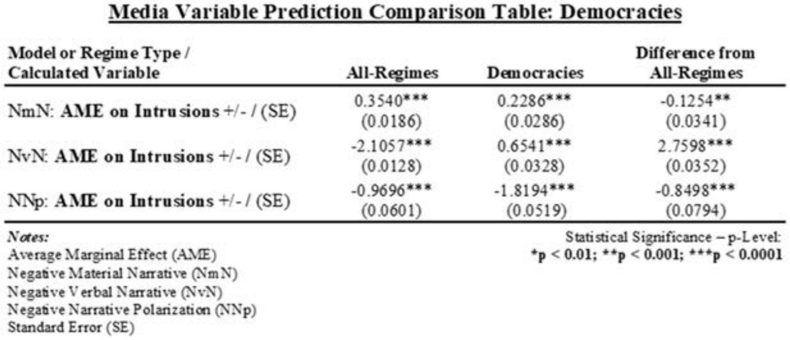
Taken all together, this *democracies* model provides evidence that the phenomena hypothesized in H1, H2, and H5 may operate in the real world, particularly at this finer level of analysis.[81] Consequently, these finding contribute valuable insights into the cyber realm. Next, the researcher will test the model on the hybrid or anocratic regime type at this same level of analysis. So, how do negative media narratives about the U.S. stemming from dyadic interactions with anocratic countries *today* impact cyber intrusions on U.S. networks *tomorrow?*

[81] **Hypothesis #1 (H1):** *Increases* in the number of conflictual *material* interactions reported in the media narratives of other sovereign states directed at the United States (U.S.) and its interests—yesterday, regardless of regime type, results in *increased* cyber intrusion activity on U.S. networks—today.

Hypothesis #2 (H2): *Increases* in the number of conflictual *verbal* interactions reported in the media narratives of democratic states directed at the United States (U.S.) and its interests—yesterday, results in *increased* cyber intrusion activity on U.S. networks—today.

Hypothesis #5 (H5): *Increases* in the variation of negative narrative tone, indicating an increased level of media polarization, across media stories originating from **democratic** and **anocratic** states directed at the U.S. and its interest—yesterday, results in *decreased* in cyber intrusion activity on U.S. networks—today.





Media Variable Prediction Comparison Table: Democracies

Model or Regime Type / Calculated Variable	All-Regimes	Democracies	Difference from All-Regimes
NmN: **AME on Intrusions** +/- / (SE)	0.3540*** (0.0186)	0.2286*** (0.0286)	-0.1254** (0.0341)
NvN: **AME on Intrusions** +/- / (SE)	-2.1057*** (0.0128)	0.6541*** (0.0328)	2.7598*** (0.0352)
NNp: **AME on Intrusions** +/- / (SE)	-0.9696*** (0.0601)	-1.8194*** (0.0519)	-0.8498*** (0.0794)

Notes:
Average Marginal Effect (AME)
Negative Material Narrative (NmN)
Negative Verbal Narrative (NvN)
Negative Narrative Polarization (NNp)
Standard Error (SE)

Statistical Significance – p-Level:
***p < 0.01; **p < 0.001; ***p < 0.0001**

Figure 10. Media Results: Democracies

2. Anocracies in Cyberspace

Anocracies, known as imperfect, partly free, hybrid or mixed democracies, occupy the middle ground between democracies and autocracies. This regime-type space appears transitory, where some states seem destined to become either a democracy or autocracy, yet, others appear stuck in anocratic stasis, such as Russia, which appears to seek the economic trappings of a democratic regime while maintaining the societal control of an autocracy (Freedom House, 2017; Gunitsky, 2015; Hussain, 2016; MacKinnon, 2012; Manokha, 2018; Marshall & Elzinga-Marshall, 2017; Morozov, 2011; Zittrain, et al., 2017). Or consider Turkey, which seems destined to discard the secular democratic ideals of Mustafa Kemal Ataturk. As Turkey continues its journey to an autocratic neo-Ottoman future by leveraging *mediatized* and *securitized* instruments of a digital panopticon to cement societal control of the state (Akgül & Kirlidoğ, 2015; Bilgiç, 2018).[82]

Thailand, on the other hand, seems to shift between democracy and anocracy, as it struggles between supporting its centuries old monarchy and its populations craving for greater democratic access to government institutions (Pinkaew, 2016). In 2014, Thailand settled into the anocratic middle with its elites working hard to create and maintain a peaceful digital panopticon to monitor their population's social media postings in an effort to sustain their culture and monarchial heritage (Gebhart, Anonymous, & Kohno, 2017; Pinkaew, 2016; Sinpeng, 2013). In still another example, Tunisia installed an interim government to chart a path toward democracy after the swift exit of their longtime President Zine el-Abidine Bin Ali to Saudi Arabia as a result of the 2011 *Jasmine Revolution (Carrieri, Deibert, & Khan, 2016; Freedom House, 2017; Hinnebusch, 2015).*[83]

Elites in this regime-type, unlike in democracies, often receive their status from hereditary or generational class affiliation. Incumbent with their status comes the wealth

[82] Mediatized – where persons construct their social reality, instead of engaging in face to face interactions, through the sharing of their views using communications [information] technology (i.e., social media, online news channels, blogging, and photo sharing), which because of its modalities can be recorded and monitored by the state, (Bilgiç, 2018, pp. 261-262).

Securitized – where a given country, under the auspices of national security, records, monitors, collects, and stores the everyday [information technology] interactions of its citizenry for use in addressing risks or threats to the state (Bilgiç, 2018, p. 262; Committee on National Security Systems, 2015).

[83] Subsequently, Tunisia has sought to modify or change its internet structure, originally built for state surveillance and control, to one where freedom of expression may thrive without the threat of government censorship (Chakchouk, Kehl, Ben-Avie, & Coyer, 2013; Wagner, 2012). Certainly, that transition will pose a challenge and may not occur as fast as the people of Tunisia may appreciate Tunisia gained democracy status in 2017 achieving a polity score of +6 (Marshall & Elzinga-Marshall, 2017).

accumulated by their families, which enables their social mobility to higher levels in their class structure. This class structure may act for many as a barrier to entry into the elite ranks. Further, these anocratic elites permeate many of the vocations within a given country's civil society. This positioning enables anocratic elites to perform the interlocutor function between a society's leadership and the citizenry (Best & Higley, 2018; Newton, 1999; Putnam, 1988). Further, this characteristic becomes acutely important when their country's leadership engages in dialog, negotiations, or an exchange of narratives with another country (i.e., level-one of international relations theory) (Putnam, 1988).

For the purposes of this study, the focus remains on negative narratives created by anocratic countries, reported by the media about the U.S. State leaders normally use these narratives as an instrument of negotiation to coerce, compel, or cajole the country opposite them in a dyad, in this case the U.S., into a position favorable to the negotiating nation. Further, if a state leader remains unencumbered by domestic (i.e., level-two / domestic politics) beliefs, opinions, or attitudes towards a given position, the greater the probability of success during an international negotiation (Putnam, 1988, p. 449). While no leader enjoys total immunity from domestic or level-two pressures during a negotiation, their ability to control or manage the media narrative aimed at domestic audiences would prove beneficial, particularly if anocratic regimes controls the media though outright ownership, legal or regulatory structures (Best & Higley, 2018; Putnam, 1988).

As hypothesized in H1, H3, H5, and H7 anocratic leaders, with their panoptic capabilities, execute greater influence over their press and their population's use of the internet than democracies, during what Putnam (1988) refers to as level-one discourse (i.e., international negotiations / politics), thereby providing them with greater negotiation space during these discussions. Specifically, these anocratic leaders use these control mechanisms to regulate the narrative, particularly, during the *verbal* phase of level-one negotiations. This control serves to solidify the media narrative both at home and abroad.

Simultaneously, the countries' elites digest the telegraphed *verbal* narrative, following Lazarsfeld's (1944) two-step information flow, and communicate these domestically (i.e., Putnam's level-two), cueing their citizens to exercise patience as their leadership uses negative rhetoric to potentially improve their negotiating position with the

U.S. (i.e., Putnam's level-one). The resulting flat line level of intrusions appears as a manifestation of societal control engendering disengagement, while their country's leaders work through the negotiation process. Specifically, the two-step information flow may operate within, and reinforce, regime messaging within level-two of domestic politics. Table 5 and Figure 12 provide indications of this operationalization within anocratic regimes types.

In Table 5, notice how the negative *material* narrative coefficients track closely in direction with the other models. Further, recognize how the negative *verbal* narratives yesterday appears to have *no effect* on intrusions today, quite different from the other two models. This negative *verbal* narrative coefficient indicates that the two-step process operates within and reinforces anocratic regime narratives at level-two of this international relations theory (i.e., domestic politics), potentially, revealing how anocratic leaders use the digital panopticon to manage and communicate with their domestic audiences through the media and elites during their *verbal* scuffling with the U.S. This management and communication mechanism signals to their citizens to cease their activities, while the level-one (i.e., international negotiation) remains *verbal*, which leads to *flat* intrusion activity, an indication of the populations allowing their leadership more maneuver space in the negotiation process.

Further, one could view the magnitude, direction, and p-value significance of the internet not free, dichotomous control variable as evidence to buttress this finding as shown in Figure 36 of Appendix F. Also, note the absence of a value for the media not free control coefficient, denoting that anocracies enjoy control of their media milieu. Thus, those anocracies that curtail internet freedoms can and do rheostat online activity using generational content controls and manifest strict control of media messaging allows the regime to exercise greater control over the internet and media environment. A convenient option at the regime's disposal when engaged in level-one dialog with the US.

Once the *verbal* media fracas ends, which signifies a real or *material* outcome of the dyadic interchange at level-one, anocratic leaders message the population through the media and the elites to resume their normal activities, while relaxing their use of generational content controls. How the anocracy perceives the outcome will determine whether the media *material* narrative describing the actual result is positive or negative.

Should the outcome prove unfavorable to the anocracy, an *increase* in negative *material* narratives—*today* may result. Table 5 and Figure 12 show that, as negative *material* narratives—*yesterday* describing the material or realized outcome of the negotiation between an anocracy and the U.S. increase, correlates to an *increase* in cyber intrusion attempts on U.S. networks the next day. These model results provide evidence that the two-step process operates within and reinforces the two-level process of international relations in anocratic regime-types.

This mechanism could be further reinforced by internet content control mechanisms, as discussed above and in the literature review. Other possible hacktivist mobilization or demobilization mechanisms , as previously posited, might include social movement elites tuned into the issue being negotiated or state-sponsored hackers to perform these intrusions, which has been posited by multiple scholars (Biçakci, Doruk, & Mitat, 2015; Esen & Gumuscu, 2016; Gunitsky, 2015; Hussain M. M., 2016; Marcellino, Marcinek, Pezard, & Matthews, 2020; Pinkaew, 2016; Saka, 2018; Sinpeng, 2013; Yesil, Sözeri, & Khazraee, 2017; Zittrain, et al., 2017). Indeed, the average citizen within these anocratic regimes does not possess the capabilities or the internet access to execute such intrusions to this scale and so precisely to coincide with media events (Biçakci, Doruk, & Mitat, 2015; Esen & Gumuscu, 2016; Gunitsky, 2015; Hussain M. M., 2016; Marcellino, Marcinek, Pezard, & Matthews, 2020; Pinkaew, 2016; Saka, 2018; Sinpeng, 2013; Yesil, Sözeri, & Khazraee, 2017; Zittrain, et al., 2017). While the fidelity of this data makes it difficult to discern which of these mechanisms or processes lead to increased intrusion activity, it is safe to say the latter two would rest upon the previously posited nesting of the two-step within level-two of international relations theory (i.e., domestic politics).

Observe how the negative narrative polarization coefficient continues the trend of the other two models decreasing intrusions tomorrow as a result of increased negative media polarization today. Perhaps, this is a result of the hacktivist population knowing that they do not enjoy a free media, indicated by the absence of a coefficient value for media not free in Table 5. As such, any variation in media messaging would be regime sanctioned, perhaps viewed by the hacktivist as faux narratives generated to further the regime's purposes. Resulting in the dampening effect of yesterday's NN polarization on intrusions today.

Yet, for those anocracies that control their internet and media environments and foster media self-censorship, this latter control variable scores a high positive value with an accompanying statistically significant p-value. Taken together, in these regimes, known media self-censorship in reporting yesterday's NNs triggers an increase in intrusions coming from anocratic hackers—today, ceteris paribus. These sensitized hackers could be indulging in information seeking behavior looking to assuage their curiosity, hunting down more information or seeking the rest of the story on the situation described in yesterday's press. Figure 36 in Appendix F quantifies the magnitude of the change in evident media self-censorship with the predicted level of intrusions rising +42 for anocracies, while the All-Regimes and democracies models show rises of +4 and +3, respectively.

Thus, media self-censorship displays a greater influence over today's intrusions amongst anocracies than was seen in the other two models. As stated earlier, since anocratic citizens know the state controls the domestic media, this would logically lead journalists to self-sensor their narratives. The widely known media self-censorship, within the society magnifies intrusions, which ultimately drives intruders from these anocracies to the internet seeking information.

Now to evaluate the negative tone interaction coefficient. The interactive effect of the negative media tone and level of democracy come in at the same sign (i.e., negative) as the initial model, but opposite to that of the Democracies model. The difference in the later comes from the negative or positive sign of the level of democracy ascribed to Anocracies spanning from +5 to –5 as shown on the z-axis of Figure 11. As such, for anocratic countries enjoying a higher level of democracy (i.e., open anocracies in the dark green line or +3 below) such as Tanzania and Turkey, this coefficient would have a dampening effect on cyber intrusions with a mean value of 34, dropping by –9 across the x-axis negative tone range depicted in Figure 11. Those anocracies closer to autocracies, for example Ethiopia, Myanmar, Rwanda, or Thailand (i.e., the red line or –3), record a slightly greater amplifying effect on cyber intrusion attempts, recording a mean value of 40, rising by +11 across the negative tone range, essentially *doubling* the impact over more democratic anocracies, increasing today's intrusions as shown in Figure 11. Thus, this finding is consistent with Figures 5 and 7 allowing for the acceptance of H7 for anocracies at this level of analysis.[84]

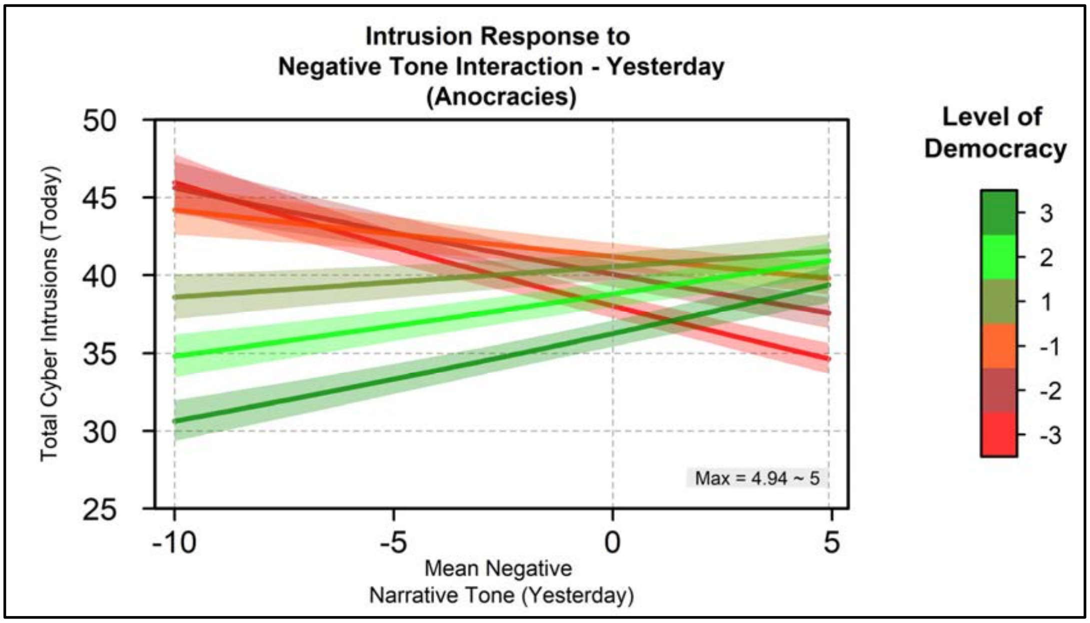


Figure 11. Negative Narrative Tone results: Anocracies.

Further, as shown in Figure 12, this Anocracies model provides evidence in support of the posited hypotheses, H1, H3, and H5. These anocracies appear to manifest many similarities to democracies, except for how negative verbal narratives—*today* affect cyber intrusions—*tomorrow*, which shows *no significant effect*. The researcher explained earlier how the two-step information flow operated within, and reinforced, anocracies domestic narratives used in the level-two domestic narrative (Lazarsfeld, Berelson, & Gaudet, 1944; Putnam, 1988). Figure 12 graphically suggests that anocracies *material* narratives mirror the results of the All-Regimes model, but at an average marginal effect (AME) rate *77%*

[84] **Hypothesis #7 (H7)**: *Increases* in the accumulated conflictual or negative *tone* of interactions reported in media narratives from other countries directed towards the United States (U.S.) and its interests—yesterday, results in *decreased* cyber intrusion activity on U.S. networks—today, with the effect becoming stronger as the level of democracy of the originating country *increases*.

higher than All-Regimes' material narratives, providing further evidence for the acceptance of H1.[85] While yesterday's negative verbal narratives records a *statistically insignificant* or *no effect* on today's intrusion activity, which supports H3.[86]

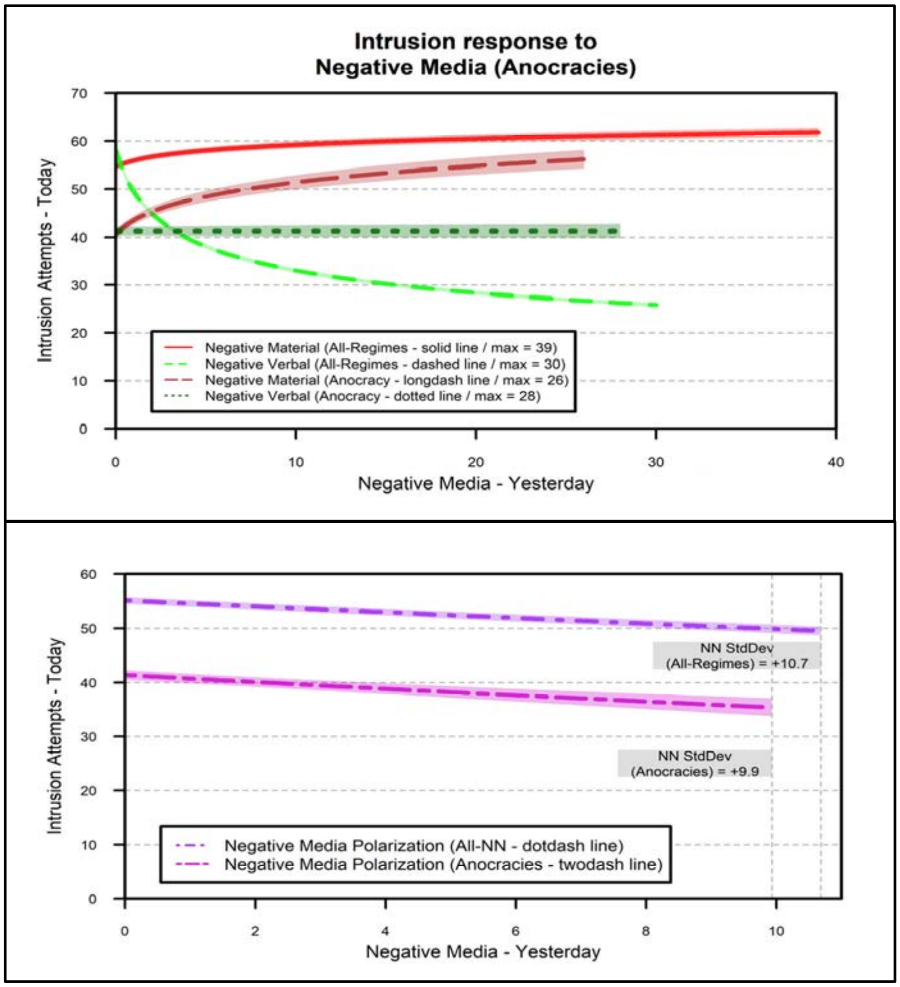
Finally, notice how yesterday's negative media polarization coefficient seems to produce a dampening impact on today's intrusions producing an average marginal impact 35% less than the All-Regimes model, which supports acceptance of H5. Thus, at this level of analysis H1, H3, and H5 can be accepted and the null rejected.[87] Now, the research turns to the final regime type—autocracies, seeking to answer the same question. How do negative media narratives about the U.S. resulting from dyadic negotiations or dialog with autocratic countries *today* affect cyber intrusions on U.S. networks *tomorrow*?

[85] The model used to derive the AME for anocracies is shared with autocracies and removes the Internet and Media Not Free and Media self-censorship control variables because they do not vary for autocracies and the media self-censorship fluctuates very little for anocracies. Since, the predicted values of NmN, NvN, and NNP are being used holding all of the other variables constant at their mean values, while the prediction estimate is derived, very little, if any change in these coefficient value was observed due to the removal these control variables, which allows for prediction of the AME in each case. Therefore, by comparing the NN Polarization AME prediction values in Figure 12 confirms that the All-Regimes scores a +0.354 and the anocracies clock in at +0.626 giving a projected negative material rate 74% greater than the All-Regimes or (0.626 – 0.354) / 0.354 = .768 ~ 77%.

Hypothesis #1 (H1): *Increases* in the number of conflictual *material* interactions reported in the media narratives of other sovereign states directed at the United States (U.S.) and its interests—yesterday, regardless of regime type, results in *increased* cyber intrusion activity on U.S. networks—today.

[86] **Hypothesis #3 (H3):** *Increases* in the number of conflictual *verbal* interactions reported in the media narratives of anocratic states directed at the United States (U.S.) and its interests—yesterday, results in *no change* in cyber intrusion activity on U.S. networks—today.

[87] **Hypothesis #5 (H5)**: *Increases* in the variation of negative narrative tone, indicating an increased level of media polarization, across media stories originating from **democratic** and **anocratic** states directed at the U.S. and its interest—yesterday, results in *decreased* cyber intrusion activity on U.S. networks—today.



Media Variable Prediction Comparison Table: Anocracies

Model or Regime Type / **Calculated Variable**	**All-Regimes**	**Anocracies**	**Difference from** **All-Regimes**
NmN: **AME on Intrusions** +/- **/** (SE)	0.3540*** (0.0186)	0.6260*** (0.0333)	0.2720*** (0.0381)
NvN: **AME on Intrusions** +/- **/** (SE)	-2.1057*** (0.0128)	0.0153 (0.0251)	2.0904*** (0.0282)
NNp: **AME on Intrusions** +/- **/** (SE)	-0.9696*** (0.0601)	-0.6321*** (0.0833)	0.3375** (0.1027)

Notes:
Average Marginal Effect (AME)
Negative Material Narrative (NmN)
Negative Verbal Narrative (NvN)
Negative Narrative Polarization (NNp)
Standard Error (SE)

Statistical Significance – p-Level:
***p < 0.01; **p < 0.001; ***p < 0.0001**

Figure 12. Media Results: Anocracies.

3. Autocracies in Cyberspace

The autocratic form of government spans from monarchs to dictators.[88] Yet, most autocratic states share the same method of governing their citizenry. First, most autocracies have pre-existing barriers to entry for admission and acceptance into the ruling or elite class of civil society. These barriers usually hinge upon a person's genealogy, allegiance to the ruler, affiliation with the ruling party or the dominant religious group. Certainly, the elite class evolves, changes, and refreshes periodically; however, the periodicity of renewal cycles happens less often than in democracies and anocracies (Cotta, 2018). Secondly, autocratic regimes tend to enjoy greater stability and continuity, since as implied above, changes to the ruling or elite structure rarely occur. As a result, the average, non-elite citizen holds very little influence over their society's governing structures, laws, or operations (Marshall & Elzinga-Marshall, 2017). Autocratic regimes hold fast to either ideological or religious tradition and do not appreciate transgressive movements or behaviors, regardless of rationality (Gebhart, Anonymous, & Kohno, 2017; Greitens, 2013; Hussain M. M., 2016; Keck & Sikkink, 1998; Rød & Weidmann, 2015; Stier, 2015).

While autocracies share many common characteristics, they also possess distinct differences, which seem to originate from their unique histories. For example, many of the autocratic countries spanning the Middle East, as former protectorates or vassal states of Britain or France, chose to combine what they learned from their past colonizers into their pre-existing governing structures (Best & Higley, 2018). Some with great success (i.e., Bahrain, Oman, Qatar, Saudi Arabia, and United Arab Emirates), others resulting in failed states such as Syria, while others, specifically Iran, seem to remain in constant turmoil with itself and others (Henry, 2018; Higley, 2018; Marshall & Elzinga-Marshall, 2017; Pollack, 2004).

Some emergent autocracies blend in new ideologies (i.e., Communism) with past governing structures, throwing out some of the old and keeping some of the new to create

[88] The nineteen autocratic regimes included in this study span Azerbaijan, Belarus, Bahrain, China, Cuba, Eritrea, Iran, Kazakhstan, Kuwait, Laos, North Korea, Oman, Qatar, Saudi Arabia, Swaziland, Syria, United Arab Emirates, Uzbekistan and Vietnam.

the governing structure uniquely their own. This group of autocracies include Azerbaijan, Belarus, China, Cuba, Kazakhstan, Laos, North Korea, and Uzbekistan (CIA, 2019). The most populous of these is China, whose rise has encountered some setbacks recently with repression of democracy in Hong Kong and the coronavirus outbreak.

Amongst these autocrats, Iran remains unique, blending Islamic religious ideology with mechanisms of government that appear democratic. Adhering to their historical roots, where the country's leader, then the Shah and now the Ayatollah, stand as the central figure of leadership and governance (Ansari, 2017; Duindam, 2018; Pollack, 2004). Iran remains distinctive as a theocracy, which appears to manifest all of the governmental mechanisms of a democracy (i.e., national elections), yet, when taken in sum remains firmly autocratic (Marshall & Elzinga-Marshall, 2017; Pollack, 2004). A subsequent chapter will explore the enigmatic Iran in greater detail.

All of this taken together permits autocracies to develop an internet infrastructure that facilitates state censorship and surveillance, thus allowing the state to propagandize media narratives in support of the regimes' policies (Diamond, 2010; Freedom House, 2017; Gunitsky, 2015; Morozov, 2011; Rød & Weidmann, 2015; Shirky, 2011; Stier, 2017; Zittrain, et al., 2017). These regimes control, surveil, and trace their citizens using the internet and associated IT media platforms (Morozov, 2011). They view this technology as an instrument of repression, not liberation, fully embracing the digital panopticon, exploiting its vast capabilities to achieve their desired ends (Gebhart, Anonymous, & Kohno, 2017; Morozov, 2011; Pinkaew, 2016; Sinpeng, 2013; Yesil, Sözeri, & Khazraee, 2017; Zittrain, et al., 2017). Further, these autocracies, deliberately, build the physical and syntactic layers that make up their indigenous internet to provide optimal control. This optimal control enables the regime to effectively monitor, manage, and manipulate the semantic layer; thereby, ensuring the supremacy of their chosen media narrative (Greitens, 2013; Libicki, 2007; MacKinnon, 2011; MacKinnon, 2012; Manokha, 2018; Ruijgrok, 2017). These autocratic traits play out well in the *Autocracies* model.

In Table 5, notice how the negative *material* narrative coefficient remains positive tracking with the other models. Further, observe how the negative *verbal* narratives coefficient tracks closely with the All-Regimes model but opposite of democracies in sign value trending negative as opposed to the *neutral* Anocracies, each provides evidence of the operation of H1 and H4.[89] Secondly, see how the NN polarization coefficient tacks opposite in direction to the All-Regimes model and other regime types.

Next, notice how the internet and media freedom coefficients, as well as, the media coefficient for media self-censorship do not vary and, consequently, are blank in Table 5. This signifies that autocracies, as stated earlier, as a regime type do not allow or foster freedom of the press or of the internet and uniformly encourage media self-censorship.

Now observe the analysis of the multiplicative interaction term combining NN media tone and each country's level of democracy, which provides some interesting results. Note how the NN tone coefficient, in Table 5, tracks in the same direction as the Democracies model, but appears to have greater negative influence over today's intrusions when comparing the y-axis values in Figures 9 and 13, respectively. This interaction results in a decrease in intrusions *today* coming from autocracies, whose polity scores range from –6 to –10, as *yesterday's* tone of NN's originating from these autocrats increases.

Visually, one can view the red line in Figure 13. Note how increases in yesterday's NN tone predicts decreases the number of intrusion attempts today for NN emanating from countries similar to Swaziland, Syria, and Uzbekistan with a polity score of –9. Further, the mean value intrusions per day captured by the red line is 62, while decreasing over the range by 89 less intrusions as yesterday's NN tone becomes increasingly negative across the x-axis. While, the green line depicts the same effect but at a different level forecasting a decrease in intrusions today resulting from an increase in yesterday's NN tone for narratives originating from a country similar to China, Cuba, Iran, or Vietnam. The number of intrusions per day coming from these autocracies with higher levels of democracy (i.e., the green line) falls across the increasing NN tone range from 263 to 179, a drop of 84 intrusions per day and scores a mean predicted intrusion value of 218. That mean value of

[89] **Hypothesis #1 (H1):** *Increases* in the number of conflictual *material* interactions reported in the media narratives of other sovereign states directed at the United States (U.S.) and its interests—yesterday, regardless of regime type, results in *increased* cyber intrusion activity on U.S. networks—today.

Hypothesis #4 (H4): *Increases* in the number of conflictual *verbal* interactions reported in the media narratives of autocratic states directed at the United States (U.S.) and its interests—yesterday, results in *decreased* cyber intrusion activity on U.S. networks—today.

the green line equates to a greater than *two*-fold increase in intrusions per day above those autocracies represented by the red line.[90] Thus, these autocracies recording higher levels of democracy appear to intrude more actively on their U.S. rival's networks, even though they manifest a decreasing trend as the NN tone becomes more negative. This result calls for the rejection of H7 for autocracies, acceptance of the null, and efforts to use this finding to proffer further hypotheses relating to China and Iran in Chapter IV.[91]

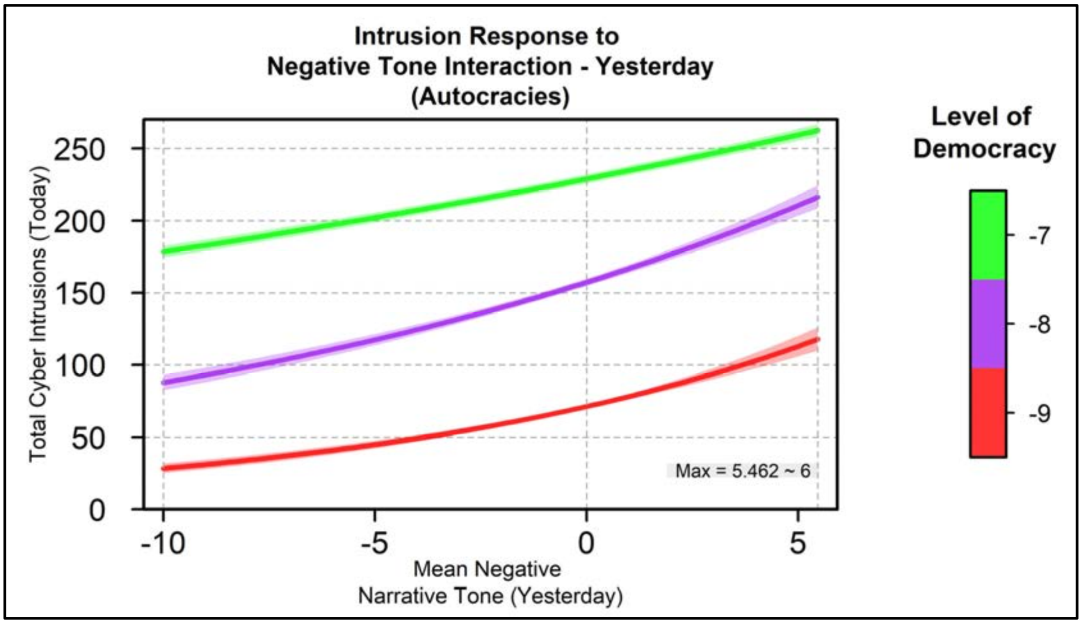


Figure 13. Negative Narrative Tone Results: Autocracies.

Now the research turns to addressing H1, H3, and H6, the results of which were discussed above and are graphically depicted in Figure 14. Notice how autocratic leaders engage with the U.S. in verbal rhetoric at level-one, where the effect of negative verbal interactions becomes increasingly negative, as they communicate with their citizens at level-two through the media and through their elites or rheostat their sovereign internet through the use of generational content controls. First, their elites digest the media narrative

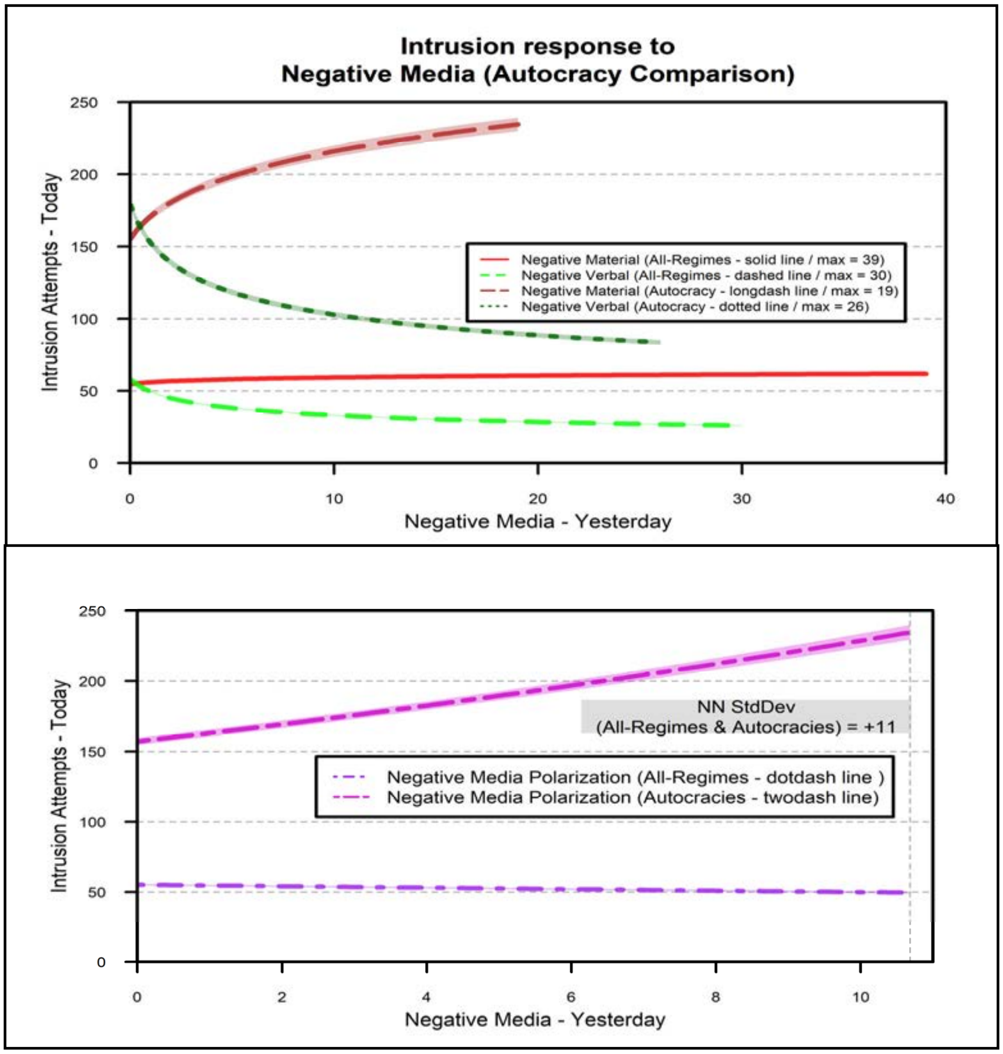
[90] (218 – 62) / 62 = 2.52 ~ > 2 times greater.

[91] **Hypothesis #7 (H7)**: *Increases* in the accumulated conflictual or negative *tone* of interactions reported in media narratives from other countries directed towards the United States (U.S.) and its interests—yesterday, results in *decreased* cyber intrusion activity on U.S. networks—today, with the effect becoming stronger as the level of democracy of the originating country *increases*.

and then communicate the regime message to the citizens encouraging restraint in their internet activities while the negotiations at level-one remain *verbal*. Second, once the outcome of the negotiations become tangible or *material* at level-one, elites receive the narrative and cue their citizens or state-sponsored groups to resume or increase internet activity, with the material long-dashed red line trending consistently above the green dotted line depicting autocratic verbal NNs.

Finally, unlike any of the other models, *increases* in yesterday's negative narrative polarization predicts an *increase* in today's intrusions for autocracies. Apparently, autocracies with their patent lack of media freedoms leads their intrusive population to be triggered by NN polarization indulging in information seeking behavior, scoring a *thirty-fold* shift over the All-Regimes dampening effect shifting to the significantly heightened effect on today's intrusion coming from autocracies.[92] Alternatively, autocratic regimes could use NN polarization to mobilize their hacktivist population either through social movement connections or state-sponsored groups; nevertheless, this mobilization may rely on the two-step process operating within level-two conveying the message to hack.

[92] The model used to derive the AME for autocracies is shared with anocracies and removes the Internet and Media Not Free and Media self-censorship control variables because their values do not vary for autocracies. Thus, the predicted values of NmN, NvN, and NNP are being used holding all of the other variables constant at their mean values, while the prediction estimate is derived, no change in these coefficient value resulted from removal these control variables, which allows for prediction of the AME in this case. Therefore, through use of the NN polarization values in the table in Figure 14, the All-Regime records an average marginal effect of -0.9696 intrusions across the x-axis range, while autocracies score a growth of +27.9613 across the same range, an increase of intrusions thirty times greater [(27.9613– (-0.9696) / 0.9696 = 29.8 ~ 30) than the All-Regimes model.



<u>Media Variable Prediction Comparison Table: Autocracies</u>

Model or Regime Type / Calculated Variable	**All-Regimes**	**Autocracies**	**Difference from All-Regimes**
NmN: **AME on Intrusions** +/- / (SE)	0.3540*** (0.0186)	16.3975*** (0.3311)	16.0435*** (0.3316)
NvN: **AME on Intrusions** +/- / (SE)	-2.1057*** (0.0128)	-14.8539*** (0.1488)	-12.7482*** (0.1493)
NNp: **AME on Intrusions** +/- / (SE)	-0.9696*** (0.0601)	27.9613*** (0.8279)	28.9309*** (0.8301)

Notes:
Average Marginal Effect (AME)
Negative Material Narrative (NmN)
Negative Verbal Narrative (NvN)
Negative Narrative Polarization (NNp)
Standard Error (SE)

Statistical Significance – p-Level:
***p < 0.01; **p < 0.001; ***p < 0.0001**

Figure 14. Media Results: Autocracies.

This explanation does not imply consistency of direction in that *verbal* always leads to *material*, certainly, the opposite could occur. Further, the polarization of NN's could occur at any time in the process. Nevertheless, these three pieces taken together describe how the two-step process theory operates and reinforces communications and control within level-two of domestic relations in autocracies, as shown graphically in Figure 14. Thus, by reviewing this statistical evidence discussed here, the research provides evidence to support hypotheses H1, H4, and H6, which surmise that this phenomenon operates in autocracies.[93]

Interestingly, as shown in Figure 14, notice how the material and verbal result from the autocracies appear to mirror those from the All-Regime model, except each clocks in at a much higher average marginal effect. Notice in Figure 14, it is easy to see that negative material narratives score a *forty-five-fold* increase in predicted intrusions, while verbal narratives record a *six-fold* decrease in intrusions, above or below the corresponding All-Regimes' AME values. Yet, the researcher still cannot account for the fact that the set of intruders might use IP anonymizers or ONION routing to mask the true origin of the intrusion. Nevertheless, the model remains consistent in its predictive properties across all regime types at this level of analysis, as shown above, in the plots in Appendix F, and in the model coefficient comparison plots in Appendix I.

F. CONCLUSION

This chapter began by describing the macro model and the eleven focused models, displaying their output statistics in Appendix D. Subsequently, the basic *Poisson* distribution model was chosen because it best fit the discrete, per country-day data, and recorded the lowest Mean Average Error (MAE) and Root Mean Square Error (RMSE) calculated from the test sample drawn from the main data set used in this research. Then, the research focused the chosen model on those countries that reported negative narratives directed at the U.S. over the period of analysis. This next level of research began with an

[93] **Hypothesis #1 (H1):** *Increases* in the number of conflictual *material* interactions reported in the media narratives of other sovereign states directed at the United States (U.S.) and its interests—yesterday, regardless of regime type, results in *increased* cyber intrusion activity on U.S. networks—today.

Hypothesis #4 (H4): *Increases* in the number of conflictual *verbal* interactions reported in the media narratives of **autocratic** states directed at the United States (U.S.) and its interests—yesterday, results in *decreased* cyber intrusion activity on U.S. networks—today.

Hypothesis #6 (H6): *Increases* in the variation of negative narrative tone, indicating an increased level of media polarization, across media stories originating from **autocratic** states directed at the U.S. and its interest—yesterday, results in an *increase* in cyber intrusion activity on U.S. networks—today.

All-Regimes' Negative Narratives model and then proceeded to apply the model to different regime-types: democracies, anocracies, and autocracies. The research revealed that negative *material* narratives *today* strongly correlated with cyber intrusion attempts on U.S. networks *tomorrow* across *all* regime types. These results supported the expectations of H1 across all regime types. Next, the research discovered that negative *verbal* narratives emanating from democracies *today* also increases intrusions on U.S. networks *tomorrow*, allowing for the acceptance of H2 and the rejection of the null hypothesis.

Subsequently, the research analyzed how yesterday's negative *verbal* narratives generated by anocracies and autocracies resulted in no effect (i.e., no correlation) or a dampening effect (i.e., negative correlation) on cyber intrusion attempts on U.S. networks today, respectively. These results support the expectations for H3 and H4, as well. Next, the NN polarization coefficient was evaluated for each model, finding increased NN polarization—yesterday resulted in fewer intrusions *today* for democracies and anocracies supporting H5. On the other hand, NN polarization in autocracies swung the other direction with increased polarization leading to increased intrusions, which supported and allowed for the acceptance of H6.

Taken together, these results indicate that two-level process theory of international and domestic politics and two-step flow of communication theory operate within anocracies and autocracies (Lazarsfeld, Berelson, & Gaudet, 1944; Putnam, 1988). While these theories may apply within democracies, the analysis at this level does not provide evidence of their operation. However, anocracies and autocracies manifest significant indications that the two-step flow operates and reinforces level-two of domestic politics, providing the population with input on how to respond to negative *material* and *verbal* narratives or NN polarization about the U.S. originating from their country's leadership. At any rate, these actuated hackers, who may be individuals, part of a social movement groups, or state-sponsored actors (which is impossible to determine precisely with this dataset) appear to be conducting these intrusions.

Finally, in reviewing the analysis of the interactive variables, H7 holds across All-Regimes and anocracies indicating that increases in NN tone decrease cyber intrusions as the level of democracy becomes more positive. However, H7 was rejected for democracies and autocracies as it appears that increases in NN tone increase intrusions coming from autocracies and democracies at higher levels of democracy within each regime types. Although intrusions decreased across the x-axis range as the NNs became more negative for both regime types, in each case higher levels of democracy produced more intrusions, a finding that the research will explore in subsequent chapters. In these case study chapters, the research will explore each of these regime types down to the country level to ascertain whether the hypotheses remain valid at deeper levels of analysis or whether differing hypotheses should be offered at the country level based on closer examination. Logically, the case study starting point will begin where this chapter ended, with autocracies.

THIS PAGE INTENTIONALLY LEFT BLANK

IV. CASE STUDIES: AUTOCRACIES IN CYBERSPACE

A. INTRODUCTION

Autocracies appear to manifest some unique characteristics in this media effect realm and its impact in cyberspace. This research will explore two countries with frequent and ongoing contact with the United States-China and Iran. For a complete list of the nineteen autocracies and all the other countries, per regime type, the reader can review Appendix G.

First, this chapter will begin by briefly introducing how autocracies view and use cyberspace. Second, the case study will survey the extent literature to examine the similarities and differences between China and Iran, focusing specifically on how they control the internet, the narrative, and its impact on their unique civil societies. As the exploration of these nuanced civil societies proceeds, other hypotheses will be proffered for both countries. Thirdly, the author provides a brief review of some of the conclusions discovered about autocracies using the model introduced in the last chapter. Finally, the researcher shall apply the existing model described in the previous chapter to China and Iran to discern how yesterday's negative material and verbal narratives, tone, and variation affect cyber-intrusions on U.S. networks.

B. AUTOCRACY IN THE THIRD WAVE

Autocratic regimes span across countries that include China, Cuba, Iran, Kazakhstan, North Korea, and Syria (Marshall & Cole, 2014; Marshall & Elzinga-Marshall, 2017). These states approached the adoption and use of the internet slowly at first potentially due to their inability to control the information on it, their initial lack of understanding of it, and their reticence to embrace this technology due to its alleged democratic properties (Morozov, 2011). However, their pace of adoption and use began to accelerate in the early 2000s, because autocrats began to understand how to use the internet to *efficiently* meet the Orwellian needs of every autocracy—the unencumbered use of *censorship, propaganda,* and *surveillance* to sustain the status quo at home and gain influence abroad (Morozov, 2011, p. 82; Orwell, 1949; Rød & Weidmann, 2015; Walker, Kalathil, & Ludwig, 2020).

Thus, some autocracies proceeded slowly in their adoption of the internet, presumably due to WWW's inherit characteristic of enabling open and transparent access to media in its many forms. Some have conjectured how the internet spawned many apparently *leaderless* protests from the Philippines (2001) to Iran (2009 / 2017–2018), viewed by scholars as one side of the *dictator's dilemma (Al Jazeera, 2018; Shirky, 2011; Morozov, 2011)*. The other side being a dictator's understanding that any state not connected to the internet will remain behind economically and technologically, both threats to the longevity of an authoritarian regime (Morozov, 2011, pp. 93-97; Shirky, 2011). Many believed that the internet would allow repressed populations to access the global media sources. This media exposure would transform their citizens into netizens, thereby enlightening them to the means with which autocratic regimes maintain control of their countries. Ultimately, this would spawn a social movement within these countries and lead to democratization-*liberation technology* theory (Diamond, 2010; Gunitsky, 2015; Morozov, 2011; Rød & Weidmann, 2015; Shirky, 2011; Stier, 2017).[94] However, what liberals and realists, neo or otherwise, fail to realize is that any new technology can lead to multiple often *unexpected* uses and outcomes.[95] For example, while western democracies

[94] Netizen – citizen of the internet (Diamond, 2010; Lindsay J. , 2014).

[95] Liberalism – an analytical approach to international relations where states are part of a global society that modulates their interactions based on norms and rules established through interaction, initially through transnational and more recently international trade (Nye J. S., 2007, p. 288). National borders signify moral importance because states represent the collective ideals and rights of the peoples inhabiting them; thus, it follows that respect for the sovereignty and territorial integrity of a given state shows respect for the rights of its citizens (Nye, 2007, pp. 23-24; Walzer, 1977; Walzer, 1980).

Neo-Liberalism – similar to liberalism except that state actions are constrained by economic interdependence and international institutions (Nye, 2007, p. 288).

Realist – an analytical approach to interstate relations based on the societal, economic, or military power structure. Individual states react, interact, and counteract the actions of other states to maintain their power base, in effect, attempting to strike a balance. This concept of balance of power is foundational to the realist. Each state continually seeks to defend or expand their territory or interests, to grow their economy, or to enhance their influence internationally. For the realist preserving the balance of power creates order, which leads to peace – a moral imperative (Morgenthau, 1947; Nye, 2007, p. 25; Waltz, 1979). Morality requires that states make tradeoff choices as they seek to maintain or better their position on the world stage (Nye, 2007, p. 23). Regardless of the tradeoff choices made by the states involved in a given interaction and irrespective of just or unjust nature of the peace achieved, if order and balance were maintained – the ends view the internet as a *liberating technology*, authoritarian regimes may use it as a *repressive technology* employed to censor, propagandize, surveil, and trace their populations (Deibert, 2015; Greitens, 2013; Mackinnon, 2011, 2012; Morozov, 2011; Quinn, 2017; Rød & Weidmann, 2015).

This chapter will explore the two autocracies at the center of this study: China and Iran. The former a well-established communist regime, which chooses to compete regionally and globally effectively using all instruments of national power. The later, a theocratic republic, often appears at odds with itself, desperately trying to hold itself together, while draining its resources by engaging in proxy wars jousting with its regional and global rivals. Though both are autocracies, each possesses different levels of proficiency and capability, choosing to use their stylized versions of the internet as a repressive technology domestically and as an instrument of influence, coercion, and industrial espionage abroad.[96]

Each created their own version of a national internet or state *intranet*, as a proactive measure (Golkar, 2011; Rahimi, 2015). Iran created the *Halal* internet and China's version resides behind the Great Firewall of China (Akgül & Kirlidoğ, 2015; Aryan, Aryan, & Halderman, 2013; Barme & Ye, 1997; MacKinnon, 2012; Morozov, 2011; Pinkaew, 2016).[97] Both created their respective national internets to maximize control, optimizing their regimes' ability to swiftly censor any narratives critical of state policy and replace

justify the means. The realist views the tradeoffs between justice and order as situationally dependent; further, the spatial and temporal position of the state matters in the transactional nature of international affairs.

Neo-Realist – an analytical approach to interstate relations in which each state's actions are governed by the structural balance of military power (Nye J. S., 2007; Waltz, 1979).

[96] Non-Monarch autocracies seem to follow similar patterns in cyberspace seeking to gain a capability through espionage or theft (Lindsay & Cheung, 2015; Stier, 2017; Valeriano, Jensen, & Maness, 2018). Authoritarian regimes find it difficult to foster innovation while propagandizing, censoring, or surveilling their populations; thus, stealing intellectual property or national security secrets from more innovative states provides a suitable alternative to nurturing homegrown innovation when competing with an ingenious rival (Lindsay & Cheung, 2015; Stier, 2017; Valeriano, Jensen, & Maness, 2018). Yet, dependence on industrial espionage not only stifles domestic innovation, but also may not necessarily ensure that the state parlaying in stolen technologies can even replicate the manufacturing process necessary to achieve the capability (Lindsay & Cheung, 2015; Stier, 2017; Valeriano, Jensen, & Maness, 2018, p. 165). Most other non-monarch, authoritarian regimes follow the same behavior patterns, although regionally (Valeriano & Maness, 2015; Valeriano, Jensen, & Maness, 2018).

[97] Halal – in Arabic means lawful, referring to any object or act considered as permissible under Islamic law (MacKinnon, 2012, p.55).

them with propagandized stories favorable to the regime, while simultaneously sustaining a surveillance apparatus efficient enough to know precisely what their citizens are discussing and with whom (Akgül & Kirlidoğ, 2015; Aryan, Aryan, & Halderman, 2013; Barme & Ye, 1997; MacKinnon, 2012; Morozov, 2011; Pinkaew, 2016; Ruijgrok, 2017).

In this aspect, China displays a remarkable level of sophistication far superior to other autocracies including Iran (Akgül & Kirlidoğ, 2015; Deibert, 2015; MacKinnon, 2012; Morozov, 2011; Rød & Weidmann, 2015). China leverages quantity over quality of intrusion, as seen in Appendix J, while Iran appears to employ the intrusion level necessary to achieve their goal. Ultimately, each state's capacity drives their customized use of the digital panopticon, leading each to employ their capabilities in different ways; yet, most strive to achieve China's level of efficiency (Deibert, 2015; Hussain M. M., 2016; MacKinnon, 2012; Morozov, 2011). Indeed, these cultural and economic differences imply how each state views the use and the employment of the internet to further their specific domestic and international aspirations in cyberspace.

1. China in the Third Wave

Internally, China can only be described as a true digital panopticon, both digitally and physically (Greitens, 2013; Gunitsky, 2015; Hussain M. M., 2016; MacKinnon, 2011; Morozov, 2011; Ramli, Bergen, & Hunter, 2018; Rød & Weidmann, 2015; Shi, 2020). Again amongst authoritarians, China remains the leader in sophisticated censorship tactics, techniques, and procedures, which allows the regime to effectively surveil and propagandize its population, using censorship to quash any organized dissent and to control the media narrative—simultaneously by leveraging the internet and its capabilities (Custer, Prakash, Solis, Knight, & Lin, 2019; Freedom House, 2017; Greitens, 2013; King, Pan, & Roberts, 2013; Lindsay, 2014; Richet, 2013; Stockmann & Gallagher, 2011; Wang & Minzner, 2015; Zittrain, et al., 2017).[98] Employing the most advanced use of artificial

[98] The Chinese continue to hone their methods of controlling the media narrative in cyberspace, beginning in the mid-1990s, through a sophisticated labyrinth of censorship and surveillance created by a public-private partnership between the internet providers and the Chinese government (Greitens, 2013). This sophisticated means of control begins with censorship policies placed on internet providers making them accountable for any content seen as anti-regime or subversive (Barme & Ye, 1997; Greitens, 2013; Lindsay J. , 2014; MacKinnon, 2011; Morozov, 2011; Rød & Weidmann, 2015; Shirky, 2011; Stier, 2017). This

intelligence (AI) to surveil the Chinese population, unencumbered by any of the moral quandaries that accompany the use and development of AI (Ramli, Bergen, & Hunter, 2018).[99] Further, by enacting restrictive telecommunications laws and regulations or by simply owning the Internet Service Providers (ISP) outright, the People's Republic of China (PRC) in effect controls Chinese society through the efficient use of censorship, surveillance, and propaganda (Deibert, 2015; Golkar, 2011; Greitens, 2013; Lindsay, 2014; Morozov, 2011; Rød & Weidmann, 2015; Shirky, 2011; Stier, 2017).[100]

Many western companies, who provide internet services in China, chose to submit to the PRC demands for censorship and surveillance (Deibert, 2015; Greitens, 2013; MacKinnon, 2011; MacKinnon, 2012; Morozov, 2011; Quinn, 2017; Rød & Weidmann, 2015). The economic advantages of having a presence in the Chinese market are just too lucrative; however, for some companies the cost is too high. For example, Google chose not to submit to demands for monitoring, removing, and reporting online content dubbed

coerces private ISPs to establish unique departments whose sole purpose is to police users and censor content to avoid the possibility of fines, license termination, or shut down by the Chinese government (MacKinnon, 2011, p. 38; MacKinnon, 2012, p. 36). Above the internet providers exists an elaborate bureaucracy of Ministries, Bureaus, and Offices with subordinate organizations reaching down to the provincial, municipal, and county level policing media and online content (Greitens, 2013). Within these bureaucracies reside the internet police, who enforce the internet laws and can penalize anyone from the internet provider down to the individual. These internet police may incarcerate any Chinese citizen for creating transgressive content (i.e., political dissent, collective action, social mobilization, etc.) (Greitens, 2013). Rebecca Greitens (2013) estimates the size of Chinese Internet Police Force to be between 20,000 and 50,000. This organization possesses the authority to warn, detain, arrest, or imprison anyone with China's jurisdiction suspected of engaging in political dissent (MacKinnon, 2011). Further, the regime added another larger layer for depth, known in e-parlance as the fifty-cent party. Retired Chinese Communist Party (CCP) members, college students or other citizens who may be aspiring to join the CCP fill the ranks of the fifty-cent party and receive half a yuan (~ 50 cents) for positive post, blog, electronic statement made online about the regime (Deibert R. , 2015; Greitens, 2013; King, Pan, & Roberts, 2013). The fifty-cent party's size is estimated to be approximately 250,000 to 300,000 strong (Greitens, 2013; MacKinnon, 2011; MacKinnon, 2012). This group of paid volunteers monitor content, report political deviant narratives, and author positive regime storylines – essentially guiding the on-line conversation toward themes complementary of the CCP and the government (Greitens, 2013; MacKinnon, 2011; MacKinnon, 2012).

[99] Artificial Intelligence (AI) – the theory and development of computer systems able to perform tasks that normally require human intelligence, such as visual perception, speech recognition, decision-making, and translation between languages (Oxford Dictionary, 2015, sec. "AI").

AI's moral quandaries have been showcased in science fiction literature as well as motion pictures. The scenario usually involves the unfettered development of AI by mankind followed soon after by an uprising of artificially intelligent machines bent on dominating or destroying humanity.

[100] Internet Service Provider (ISP) – An organization that provides access to the Internet, as well as other services such as web hosting or e-mail. It is a primary control point, since all traffic from an individual or organization flows through its ISP (Singer & Friedman, 2013, p. 74). Synonymous with Internet Provider in this paper.

unlawful by the PRC leaving mainland China (i.e., .cn domain) for Hong Kong (i.e., .hk domain) in 2010 (Lindsay, 2014; MacKinnon, 2011; MacKinnon, 2012; Morozov, 2011; Nye, 2011; Quinn, 2017).

The Chinese system consists of a legally justified, interlocking behemoth of technology enabled humanity, which effectively monitors, modifies, blocks, or removes content, deemed as transgressive, replacing it with media narratives favorable to the regime's actions, objectives and policies (Greitens, 2013; MacKinnon, 2011; MacKinnon, 2012; Ruijgrok, 2017). Further, Stockmann and Gallagher (2011) discovered that the majority of Chinese citizens, mainly in urban centers, were susceptible to believe media messaging particularly when stories covering social problems or legal grievances, principally at the local-level, were sensationalized. Additionally, they found consistent flow of information (i.e., propaganda) contributed to the tractability of media messages (Stockmann & Gallagher, 2011).

Simultaneously, this Chinese digital panopticon enables the efficient surveillance of their properly propagandized population.[101] In 2014, the Chinese Communist Party (CCP) rolled out the Social Credit System (SCS), about five years after India began its similar Aadhaar project, which will be discussed in the democracy case study. However, the CCP had been planning for the establishment of a SCS and its envisioned Orwellian capabilities since 2002 (Botsman, 2017; Creemers, 2018). Initially, the SCS was described by the state-run media as being similar to the credit systems (i.e. Equifax, Experian, & TransUnion) used in capitalist economies to evaluate a citizen's financial creditworthiness (Creemers, 2018; Shahin & Zheng, 2020). Yet soon after, the CCP media narrative quickly morphed into a description of SCS as a system that also evaluated an individual citizen's sincerity, trustworthiness, and creditworthiness, revealing their true intention (Creemers, 2018; Shahin & Zheng, 2020). The additions of sincerity and trustworthiness allow for the CCP to *monitor* and *track* an individual's social associations, behavior, contacts, online activity, and what bills or taxes they paid or did not pay (Botsman, 2017; Shahin & Zheng,

[101] In China, political dissent of any type, broadly defined, is a punishable crime (MacKinnon, 2011, p.41; MacKinnon, 2012).

China's population was estimated to be 1,382,323,332 (Internet Users by Country, 2017).

2020). Further, the development of the SCS allows for the CCP to electronically *centralize* its power structure making it the guarantor of sincerity, trustworthiness, and morality (Creemers, 2018).[102] Ultimately, positioning itself as morally superior to local authorities (Creemers, 2018, p. 6). A theme played out in state-media narratives that will be discussed later.

In conjunction with this advanced system of societal control provided by the SCS, the PRC developed the proactive measure of creating a state-sponsored high-speed internet alternative in order to stave off their citizen's use of western media outlets and platforms (Diamond, 2010; Greitens, 2013; MacKinnon, 2012; Rahimi, 2015; Walker, Kalathil, & Ludwig, 2020; Zittrain, et al., 2017). Thus, empowering the regime to maintain absolute control of the tone, type, and variation of domestic narratives, which remain the focus of this study.

The PRC's main motivation for creating this vast digital panopticon appears focused on the prevention of *any* social unrest, public demonstrations or dissent, and collective action or expression, while allowing criticism of some local or state officials and policies (Custer, Prakash, Solis, Knight, & Lin, 2019; Greitens, 2013; King, Pan, & Roberts, 2013; Lindsay, 2014; Richet, 2013; Stockmann & Gallagher, 2011; Wang & Minzner, 2015). On the surface, this may appear to be oxymoronic; however, the Tiananmen Square demonstration and the nearly coincidental fall of the former Soviet Union motivated elites within the CCP to proactively monitor and prevent social unrest, while allowing some criticism and legal leveeing of grievances with local and state officials or policies, using the later to prevent the former (Cong, 2013; King, Pan, & Roberts, 2013; Stockmann & Gallagher, 2011; Wang & Minzner, 2015). As such, the Chinese digital panopticon allows for some dissent with *local* or state officials and/or policies, but harshly censors any narrative residing in the semantic layer encouraging, emboldening, or inspiring any type of collective action, dissent, or protests (Custer, Prakash, Solis, Knight, & Lin,

[102] Enrollment and participation in the SCS will be mandatory throughout China by 2020, which is also when each citizen will receive their first SCS score (Botsman, 2017).

2019; Greitens, 2013; King, Pan, & Roberts, 2013; Lindsay, 2014; Richet, 2013; Wang & Minzner, 2015).

Further, by banning the use of virtual private networks (VPN)s and IP anonymizers, such as TOR, the PRC further cements its grasp on the narrative (Akgül & Kirlidoğ, 2015; Deibert, 2015; Ensafi, Winter, Mueen, & Crandall, 2015; MacKinnon, 2011; Morozov, 2011). Thus, in China, the true digital Panopticon exists, allowing for the censoring and control of information residing in the semantic layer. Enabling them to effectively employ the information instrument as *sharp power* to bend the harmonized domestic and international narrative to their will (Custer, Prakash, Solis, Knight, & Lin, 2019; Diamond, 2018; Walker & Ludwig, 2017; Walker, Kalathil, & Ludwig, 2020).

Externally, China led the way amongst the top 10 states across the globe who engaged in rivalrous cyber disputes between 2000 and 2014, potentially, because of its desire to gain and maintain position as a regional hegemon and a global challenger of the U.S. and its policies (Valeriano & Maness, 2015; Valeriano, Jensen, & Maness, 2018, p. 73). As such, most of the cyber incidents initiated by China began with a malicious vector (~ 95%) leading ultimately to an information seeking objective (~ 79%) (Valeriano, Jensen, & Maness, 2018, pp. 143-170).

The Chinese objectives span from stealing intellectual property or weapon system plans, to covertly surveying network vulnerabilities, which they intend to exploit at some future date (Axelrod & Iliev, 2014; Lindsay, 2014; Valeriano & Maness, 2014; Valeriano & Maness, 2015; Valeriano, Jensen, & Maness, 2018).[103] Simply, China pursues this information seeking behavior, preferring mass over cyber sophistication in their intrusions (see Appendix K), to surveil the U.S. and its regional rivals, to monitor plans and capabilities in all domains, and to ensure that no other state is able to achieve predominant competitive advantage (Axelrod & Iliev, 2014; Ball, 2011; Lindsay, 2014; Porter, 1991; Valeriano & Maness, 2014; Valeriano & Maness, 2015; Valeriano, Jensen, & Maness,

[103] China’s malicious intent method calculation equates to 58 out of 61 incidents equating to 0.9508 or approximately 95% (Valeriano, Jensen, & Maness, 2018, p. 160). The information seeking intent calculation equates to 48 out of 61 incidents equaling 0.787 or approximately ~ 79% (Valeriano, Jensen, & Maness, 2018, p. 158).

2018).[104] Further, China's cyberspace capability is augmented by a well-resourced and well-cultivated labyrinth of influence leeching into academic, entertainment, and commercial sectors of their global and regional rivals, employing what some scholars have described as *sharp power* (Custer, Prakash, Solis, Knight, & Lin, 2019; Diamond, 2018; Walker & Ludwig, 2017; Walker, Kalathil, & Ludwig, 2020).

Even though China does not have established doctrine like the reflexive control, advanced by the Soviets, their actions reflect what realists describe as *sharp power*. China's patience in husbanding the development of their influence network abroad is impressive, spanning across academic, entertainment, and commercial sectors.[105] Inevitably, their effort to cultivate influence has bolstered their impact abroad. When the PRC chooses to prudently use their influence, they bend the narrative to suit Chinese interests internationally (Diamond, 2015; MacKinnon, 2012; Nathan, 2017; Walker & Ludwig, 2017; Walker, Kalathil, & Ludwig, 2020; Wong, 2020). Domestically, the PRC seeks to stifle any opposition, whatsoever, by simultaneously saturating the domestic media narrative with normative stories tightly aligned with the PRC objectives (Diamond, 2010; Freedom House, 2017; MacKinnon, 2011; Morozov, 2011; Walker, Kalathil, & Ludwig, 2020; Wong, 2020).

Thus, through its influence abroad and control domestically, China employs a vast array of informational tools. These tools underpin PRC's ability to effectively manage the international narrative, while controlling domestic storylines, residing in Habermas' (1991) public sphere, in effect controlling the two-step process operating within and reinforcing within level-two domestically within China. Essentially, the PRC manipulates the levers in

[104] As for remainder of these incidents (~ 21%), China intends to manifest their cyber capability with a subversive intent to pushback, metaphorically speaking, against the U.S. or other competitors (Valeriano, Jensen, & Maness, 2018, pp. 143-170).

[105] In academic circles, they provide scholarships, fund research, and create academic partnership through their Confucius Institute network across the globe (Custer, Prakash, Solis, Knight, & Lin, 2019; Diamond, 2018; Walker & Ludwig, 2017). Their span of influence in the commercial realm is vast, with their low cost of labor, many private sector companies have come to rely on China for their supply chain needs, which include the assembly, manufacture, and transportation of products destine for global markets. (Lindsay, 2014; Tripp & Kubota, 2020). Indeed, as seen during the recent coronavirus outbreak, a disruption in China can lead to a global disruption (Tripp & Kubota, 2020). Yet, in either case, whether it is access to Chinese research funding on the academic side or access to Chinese markets on the other, each is contingent on compliance with the PRC's state objectives and narrative (Diamond, 2018).

the digital Panopticon, allowing the elite narratives of the CCP to dominate their national media environment and effectively squelching any dissenting stories or messages that run counter to their objectives. Their manifest ability to control the level-two narrative, via the two-step process, allows the Chinese greater opportunities in level-one negotiations (Bjola & Manor, 2018; Conceição-Heldt & Mello, 2017; Putnam, 1988; Strong, 2017; Trumbore, Boyer, Gibson, Harvey, & Wilkenfeld, 2000).

Previously, in Figure 14 in Chapter III, this research provided evidence of the operation of the two-step flow of information within level-two domestically for autocracies. Further, Figure 14 quantified how increased NN polarization in today's media stories directed at the U.S., leads to increased intrusions tomorrow. Additionally, the evidence shown in Figure 13 in Chapter III, also indicated that increases in NN tone on a given day in autocracies corresponded to a decrease in cyber intrusions on the following day. Particularly when considering the green line in Figure 13, it predicts a decrease of intrusions on the day following the narrative as the NN tone becomes more negative for countries comparable to China and Iran who come in at a higher level of democracy amongst the autocrats (i.e., –7). Perhaps, these autocracies use negative media tone as a way of controlling domestic politics at level-two, while the rhetoric at level-one heats up in reference to a given issue between some autocracy and the US.

Thus, the next step in this research will be to separate the Chinese negative narratives and cyber intrusions from those other countries in the data set. Then use the model, described in Chapter III, to discern if Chinese negative narrative types, variation, and tone on a given day effects cyber intrusion attempts on U.S. networks the next day. As such, the research seeks to use the previous model applying it to this dyadic relationship between China and the U.S. to test the hypotheses proffered in Figure 15.

Hypothesis #8 (H8): *Increases* in the number of conflictual (i.e. negative) *material* interactions reported in Chinese media narratives directed at the United States (US) or its interests—yesterday, results in *increased* cyber intrusion activity, emanating from China, on U.S. networks—today.

Hypothesis #9 (H9): *Increasingly* conflictual (i.e. negative) *verbal* interactions reported in Chinese media narratives directed at the United States (US) and its interests—yesterday, results in *decreased* cyber intrusion activity, emanating from China, on U.S. networks—today.

Hypothesis #10 (H10): *Increases* in the variation of negative narrative tone, indicating an increased level of media polarization, across media stories originating from China directed at the U.S. and its interests—yesterday, results in *increased* cyber intrusion activity on U.S. networks—today.

Hypothesis #11 (H11): *Increases* in the conflictual or negative *tone* of interactions reported in media narratives from China directed at the United States (US) and its interests—yesterday, results in *decreased* cyber intrusion activity on U.S. networks—today.

Figure 15. China – Case Study Hypotheses

Many states emulate different aspects of China's manifest capabilities, but none can surpass the sheer breadth and capability attained by its regime. Iran provides an object lesson of how authoritarians imitate the *Chinese way* of taking the slow yet deliberate path of internet diffusion within their populations (MacKinnon, 2011; MacKinnon, 2012; Morozov, 2011).[106] In this research, Iran appears to be walking that deliberate path, but does not seem to possess the apparent capacity either in population nor in resources necessary to achieve China's level of societal control. However, where they have gaps in technology, the Iranians cover with humans, using the same tactics and procedures to achieve similar, if not more effective results on their population.

[106] First, by allowing the government to become familiar with the domain (Greitens, 2013; Morozov, 2011). Next, they emplace controls to manage censorship and surveillance capabilities, build the infrastructure, and establish the necessary legal governance to legitimize their control. Finally, they begin to allow access, first to the elites and then slowly to the public writ large (Greitens, 2013; Morozov, 2011).

2. Iran in the Third Wave

On the world stage, the Islamic Republic of Iran (IRI) faces different circumstances than China, which causes the regime to approach their censorship and surveillance capabilities, brought about by advances in information technology, differently. First, Iran's relationship with the West writ large, particularly with the U.S., has flirted with cooperation, but by and large remains rivalrous and conflictual to date. Secondly, as stated in Chapter II, Iran often hurts itself both regionally and internationally as it lashes out at its rivals, eroding its position globally and draining its resources domestically, as is common with most locked in—long standing rivals. For example, Iran involves itself in regional proxy wars (i.e., Iraq, Syria, and Yemen), which engenders western countries to impose economic sanctions. Sanctions result in domestic shortages falling the hardest on the average Iranian, ultimately isolating the regime internationally and causing domestic strife and protests (Ansari, 2017; Henry, 2018; Mattis, 2018; Price, 2012; Sadjadpour, 2020; Valeriano & Maness, 2015; Zittrain, et al., 2017). Thirdly, Iran's leadership over the past 25 years has oscillated from reformists, to Islamic fundamentalists, and now to moderates residing between the two extremes (Ansari, 2017; Best & Higley, 2018; Blout, 2017; Golkar, 2011; Hussain, 2016; Jones & Newlee, 2020; Pollack, 2004). These extremes have taken their toll on the Iranian economy and its people, manifesting itself in their control, establishment, and use of the internet. Specifically, the era under the Islamic fundamentalist leadership of Mahmood Ahmadinejad (2005–2013) saw the build out of the Iranian version of the digital panopticon setting in place many of the elements necessary to effect societal control, albeit focusing on First-Gen internet content controls (Blout, 2017; Deibert & Rohozinski, 2010; Golkar, 2011; MacKinnon, 2012; Morozov, 2011; Price, 2012; Rahimi, 2011).

On the international stage, Iran remains constrained and clandestine in its chosen cyber tactics (Valeriano & Maness, 2015; Valeriano, Jensen, & Maness, 2018). Iran ranks seventh among the top 10 states that engaged in rivalrous cyber disputes between 2000 and 2014 (Valeriano, Jensen, & Maness, 2018, p. 73). In general, Iran tracks closely with many of China's autocratic techniques of cyber incidents choosing malicious vector as their method of choice for gaining access to their rival's networks.[107] However, Iran's cyber objectives do not align with China's. More often, Iran seeks to achieve a subversive intent (~ 60%) with an information seeking objective coming in second (~ 40%).[108] Iran appears set upon using the information instrument to push back against the power or influence of their regional (i.e. Israel, Saudi Arabia, etc.) and global rivals (i.e., the US), ultimately seeking to demonstrate their cyber prowess, while in general falling far behind its rivals in cyber sophistication (Anderson & Sadjadpour, 2018; Lindsay, 2013; Maness & Valeriano, 2016; Valeriano, Jensen, & Maness, 2018; Valeriano & Maness, 2015).[109] Their use of cyber tactics runs parallel with their use of terrorism, because Iran cannot compete militarily with its rivals (Findley, Piazza, & Young, 2012; Valeriano & Maness, 2015). Thus, it deliberately chooses these low-cost tactics to coerce, deter, or pushback its adversaries, which provides plausible deniability and shows restraint, while resisting their rival's manifest desires (Lindsay, 2013; Maness & Valeriano, 2016; Valeriano & Maness, 2015; Valeriano, Jensen, & Maness, 2018).

The Iranians regime manifests a peculiar obsession with the West, particularly the U.S., seeing every action, deed, or statement made by the West, however benign, as an attempt to exert undue influence over their country and culture (Ansari, 2017; Blout, 2017; Golkar, 2011; Jervis, 1976; Heradstveit, 1979; Maoz, 1990; Maoz & Mor, 2002; Price, 2012). Certainly, ample historical facts exist of the West applying an outsized influence over Iranian internal affairs, which has resulted in this quasi-phobic regime behavior pattern (Blout, 2017; Pollack, 2004; Price, 2012). Indeed, this behavior remains consistent with rivalry behavior; yet, it fails to explain why Iran's leadership waxes and wanes in its engagement with the West (Ansari, 2017; Blout, 2017; Golkar, 2011; Jervis, 1976;

[107] Iran's malicious intent method calculation equates to 9 out of 15 incidents equaling 60% (Valeriano, Jensen, & Maness, 2018, pp. 215-224 & 230-237).

[108] Iran's subversive intent objective equates to 9 out of 15 or 60%, with the remainder having a information seeking objective or 6 out of 15 or 40% (Valeriano, Jensen, & Maness, 2018, pp. 215-224 & 230-237).

[109] This lack of cyber sophistication mainly stems from Iran's economic and political isolation, which severely constrains the acquisition of cyber technology and the expertise to use it (Anderson & Sadjadpour, 2018).

Heradstveit, 1979; Maoz, 1990; Maoz & Mor, 2002; Price, 2012). An answer for the later point resides in the regime's power structure.

Domestically, Iran is definitely enigmatic; on the one hand it adheres closely to its constitution, with its elaborate system of checks and balances, and its mandate for periodic elections, which does allow for changes in government from time to time (Ansari, 2017; Freedom House, 2020; Henry, 2018). The most recent election of Hassan Rouhani as President of Iran (2013–present) is believed by many to be a move toward a more moderate position (Best & Higley, 2018; Blout, 2017; Hussain, 2016; Jones & Newlee, 2020; Rahimi, 2015). On the other hand, when Islamic fundamentalist were in charge, under Ahmadinejad (2005–2013), domestic tactics employed by the regime both physically and in cyber space were consistently dictatorial, absolute, and draconian.[110]

The real power in Iran resides in the office of the Supreme Leader, who is simultaneously Commander in Chief of the armed forces and approves the leadership of all three branches of government: judiciary, legislative (i.e., the Majlis), and executive (Ansari, 2017; Baharan, 2009; Freedom House, 2020; Pollack, 2004). The Supreme Leaders possess the authority over who may and may not run for election in the Majlis, the executive, and appointments to the judiciary (Ansari, 2017; Freedom House, 2020; Pollack, 2004; Rahimi, 2016). The Islamic fundamentalists make up the Supreme Leader's

[110] The Islamic fundamentalist believed that very idea of democracy was ill-suited to Iran under its present circumstance (Ansari, 2017). Although, many reformist leaders had dabbled with the idea of democracy, many of the conservatives (i.e. Islamic fundamentalists) believed that politics itself only existed for a chosen few, who had been elected, and thus, were uniquely qualified to rule (Ansari, 2017). Setting aside the elected part, many of the former Shahs and autocratic leaders would have found this line of thought quite familiar (Ansari, 2017; Best & Higley, 2018; Hussain, 2016; Morozov, 2011). The conservatives used this argument as a means to justify the position of the Supreme Leader, their elite position in the regime's power structure, and their need to control the society to shield their population from the secular mores and debaucherous culture of the West (Ansari, 2017; Blout, 2017; Golkar, 2011; Price, 2012; Rahimi, 2016).

powerbase.[111] So, while some Iranian Presidents may dabble with reform and flirt with the West, on occasion, the regime's power structure rests on the conservative Islamic fundamentalists who underwrite the Supreme Leader and serve as the monolithic and immutable basis of this theocratic republic, which in reality operates as a theocratic autocracy (Ansari, 2017; Blout, 2017; Freedom House, 2020; Golkar, 2011; Morozov, 2011; Pollack, 2004; Rahimi, 2016). Thus, as in most autocracies—control of the internet and all IT systems remains a priority in the facilitation of societal control (Blout, 2017; Freedom House, 2020; Golkar, 2011; Morozov, 2011; Pollack, 2004; Rahimi, 2016).

In 1998, soon after internet technology arrived in Iran, a large student protest showed the regime how the students used their internet connections to organize the protest (Golkar, 2011; Jones & Newlee, 2020).[112] Several years later, Ayatollah Khamenei, the current Supreme Leader of Iran, ordered ISPs to begin *filtering* internet websites, shortly thereafter, the Supreme Council for the Cultural Revolution decreed that all ISPs should be brought under state control (Golkar, 2011). This form of state control seems to follow the Chinese model of strict regulation coupled with some ownership, ultimately, placing the onus and responsibility on the ISPs for policing, removing, and reporting content that does not align with regime objectives (Anderson C. , 2013; Aryan, Aryan, & Halderman, 2013; Deibert, 2015; Golkar, 2011; Gunitsky, 2015; Jones & Newlee, 2020; Morozov, 2011; Rahbarqazi & Baghban, 2019; Rahimi, 2015). While Iran's digital panopticon may not have achieved the level of sophistication attained by the Chinese, many scholars have recorded its effectiveness in societal control.

[111] Iran has had two Supreme Leaders Ayatollah Khomeini (1979 – 1989) and Ayatollah Khamenei (1989 – present). They both wore the black turban identifying them as Sayyid or lineal descendants of the Prophet, designating them as religious elites (Ansari, 2017). Both manifested a certain disdain of western democratic system, declaring Iran unfit for such a system of government (Ansari, 2017). Religiously and ideologically, both are closely aligned with the Islamic fundamentalists, who permeate the branches of government, the ruling councils (i.e., the Guardian Council), and the military of Iran (Ansari, 2017; Freedom House, 2020; Iran Development Organization, 2010; Price, 2012; Pollack, 2004). Conservative Islamic fundamentalists make up a large portion of the bureaucratic and elite structures of Iran (Price, 2012). The policy intends to insulate the regime from those Iranians who might be antagonistic of the system and attempt to damage it from the inside out (Iran Development Organization, 2010; Price, 2012).

[112] In 1998, the Iranian regime had chosen to shut down a leading reformist newspaper – Salam, which was the catalyst for the protest (Jones & Newlee, 2020).

The presidency of Ahmadinejad presided over the greatest build out of the digital panopticon across Iran enhancing its censorship, propaganda, surveillance, and tracing capabilities, second only to China (Rahimi, 2011).[113] Over that period, Iran followed China's more deliberate path mirroring its use of censorship and surveillance of the population, while falling short in the propaganda arena and sheer scale (MacKinnon, 2011; MacKinnon, 2012). Further, following China's lead, the Iranian regime grasped the internet's ability to trace, track, monitor, and intercept digital communications. This enabled the regime to leverage this technological nuance to become the world's premier jailer of journalists and bloggers during the 2009 Green movement protests, coming in second behind China in 2010 (MacKinnon, 2012, pp. 54-56). Impressive—considering that, Iran's population is approximately 6% of China (MacKinnon, 2012, pp. 54-56).[114] Further, evidence exists of the use of a time-honored tradition of extrajudicial killings or

[113] The Islamic Fundamentalist regime, building off of Joseph Nye's (2007) Soft Power theory, invented the term Soft War to describe and reify the subtle infiltration of Western culture and ideals into Iranian civil society, first through television and then subsequently through the internet (Blout, 2017; Golkar, 2011; Price, 2012). By consistently using this reified language to describe Iran's relationship with the West and to outline in concrete terms how the West was using media sources to corrode the very foundation of their Islamically pure society, the regime has adequately framed its relations with the West for its population (Blout, 2017; Golkar, 2011; Price, 2012). Consequently, the conservatives built this Soft War narrative to justify their need to defend Islamic ideals against the relentless, decadent attacks exogenously emanating from the West. In effect, using the age-old autocratic trick of focusing their citizens on some exogenous threat to distract them from the corruption and malfeasance of their own government. Finally, the Islamic regime effectively painted the vector of these Soft War attacks as emanating from the internet; thereby, justifying their need to physically and technologically control it through censorship and surveillance, which consequently provide the means to control the narrative through regime generated propaganda.

Ahmadinejad began the build out of the digital panopticon by first resourcing and leveraging the Basij, the paramilitary arm of the Iranian Revolutionary Guard Corps (IRGC), to develop a cyber-capability specifically for censoring content, propagating propaganda, and surveilling the population (Blout, 2017; Golkar, 2011; Jones & Newlee, 2020; Price, 2012; Rahimi, 2011; Rahimi, 2015). In 2010, Price (2012) estimated that annual funding of the Basij arm of the IRGC focused in cyber and the Soft War to be about $10M. The Basij membership stood at approximately 4 million strong in 2010 (Golkar, 2011). In that same year, they had complete built out the digital panopticon by establishing a presence in over 40,000 districts, facilities, offices, organizations, schools, and villages using an exclusive system of internet cafes (Golkar, 2011). Finally, as of 2009, the IRGC gained a controlling interest in the Iranian Telecommunications Company, which manages all ICT hardware and some of the biggest ISPs in Iran – further cementing their control (Alfoneh, 2010; Golkar, 2011). This system allows the Iranian autocracy to effectively surveil the population, censor internet for any content not favorable to the regime, and ensure that all media narratives are laced with Islamic fundamentalist dogma (Blout, 2017; Golkar, 2011; Jones & Newlee, 2020; Price, 2012; Rahimi, 2011).

[114] As of 2016, Iran's population was estimated to be 80,043,146; whereas, China's population was estimated to be 1,382,323,332 (80 / 1,382 = .0578 ~ 6%) (Internet Users by Country, 2017).

enforcement to effectively extinguishing the voices of those that disagree with the regime or its policies (Baharan, 2009; Pollack, 2004).

Iran uses their national internet internally to simultaneously monitor and cloister its population, minimizing access to the outside world, disrupting protest coordination, and attempting to control the domestic narrative by relying heavily on a combination of filtering and throttling, enabled through the use of deep packet inspection (DPI) technologies (Anderson C. , 2013; Aryan, Aryan, & Halderman, 2013; Deibert, 2015; Golkar, 2011; Gunitsky, 2015; Jones & Newlee, 2020; Morozov, 2011; Rahbarqazi & Baghban, 2019; Rahimi, 2015; Solomon, 2020).[115] Essentially, rheostating their netizen's access to outside information, while serving up a daily diet of Islamically pure information that paints the regime and its efforts in a positive light through state-owned, regulated, or controlled media sources.[116]

Further, the Iranian population seems to peer through the propaganda observing the true nature of the regime's intent, which is to maintain societal control by staving off the flow any of transgressive information (Anderson, 2013; Aryan, Aryan, & Halderman,

[115] Throttling – Adjusting or governing the amount of bandwidth to or from a server. The term is often associated with Internet Service Providers (ISPs) that limit the speed to users based on the volume or type of traffic being transmitted (PC Mag Digital Group, 2020, sec. "throttling").

Filtering – A software routine that analyzes incoming data packets and forwards them or discards them based on one or more criteria such as address, range of addresses and type (email, file transfer, etc.). Packet filtering is generally performed in a router, in which case the router is known as a "screening router" (PC Mag Digital Group, 2020, sec. "filtering").

Deep Packet Inspection (DPI) – data travels across the internet in discrete units referred to as packets. Each individual packet contains an address and the piece of content (i.e., photos, e-mails, blog texts, videos …). DPI interrogates each packet traveling through the internet and can severely decrease the packet transit time, which can be used to filter or throttle a specific portion of the internet; further, it can also allow for content manipulation (Akgül & Kirlidoğ, 2015; Anderson C. , 2013; Aryan, Aryan, & Halderman, 2013; Deibert, 2015; Jordan S. , 2017; Rahimi, 2011; Zittrain et al., 2017).

[116] Additionally, Iranian ISP broadband services are traditionally curtailed for the average citizen, in 2010 multiple authors reported that most households were governed to 128 kilobits per second (Kbps), which was extremely slow for the time (Aryan, Aryan, & Halderman, 2013; Golkar, 2011; Sreberny & Khiabany, 2010). In 2020, Ookla Speed Test clocked Iran's download speed at 12.13 megabits per second (Mbps), which is 89% slower than the U.S. (115.67), 85% slower than China (89.43), and 68% (40.75) below the global average (Ookla, 2020; World Population Review, 2020).

Iran's download broadband rate rests at 13.12 mbps in the latest 2020 speed test. In comparison with other countries, Iran reports in at 32 % (13.12 / 115.67 = 32 %) of the U.S. speed or 68% (1 – .32 = .68 ~ 68%) slower than the U.S. The same calculations were made, as show, for China and the average. These rates depict the download speeds, as this is the common measure used for comparison.

2013; Golkar, 2011; Gunitsky, 2015; Jones & Newlee, 2020; Morozov, 2011; Rahbarqazi & Baghban, 2019; Rahimi, 2015; Solomon, 2020). Simply, most Iranian citizens question the veracity of traditional media sources (Blout, 2017; Golkar, 2011; Rahbarqazi & Baghban, 2019; Rahimi, 2011). They view the narratives of their national media as regime propaganda, which drives them to seek out other media forums, with some assuming the role of citizen journalists uploading to blogs or social media platforms, enabling others to comprehend current events inside Iran (Ansari, 2017; Blout, 2017; Golkar, 2011; Rahimi, 2011; Rahimi, 2015; Rahimi, 2016). Thus, the regime's censoring or shuttering of any opposition media reporting has caused Iranian citizens to fill in the gap and perform the function of the idealized fourth estate, leveraging this technologically enabled, discursive space—the WWW (Blout, 2017; Golkar, 2011; Rahbarqazi & Baghban, 2019; Rahimi, 2011; Whitten-Woodring & James, 2012).[117] Therefore, while the two-step flow may operate and reinforce level-two in domestic politic within Iran, the media narratives directed or manipulated by the Iran regime in reference to the U.S. on a given day may not provide a good indicator of cyber intrusions on U.S. networks originating from Iran on the following day. Simply, the type of narratives described by citizen journalists posting to social media may be a better indicator of cyber intrusions, but lie beyond the scope of this research.[118] Thus, the Iranian citizenry may not be activated by increasing negative tone, type, or variation of media narratives directed by the regime toward the U.S. and its interest. Further, the Iranian regime's penchant for control of the internet and its content within their physical borders parallels that of Russia, who views their .ru net as their sovereign territory similar to that of the air, land, sea, and space domains (Choucri, 2012; Deibert & Rohozinski, 2010; Deibert, 2015; Maréchal, 2017; Nocetti, 2015; Valeriano & Maness, 2015; Valeriano, Jensen, & Maness, 2018). As such, the current model will be used to test the following hypotheses.

[117] Fourth Estate – the idealized role of journalism is that it serves as a "watchdog," keeping government honest and watching out for the interests of people (Kovach & Rosenstiel, 2001, pp. 50-53).

[118] Social Media – forms of electronic communication (such as websites for social networking and microblogging) through which users create online communities to share information, ideas, personal messages, and other content (such as videos) (Webster, 2017, sec. "social media").

Hypothesis #12 (H12): *Increases* in the number of conflictual (i.e. negative) *material* and *verbal* interactions reported in Iranian media narratives directed at the United States (US) and its interests—yesterday, results in *decreased* cyber intrusion activity, emanating from Iran, on U.S. networks—today.

Hypothesis #13 (H13): *Increases* in the variation of negative narrative tone, indicating an increased level of media polarization, across media stories originating from Iran directed at the U.S. and its interest—yesterday, results in *decreased* cyber intrusion activity on U.S. networks—today.

Hypothesis #14 (H14): *Increases* in the conflictual or negative *tone* of interactions reported in media narratives from Iran directed at the United States (US) and its interests—yesterday, results in *decreased* cyber intrusion activity on U.S. networks—today.

Figure 16. Iran – Case Study Hypotheses

Thus, the combination of filtering and throttling, enabled by DPI or simply by limiting the speed of the internet to households, allows the Iranian regime to rheostats the internet speed as needed as a form of societal control. Further, while Iranian citizens may be sensitive to increases in NN tone, they may seek media information from sources other than regime-controlled mainstream news, which means that applying the current model to Iran may not provide results consistent with other autocracies, as hypothesized above. Finally, Iran appears to manifest the same level of sophistication in its cyber intrusive tactics but seems to employ them to achieve different objectives. These two later points were buttressed by the findings in Chapter III, when comparing other regime types to autocracies, and will be reviewed in the evidence section to follow. In the following section, this research will apply the existing model to Iran and China to test this set of hypotheses.

C. EVIDENCE OF MEDIA EFFECTS IN CYBERSPACE

At this point, it seems prudent to review where the research left autocracies at the end of Chapter III. The research had provided evidence to support H1, H4 and H6 for autocracies and enabled the author to conjecture that the two-step process operates and reinforces level-two of domestic politics.[119] Basically, in autocratic regimes, the elites within the power structure digest the daily media narratives and telegraph their interpretation to the country's citizens, causing them to act accordingly. Finally, the NN type and polarization of the narrative matter. First, negative material narratives and NN polarization increased today; this predicts a corresponding rise in intrusions on U.S. networks tomorrow. Second, an increase in the number of negative verbal stories on a given day decreases cyber intrusions on U.S. networks on the following day, as shown in Figure 14 in Chapter III.

Further, the analysis in Chapter III (Figure 13) allowed for the research to test and, ultimately, reject H7 at the autocratic regime level of analysis.[120] This analysis showed that for those autocrats among the highest level of democracy for autocracies (i.e. –7) and those with increasing NN tone described in media events about the US–yesterday correlated with a lower level of intrusion attempts on U.S. networks—today. However, those autocracies at successively higher level of democracy intruded at a higher rate than those at lower levels. Thus, even though the autocratic trend was decreasing at all levels of democracy, those autocracies closer to anocracies intruded at a higher rate, a finding running opposite to H7 and causing the researcher to reject H7 for autocracies. Additionally, this finding coupled with the information provided above concerning China and Iran led to the proffering of H10 for China and H13 for Iran in the hopes of gaining a deeper understanding of impact of NN tone in these countries. Thus, the analysis to follow is expected to show that as the NN media tone rises—today, a declining number of

[119] **Hypothesis #1 (H1):** *Increases* in the number of conflictual *material* interactions reported in the media narratives of other sovereign states directed at the United States (U.S.) and its interests—yesterday, regardless of regime type, results in *increased* cyber intrusion activity on U.S. networks—today.

Hypothesis #4 (H4): *Increases* in the number of conflictual *verbal* interactions reported in the media narratives of autocratic states directed at the United States (U.S.) and its interests—yesterday, results in *decreased* cyber intrusion activity on U.S. networks—today.

Hypothesis #6 (H6): *Increases* in the variation of negative narrative tone, indicating an increased level of media polarization, across media stories originating from **autocratic** states directed at the U.S. and its interest—yesterday, results in *increased* cyber intrusion activity on U.S. networks—today.

[120] **Hypothesis #7 (H7)**: *Increases* in the accumulated conflictual or negative *tone* of interactions reported in media narratives from other countries directed towards the United States (U.S.) and its interests—yesterday, results in *decreased* cyber intrusion activity on U.S. networks—today, with the effect becoming stronger as the level of democracy of the originating country *increases*.

intrusions originating from either of these autocrats should occur—tomorrow, as depicted in Figure 13. Since, this polity score is shared by other autocracies (i.e. Cuba, Laos, Vietnam, etc.) at –7, the analyst will seek further evidence in the China and Iran evidence sections to gather before accepting or rejecting the pertinent hypotheses.

Further, the autocratic model tracks well with the All-Regimes model in most respects with the exception of NN polarization sign that tacks positive, as shown above in Figure 14. The expectation is that the Chinese results will parallel with these previous two models. Meanwhile, Iranian citizens do not view their mainstream news media as credible. As scholars have recorded, they appear to rely upon social media news created by citizen journalists, as such, the results for Iran may not prove as reliable as these previous models. Thus, the researcher will test the hypotheses proffered beginning with China followed by Iran.

1. Chinese Evidence

As shown in Table 6, China seems to track quite closely with the All-Regimes and autocracies model in most respects. Showing a higher response from negative *material,* a rate nearly *four times* (~ 3.6) higher than the significantly lessened response to negative *verbal* narratives emanating from China. Also, observe how the NN media polarization coefficient tracks in direction with both types of narratives, but at a higher rate of growth in intrusions across the variation range in Table 6 and Figure 17. Further, notice each of these variables correlates to a high rate of intrusions today from China above that of autocracies, as depicted in Figure 18.[121] Lastly, note the tight small standard error values shown in parenthesis underneath each coefficient. This tightness indicates the extent of each coefficient's variation around its calculated value an indication of model's robustness and goodness of fit.

[121] This is a result of the control variables accounted for in the autocracies model, but not in the China model. The lines in the figure are calculated holding all other regression coefficients at their mean value. Thus, the autocracies model used the mean for population and GDP of all the 19 countries captured in this research, while the China model uses China's population and GDP, which are much higher than the global mean values used in the former model.

Table 6. Results of Negative Narratives Models for China and Iran.

CYBER INTRUSION ATTEMPTS – Today (Autocracy Comparison)				
	Dependent Variable			
	TotalIntrusions – Today			
	Poisson Model			
Independent Variables (Yesterday) / Model	All Negative Narrative	Autocracies	**China**	**Iran**
Negative Material Narratives	**0.03*****	**0.14*****	**0.42*****	**–0.12*****
	(0.002)	**(0.002)**	**(0.003)**	**(0.004)**
Negative Verbal Narratives	–0.24***	–0.23***	0.09***	–0.22***
	(0.002)	(0.002)	(0.003)	(0.004)
NN Gold_Mean (Tone)	**–0.003*****	**–0.21*****	**0.12*****	**0.02*****
	(0.001)	**(0.02)**	**(0.001)**	**(0.001)**
NN Gold_SD	–0.01***	0.04***	0.15***	–0.07***
	(0.001)	(0.001)	(0.001)	(0.002)
Polity	**–0.01*****	**–2.75*****		
	(0.0001)	**(0.05)**		
Polity squared	–0.001***	–0.21***		
	(0.0000)	(0.003)		
Internet Not Free	**0.12*****			
	(0.003)			
Media Not Free	–0.21***			
	(0.003)			
Media Self-Censorship	**0.08*****			
	(0.003)			
Thursday	0.29***	0.72***	1.02***	0.15***
	(0.002)	(0.004)	(0.005)	(0.01)
Friday	**0.22*****	**0.17*****	**0.15*****	**0.58*****
	(0.002)	**(0.004)**	**(0.01)**	**(0.01)**
Saturday	0.12***	0.19***	0.18***	0.66***
	(0.002)	(0.004)	(0.01)	(0.01)
Sunday	**–0.32*****	**–0.31*****	**–0.17*****	**–0.27*****
	(0.003)	**(0.005)**	**(0.01)**	**(0.01)**
NN Gold_Mean *x* Polity	0.002***	–0.03***		
	(0.0001)	(0.003)		
Constant	**–4.49*****	**–13.75*****	**3,209.80*****	**–13,296.73*****
	(0.03)	**(0.20)**	**(77.65)**	**(104.99)**
Observations	40,608	5,184	288	288
MAE	36.9	137.1	1,245.2	841.9
RMSE	581.0	1,309.9	4,466.3	1,905.6
AIC	2,512,547.6	1,174,295.0	414,419.0	364,709.0
Log Likelihood	–1,256,240.8	–587,117.5	–207,185.5	–182,330.5
Notes:				*p<0.1; **p<0.05; ***p<0.01

Further, note the Goldstein Mean (i.e., NN tone) score, though it cannot be compared to the All-Regimes or the autocracies models, because of the use of the multiplicative interaction variables in those models, which calculates these coefficients combining NN tone with the groupings of countries level of democracy (i.e., Gold_Mean *x* Polity). As such, this would not be a correct comparison (Brambor, Clark, & Golder, 2006). Nevertheless, the magnitude, the degree of variation shown below NN tone, and the positive polarity track perfectly with the results of the interaction term for autocracies graphically represented in Figure 17.

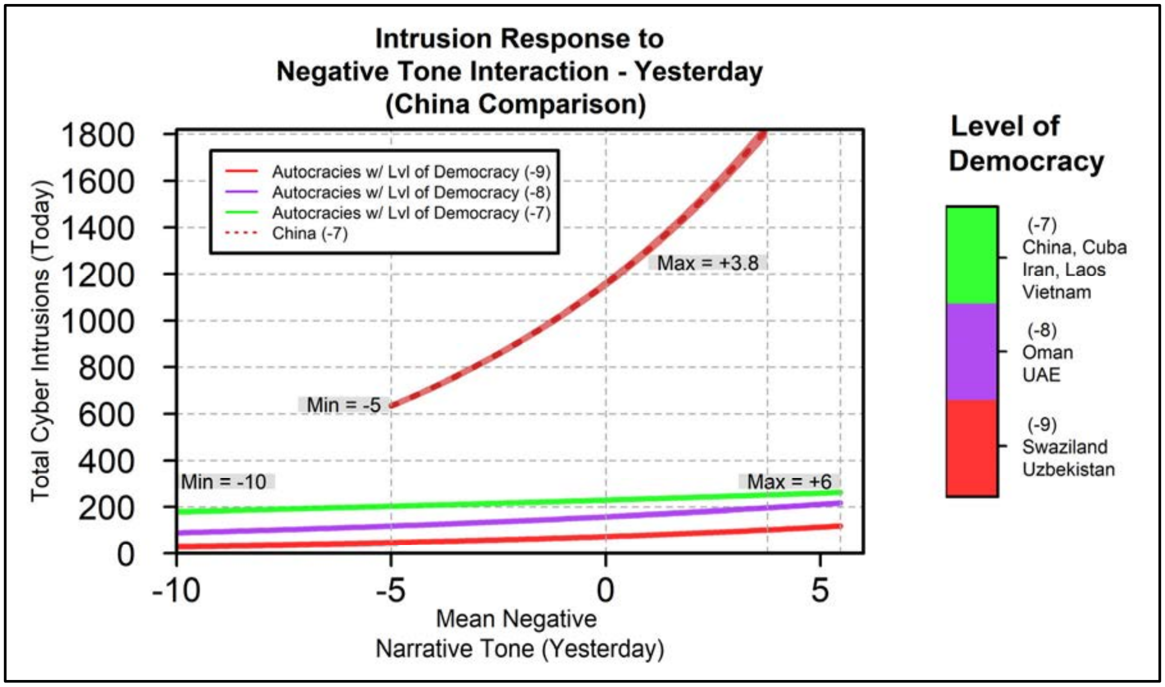


Figure 17. Negative Narrative Tone Results: China

The figure groups China with the eight other Autocracies ranking a –7 as their level of Democracy, depicted in the green, along the x and z-axis[122] Further, the figure depicts China’s NN tone effect in the dotted red line. By breaking out China’s NN tone *yesterday* discretely in the figure, one can verify visually that, although the coefficients for the

[122] The other Autocracies, as shown in Appendix G, include Azerbaijan, Belarus, Cuba, Eritrea, Iran, Kuwait, Laos, and Vietnam.

negative tone interaction in the autocracies model (–0.03) and the NN tone in the China model (+0.12) track opposite of each other in sign value, the resulting impact on today's intrusions remains the same. Both record a dampening impact on intrusions today, as NN tone increases. Further, notice how China's NN tone range (–5 to +3.8) is considerably tighter than all autocracies (–10 to +6) providing further evidence of the PRC's tight control of the level-two domestic narrative. Thus, the statistical evidence provided supports the acceptance of H11 for China.[123]

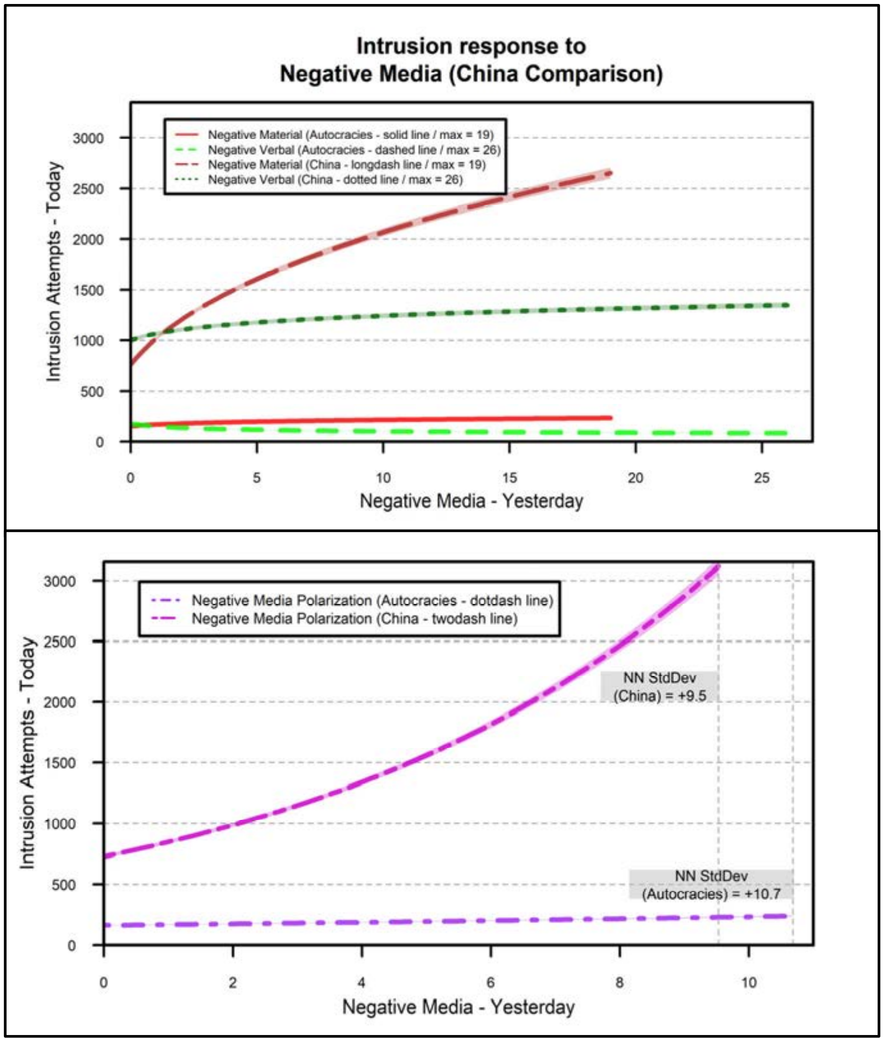
Further, as shown in Figure 18, both negative material narratives and NN polarization track closely in sign direction with the results of the autocracies model, with both at a marginal rate *twenty-three and thirty-five times*, respectively, higher than autocracies.[124] Yet, the negative verbal narratives comes in at a AME of *five times* higher than autocracies. Notice how the negative material narrative and NN polarization increase more rapidly than the autocracies model, while the verbal type increases but at a distinctly lower rate than the other two coefficients. Finally, observe the tightness of the color shading around each line, indicating the 95% confidence interval around the line predicted.

Interesting, how the PRC does not drive intrusions into the *negative* range while the negotiations remains verbal. Again, China's marginal effect across the x-axis shifts in sign, remaining positive, and scores five times higher than autocracies sloping upward showing an increase of intrusions. Perhaps, this is indicative of the PRC rheostating down intrusions from their rather substantial general population activated by elites, social movements, or party affiliation, while their state-sponsored hacktivists (i.e., fifty-cent

[123] **Hypothesis #11 (H11):** *Increases* in the conflictual or negative *tone* of interactions reported in media narratives from China directed at the United States (U.S.) and its interests—yesterday, results in *decreased* cyber intrusion activity on U.S. networks—today.

[124] The same model was used to derive the AME for each country removing all non-fluctuating variables (i.e., polity, Internet and Media Not Free, Media self-censorship, internet penetration rate, population, and GDP) because their values do not change except for Turkey and the UK in this study. As such, the predicted values of NmN, NvN, and NNP are being used holding all of the other variables constant at their mean values, while the prediction estimate is derived, very little, if any, change was observed as a result of the removal of these control variables, which allows for prediction of the AME in this case. Thus, China's AME in Figure 18 below predicts a marginal intrusion rate of +396.9 for NmN and +993.1 for NN polarization, respectively, while autocracies score +16.4 and +28 for the same variables. Thus, China's NmN comes in at [(396.9 – 16.4 / 16.4 = 23.2] twenty-three times that of autocracies, as NN polarization clocks in at [(993.1 – 28) / 28 = 34.5 ~ 35] thirty-five times higher.

party) remains active. This finding could validate how Valeriano, Jensen, and Maness (2018) described China's presence in cyberspace as consistent and constant.



Media Variable Prediction Comparison Table: China

Model or Regime Type / Calculated Variable	**Autocracies**	**China**	**Difference from Autocracies**
NmN: **AME on Intrusions** +/- **/** (SE)	16.3975*** (0.3311)	396.8643*** (4.4257)	380.4668*** (4.4381)
NvN: **AME on Intrusions** +/- **/** (SE)	-14.8539*** (0.1488)	54.0958*** (1.7826)	68.9497*** (1.7888)
NNp: **AME on Intrusions** +/- **/** (SE)	27.9613*** (0.8279)	993.0289*** (12.0724)	965.0676*** (12.1008)

Notes:
Average Marginal Effect (AME)
Negative Material Narrative (NmN)
Negative Verbal Narrative (NvN)
Negative Narrative Polarization (NNp)
Standard Error (SE)

Statistical Significance – p-Level:
***p < 0.01; **p < 0.001; ***p < 0.0001**

Figure 18. Media Results Comparison: China.

Considered comprehensively, this highlights how the PRC ratchets down the NN through media messaging to their CCP elites using the two-step process reinforcing the level-two narrative, while negotiations remain verbal and the material result has not yet been realized. To state in another way, while the negative narrative indicates verbal jousting between China and the U.S., the elite message is rheostat down intrusion activity; thereby, providing Chinese leadership maximum flexibility in level-one discourse with the U.S. Yet, maintaining their ubiquitous presence throughout as an indication of their cyber vigilance as a signal to their U.S. rival (Valeriano, Jensen, & Maness, 2018, pp. 143-170).

However, once or if a physical or tangible (i.e., material) outcome has been realized, the PRC signals their elites using both NN type and variation to return to the normal high rate of intrusions. Potentially, employing their colossal state-sponsored cyber capabilities through the malicious vector to engage in information seeking behavior maintaining careful observation of their global rival—the U.S. Again, this is not meant to imply directionality, certainly the narrative could begin with material and digress to verbal, as well.

Further, as the number of negative material or verbal narratives and NN polarization increase, notice the amplifying effect on cyber intrusions on U.S. networks the following day, shown graphically in Figure 18. In addition, notice China's tolerance of NN polarization scores only 11% less than the group of autocracies. This finding buttresses the argument that China tolerates some amount of descent, as shown here in media polarization, to hedge against outright collective action or physical protests. These results provide ample statistical evidence to support the acceptance of accept H8 and H10 surmise that the two-step process operates within and reinforces level-two of domestic politics in China.[125] Yet, the evidence provided supports rejection of H9 and acceptance of the null, because the level of intrusions only decrease in magnitude, but do not decrease as the

[125] **Hypothesis #8 (H8)**: *Increases* in the number of conflictual (i.e., negative) *material* interactions reported in Chinese media narratives directed at the United States (U.S.) or its interests—yesterday, results in *increased* cyber intrusion activity, emanating from China, on U.S. networks—today.

Hypothesis #10 (H10): *Increases* in the variation of negative narrative tone, indicating an increased level of media polarization, across media stories originating from China directed at the U.S. and its interests—yesterday, results in *increased* cyber intrusion activity on U.S. networks—today.

number of negative verbal narratives per day increase.[126] When viewed in its entirety, this evidence suggests an extreme level of societal control enabled by the digital panopticon in China as posited by this research. Next, this research turns its focus to Iran.

2. Iranian Evidence

As depicted in Table 6, Iran records a coefficient that changes in direction to that of China in negative material and verbal narratives and in the opposite direction when compared to the autocracies model's NN polarization coefficient, both of which were hypothesized in H12 and H13 respectively,[127] indicating that the Iranian regime's extensive use of First-Gen internet controls, such as filtering and throttling as mentioned earlier.

Further, the day of the week coefficients Friday, Saturday, and Sunday score at a higher rate than the other models in both positive and negative directions. Perhaps, this is because the Iranian workweek spans from Saturday through Wednesday of a given week (Anderson & Sadjadpour, 2018, p. 24). Consequently, Thursday's (i.e. Iran's Saturday) clocks in at a statistically significant coefficient value of +0.15 predicting Friday's level of intrusions. Friday's (i.e., Iran's Sunday) coefficient value scores a +0.58 forecasting a nearly *threefold* increase in Saturday's (i.e., Monday) intrusions. Saturday's coefficient value of +0.66, which only portends of a modest ~ 14% increase in Sunday's (i.e., Tuesday) intrusions. Finally, Sunday predicts a 140% drop in the following day's intrusions originating out of Iran. This appears to mirror Iran's pattern of life and will be discussed in more detail later in the analysis.

[126] **Hypothesis #9 (H9)**: *Increasingly* conflictual (i.e., negative) *verbal* interactions reported in Chinese media narratives directed at the United States (U.S.) and its interests—yesterday, results in *decreased* cyber intrusion activity, emanating from China, on U.S. networks—today.

[127] **Hypothesis #12 (H12):** *Increases* in the number of conflictual (i.e., negative) *material* and *verbal* interactions reported in Iranian media narratives directed at the United States (U.S.) and its interests—yesterday, results in *decreased* cyber intrusion activity, emanating from Iran, on U.S. networks—today.

Hypothesis #13 (H13): *Increases* in the variation of negative narrative tone, indicating an increased level of media polarization, across media stories originating from Iran directed at the U.S. and its interest—yesterday, results in *decreased* in cyber intrusion activity on U.S. networks—today.

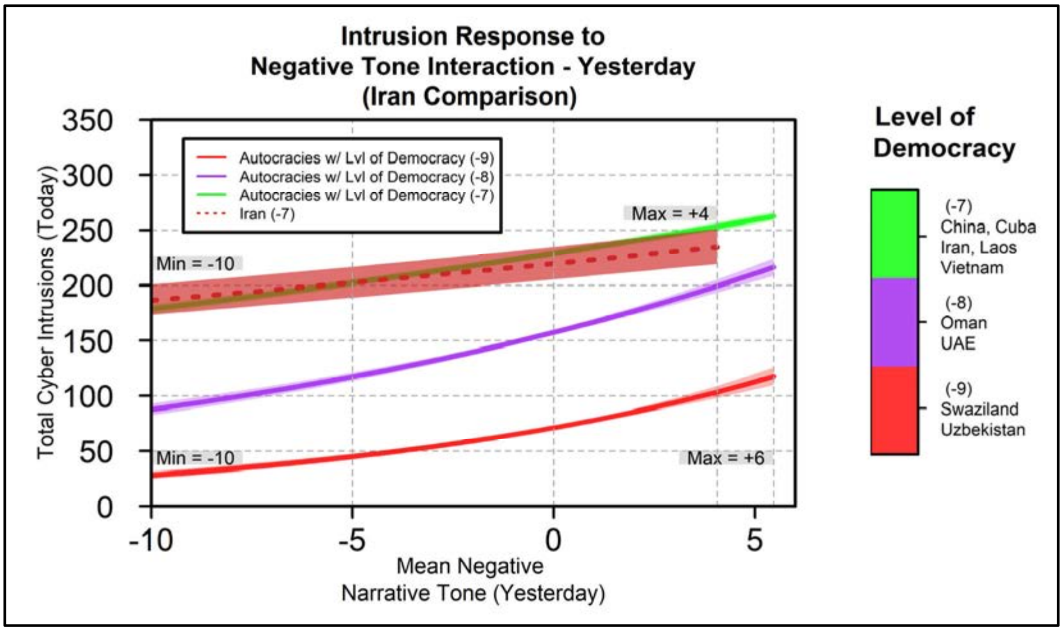


Figure 19. Negative Narrative Tone Results: Iran

NN media tone (i.e., Gold_Mean) on a given day and its effect on cyber intrusion attempts the next day traces in direction with China, with a tight standard error range. Thus, as with the Chinese model, the researcher cannot create an interaction variable because the level of democracy for Iran remains constant. Yet, the analyst can compare the coefficient's magnitude, variation, and direction in comparison to the line ascribed to Iran and eight other autocracies in Figure 19. As such, one would expect Iran to track closely with the others described by the green line in the figure corresponding to a polity score of –7.[128] As done in the China analysis above, Iran's NN tone effect was placed into the Figure 19 depicted by the dark red dotted line. Figure 19 reveals, as in the China case, that even though yesterday's NN tone coefficient tacks opposite in sign direction to the negative tone interaction coefficient used in the All-Regimes and autocracies model today's intrusions decrease in the same manner. Thus, increases in NN tone in stories emanating from Iran, corresponds to a decrease of intrusions on U.S. networks the following day. Further, consider the NN tone range (–10 to +4) employed by Iran in its rhetoric toward the U.S.,

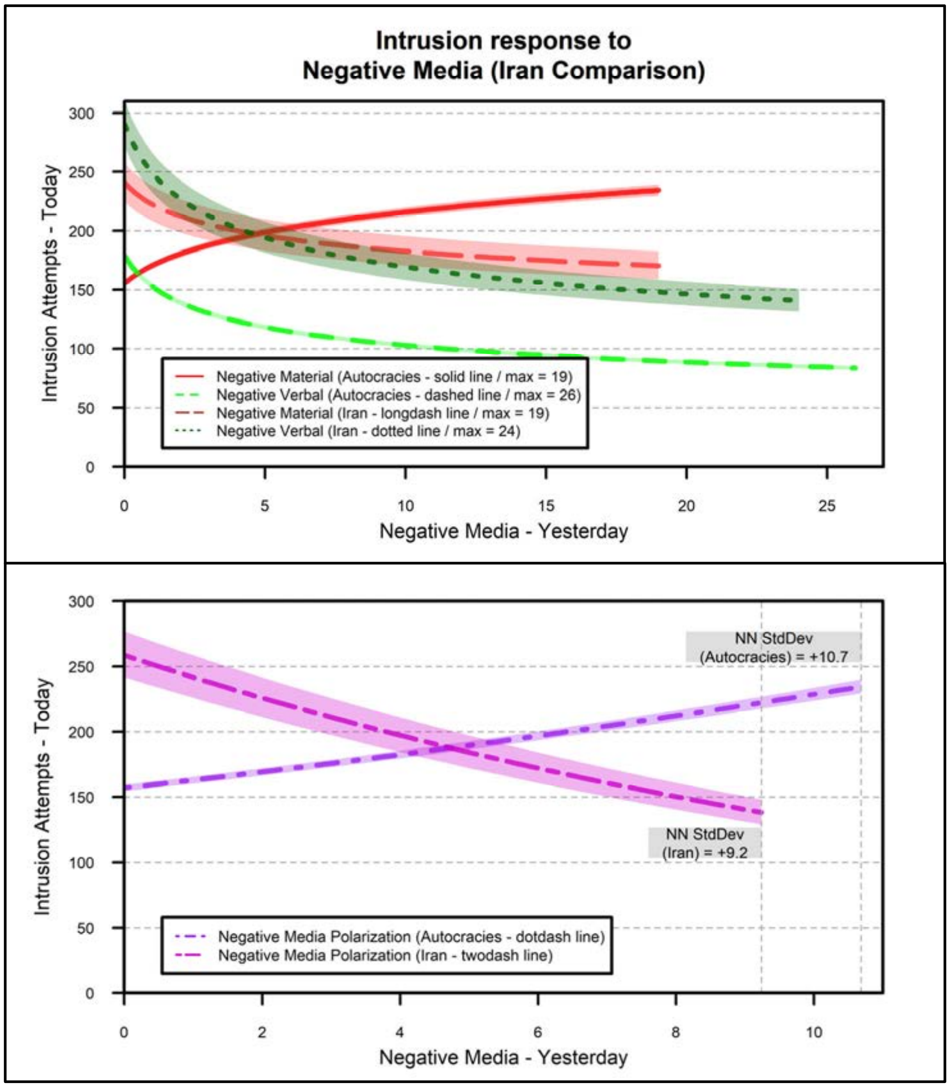
[128] The other Autocracies, as shown in Appendix G, include Azerbaijan, Belarus, China, Cuba, Eritrea, Kuwait, Laos, and Vietnam.

which stands as considerably less constrained than China at –5 to +3.8 as shown in Figure 17. Thus, revealing that the regime does not appear concerned about the impact of yesterday's rhetoric inciting Iranian hackers to intrude on U.S. networks today, perhaps due to their tight control of their indigenous cyberspace through the use of generational content controls. This evidence supports the acceptance of H14 for Iran at present, following the same methodology for acceptance of H11 used in the Chinese case.[129]

Now to return to the negative material and verbal narratives and NN polarization coefficients. Unlike any of the models, thus far, both the negative narrative material and verbal variables score as *negatively* correlated to cyber intrusion attempts the day following. Thus, intrusions drop considerably faster in response to verbal narratives than in response to material narratives, when comparing difference in forecasted intrusions across the count range in Figure 20. Further, the NN media polarization coefficient tracks negatively as well. When taken together coefficients seem to indicate what some scholars have pointed out about Iran (Blout, 2017; Golkar, 2011; Rahbarqazi & Baghban, 2019; Rahimi, 2011; Whitten-Woodring & James, 2012).

First, in general, their population does not rely on the mainstream media sources for their news. The average Iranian seem to turn to the social media citizen journalist for their news. As such, since these coefficients are derived from mainstream news media events, the research model may not be exposed to the right data necessary to provide evidence of the operation of the two-step process flow within domestic narrative at level-two.

[129] **Hypothesis #14 (H14):** *Increases* in the conflictual or negative tone of interactions reported in media narratives from Iran directed at the United States (U.S.) and its interests—yesterday, results in *decreased* cyber intrusion activity on U.S. networks—today.



Media Variable Prediction Comparison Table: Iran

Model or Regime Type / Calculated Variable	**Autocracies**	**Iran**	**Difference from Autocracies**
NmN: **AME on Intrusions** +/- **/** (SE)	16.3975*** (0.3311)	-71.1144*** (2.3679)	-87.5119*** (2.3909)
NvN: **AME on Intrusions** +/- **/** (SE)	-14.8539*** (0.1488)	-121.1658*** (2.2219)	-106.3119*** (2.2269)
NNp: **AME on Intrusions** +/- **/** (SE)	27.9613*** (0.8279)	-242.2298*** (5.3994)	-270.1911*** (5.4625)

Notes:
Average Marginal Effect (AME)
Negative Material Narrative (NmN)
Negative Verbal Narrative (NvN)
Negative Narrative Polarization (NNp)
Standard Error (SE)

Statistical Significance – p-Level:
***p < 0.01; **p < 0.001; ***p < 0.0001**

Figure 20. Media Results Comparison: Iran.

Secondly, notice how negative material narratives score an AME value of intrusions *five* times lower than autocracies and verbal narratives clock a negative AME *seven times* more negative.[130] This, for Iran, may be indicative of the IRI's extensive use of their favorite First-Gen censoring technology to throttle and filter content, particularly considering the magnitude of the effect of negative verbal narratives, which have a greater negative effect on intrusions than material ones as the number of conflictual narratives for a given day increase, as shown in Figure 20. Notice how the long-dashed red line drops drastically from left to right but *not* as rapidly as the dotted dark green line depicting the negative verbal narratives, as discussed earlier. Additionally, note how the NN polarization, the *violet* line, drops from left to right—at an AME rate of *ten times* less than autocracies.[131]

Perhaps, this is a result of the regime leveraging throttling and filtering technologies, as each of yesterday's NN variables record a coefficient dampening effect on today's intrusions with material coming in at 46% less than verbal. This small change may signify the regime's attempt to slow the population's realization of the physical or tangible consequences reported in negative *material* narratives they will ultimately have to endure. Whereas, at level-one, the Iranian regime increases its use of throttling and filtering during negative verbal jostling with the U.S., to provide their leadership with room to negotiate. Both allow the regime maximum flexibility in negotiations at level-one and enable the domestic control of the narrative via the two-step flow at level-two.

Further, since *neither* the freedom of the media nor of the internet exist in Iran, the statistical significance of these three coefficients may be more indicative of the fact that the regime can and does exercise consistent, documented control over both the dependent and independent variables in this regression equation. As such, this detail may enjoy a

[130] Using the table in Figure 20, NmN clocks in at a AME five times less [16.4 – (-71.1) / 16.4 = 5.3 ~ 5] and NvN scores an AME seven times less [-14.9 – (-121.2) / -14.9 = 7.1 ~ 7] than autocracies, respectively.

[131] As shown in the same table, the predicted average marginal effect (AME) on intrusions today based on yesterday's NN Polarization emanating from autocracies scores a 28, while Iran's predicted AME on intrusions drops by a -242.2. Thus, Iran's AME falls ten times faster [(28 – (-242.2)) / 28 = 9.65 ~ 10] than autocracies over the same range.

greater impact on the data used in the model than the Iranian citizen's choice of reliable media narratives. Nevertheless, the later argument may also contribute to these findings, but the magnitude of the contribution remains difficult to quantify, without exposing the model to data beyond the scope of this study.

Finally, turning to the day of the week coefficients. Friday is the Islamic holy day of the week, equivalent to Sunday in western cultures, the coefficient records a rate *three times* higher than Thursday, Islamic Saturday, followed by a modest 12% increase of intrusions on Saturday, or Islamic Monday. Perhaps, this is symbolic of the Islamic faithful, ginned up by the normal fiery rhetoric dispensed by Islamic fundamentalist imams (i.e., religious elites) at Friday prayer toward the U.S. and the West, leading them to seek to intrude upon U.S. networks at a significantly higher rate on Saturday and Sunday—the equivalent of western Monday and Tuesday. Ultimately, this spat of cyber intrusion activity exhausts itself in a 140% drop of intrusion attempts on Monday (i.e., Islamic Wednesday), as indicated by the –0.27 recorded for the Sunday day of the week coefficient. Interesting that the model appears to capture this aspect of Iran's pattern of life.

Thus, considering the entirety of the information provided by this model and by scholars who have studied Iran extensively, provides sufficient evidence to support H12 and H13, rejecting the null hypothesis in each case.[132] Further, this model provides evidence that the Iranian regime controls the internet and the media content quite extensively. Upon review of this Chapter, various clues pointed to this finding, which arose earlier in the discussion.

D. CONCLUSION

First, consider how the conflictual material and verbal narratives and NN polarization *yesterday* correlated negatively with *today's* cyber intrusions on U.S. networks

[132] **Hypothesis #12 (H12):** *Increases* in the number of conflictual (i.e., negative) material and verbal interactions reported in Iranian media narratives directed at the United States (U.S.) and its interests—yesterday, results in *decreased* cyber intrusion activity, emanating from Iran, on U.S. networks—today.

Hypothesis #13 (H13): *Increases* in the variation of negative narrative tone, indicating an increased level of media polarization, across media stories originating from Iran directed at the U.S. and its interest—yesterday, results in *decreased* cyber intrusion activity on U.S. networks—today.

in the Iran model. Within the China discussion, it was pointed out that the PRC wields its censorship arsenal against any narratives that incites collective action, dissent, or protests, but allows for some criticism of state and local officials (Custer, Prakash, Solis, Knight, & Lin, 2019; Greitens, 2013; King, Pan, & Roberts, 2013; Lindsay, 2014; Richet, 2013; Wang & Minzner, 2015). While Iran seems to view narratives encouraging any dissent as equivalent to narratives criticizing the regime, particularly censoring any chronicles using disparaging language in reference to the Supreme Leader, as a crime punishable by death (Ansari, 2017; Baharan, 2009; Blout, 2017; Freedom House, 2020; Golkar, 2011; Hussain, 2016; Jones & Newlee, 2020; Morozov, 2011; Rahbarqazi & Baghban, 2019; Rahimi, 2016).

The Iran model bears this out showing a negative correlation for the negative material and verbal narratives and NN polarization, revealing the IRI's extensive use of throttling and filtering to slow internet access and speeds—one facet of their intent to control the narrative. Further, as the regime's NN tone increases toward the west the use of throttling and filtering appears to apply here as well. These only serve as indicators of the IRI's determination to control the narratives and their population actions on-line, leaving little room for any type of message running contrary to that approved by the regime. Only in the dichotomous control variable capturing Friday's narrative can the impact of the NNs produced by Iranian Imams be gauged. Perhaps, a nuance unique to this culture or merely a by-product of the fiery rhetoric heaped on the population by the religious elites. Finally, both the China and Iran models scored a consistently *positive* correlation in their NN tone coefficients resulting in a dampening of intrusions the following day, as the narratives became progressively conflictual.

Multiple scholars have noted that the Iranian population relies more heavily on citizen journalists then the mainstream (i.e., state run) media. Thus, for Iran, a better explanatory variable might be negative Twitter or, the Russia-owned, Telegram social media activity on a given day and its influence over cyber intrusion attempts the following day. Perhaps, this could be the focus of some future research in this arena. For these reasons, the Iran coefficients for negative material narratives and NN polarization provide results that differ from the autocracies and China models. Negative verbal narratives track consistent with autocracies but shift opposite in sign to China, whereas the China model tracks quite closely in most respects with the autocracies model, except for negative verbal narratives, as shown in Figure 18 and Appendix I.

Yet, when reviewing their use of the internet externally, Iran and China manifest different objectives. Iran's focus remains on its regional rivals and keeping them in check using the level of sophistication necessary to manage its global rivalry in order of priority, gaining access through the use of the malicious vector chiefly to achieve a subversive intent or a secondary objective of seeking information. Whereas, China leverages the malicious vector as a means of intruding to achieve an information seeking objective 79% of the time. Preferring mass over complexity in its intrusion tactics, China's focus seems intent on keeping tabs on the U.S. and other regional rivals, intent upon monitoring or stealing their information and secrets (Valeriano & Maness, 2015). Further, China leverages their sheer mass of numbers to achieve its cyber objectives as manifested by its use of low level risk intrusions in Appendix J, which stands in sharp contrast to Iran that uses whatever cyber intrusion technique necessary for them to achieve their goal.

Both effectively rheostat the narrative and their population's use of the internet to anticipate and manage intrusions on U.S. networks on the day following the media event. Both regimes use the internet to achieve their greater aspirations, goals, and objectives in cyberspace. In different ways, both regimes use the internet, using their incumbent generational content controls, to animate the digital panopticon enabling this repressive technology to censor, propagandize, surveil, and trace their populations. This domain technology is properly controlled and tailored by both China and Iran to gain, maintain, and sustain their stylized autocratic ambitions.

Next this research will delve into the hybrid, anocracy regime type. The following case study will focus on Russia and Turkey. The intent is to explore how anocracies use the media and cyberspace to control their domestic and international narratives, to influence their rivals, and to control their respective societies.

V. CASE STUDIES: ANOCRACIES IN CYBERSPACE

A. INTRODUCTION

This chapter will cover anocracies, also known as hybrid, partly free, mixed or semi democracies (Colomer, Banerjea, & Mello, 2016; Freedom House, 2017; Marshall & Elzinga-Marshall, 2017). They occupy the regime-type middle ground between democracies and autocracies displaying some democratic leanings, while leveraging some autocratic governance structures and processes. This case study will cover two countries that the U.S. comes in frequent and continuous contact with on both regional and international issues—Russia and Turkey. The former a long-term, locked-in rival of the U.S. The later, an ally of the U.S. over the past century. Appendix D contains the complete list of countries categorized as anocracies, in accordance with the Polity IV classification and framework (Marshall & Elzinga-Marshall, 2017).

First, the chapter will open with a review of how anocracies operate in and utilize cyberspace both domestically and internationally. Second, the case study will cover the unique aspects of Russia and Turkey's use of cyberspace, surveying the impact of that use on their civil society's debates and operation. Each of these sections will culminate with a set of hypotheses covering how their separate negative narrative types (either material or verbal), tones, and polarizations about the U.S. or its interests, on any given day, will affect cyber intrusion attempts on U.S. networks the next day. Ultimately, the existing research model will be applied to Russia and Turkey to validate or invalidate the conjectured hypotheses. Finally, the chapter will culminate with a discussion covering the differences and similarities in how these two anocracies use cyberspace to maneuver in internationally or wield domestically to either control or manage the day's narrative judging from its impact on the following day's cyber intrusion attempts. The chapter will be laid out as described below.

B. ANOCRACY RIDING THE THIRD WAVE

Anocracies occupy this awkward position in the middle between democracies and autocracies. These states combine elements of autocracies and democracies into an oftenincoherent mix of governance structures affording their citizens varying degrees of individual rights, civil liberties, and political access (Marshall & Cole, 2014). For some of these countries, this regime type allows time for transition from autocracy to democracy or vice versa, while others linger in the anocratic realm (Marshall & Cole, 2014; Marshall & Elzinga-Marshall, 2017).

Those who tarry as an anocracy do so, perhaps, as a hedge against the Dictator's Dilemma or as a means to buy time to embark on a slower rate of governmental change, while avoiding the chaos that would result from a drastic regime shift. Some of these *anocratic* states employ various *autocratic* methods to control the media narrative both domestic and international to buy time needed for transition to another form of government (Marshall & Cole, 2014; Marshall & Elzinga-Marshall, 2017). While others realize that, because of their country's culture and history, their citizens simply do not have the capacity to immediately affect such a radical change from one type to the other. The realization that led to this decision normally occurs within the generational, ruling elite power structure, which often leads to anocratic stasis (Best & Higley, 2018; Colomer, Banerjea, & Mello, 2016; Maréchal, 2017; Nocetti, 2015; Ognyanova, 2018).

Anocracy describes the governance structures of states that include Russia, Turkey, Thailand, Egypt, Sudan, and Venezuela (Marshall & Cole, 2014; Marshall & Elzinga-Marshall, 2017). Many anocracies follow the autocratic practice of developing their own internet, engineering in the control of information, vis-à-vis the narrative, within the state's boundaries (Akgül & Kırlıdoğ, 2015; Ron Deibert, 2015; Diamond, 2010; Gebhart & Kohno, 2017; Greitens, 2013; Mackinnon, 2012; Rød & Weidmann, 2015; Ruijgrok, 2017; Sinpeng, 2013). Some anocrats, like the autocrats, seem set on creating a digital panopticon by layering government and non-governmental structures intent upon censorship, control, and surveillance of their population (Hussain, 2016). For example, Thailand chooses to place layers of government and co-opted private groups to assist in monitoring their citizen’s internet activity, similar to the Chinese model, seeking to discover any derisive content about their long-standing monarch.[133]

Since the 1990s, Thailand has vacillated between democracy and anocracy two consecutive times in as many decades (Marshall & Cole, 2014; Marshall & Elzinga-Marshall, 2017). The most recent transitions coincided with several government collapses ending in the coups d’états of September 2006 and May 2014 (Gebhart, Anonymous, & Kohno, 2017; Pinkaew, 2016; Sinpeng, 2013).[134] It will be interesting to see if Thailand can find its way back to democracy while a significant part of their populace censors and surveils the anti-monarchist portion of their civil society. As of 2017, Thailand continues to linger on as an anocracy (Marshall & Elzinga-Marshall, 2017).

[133] Similar to many of the autocracies, Thailand has created a cyber-militia of sorts named cyber scouts program (Pinkaew, 2016, p. 204; Sinpeng, 2013, pp. 432-433). The King’s patronage makes the organization possible recruited in their youth to serve, many are ultra-royalists, who police and report content viewed as being transgressive or anti-royalist. The Cyber Scouts, comprised of pro-royalist groups such as the Garbage Collecting Organization, the Seri Thai Movement, the Thai Netizen Network, and the People’s Alliance for Democracy, along with other government-sponsored groups buttress the Thai government’s surveillance apparatus (Pinkaew, 2016, p. 204; Sinpeng, 2013, pp. 432-433). The Cyber Scouts police internet sites reporting, publicly shaming, or intimidating those who make statements against the monarch (Pinkaew, 2016, p. 205). The lineage of these organizations tracks back to similar elements and tactics used to effectively, ferret out insurgent communist groups operating in Thailand during the Cold War (Pinkaew, 2016, p. 205; Sinpeng, 2013). Essentially, the Thai government repurposed this Cold War era apparatus to meet their growing need for societal censorship and surveillance (Pinkaew, 2016; Sinpeng, 2013).

As a result, the military backed government enacted the Computer-Related Crime Act (2007) (CCA) (Sinpeng, 2013). This act provided the government with very broad legal power to prosecute *cybercrimes* (Sinpeng, 2013). As the government, transitioned back to a tract toward democracy the CCA remained in place, potentially as a hedge against future societal disorder. Certainly, the CCA proved its usefulness in and after the 2014 unrest (Sinpeng, 2013). Subsequently, due to the use of broad and vague language in the CCA, the use of censorship and surveillance became a common government tactic in cyberspace (Gebhart, Anonymous, & Kohno, 2017; Pinkaew, 2016; Sinpeng, 2013). In addition, the CCA effectively criminalizes the concealment of an individual’s IP address – one of the less vague authorities granted by the act (Gebhart, Anonymous, & Kohno, 2017). Even autocratic regimes such as China, Saudi Arabia, Iran, and Vietnam do not resort to such measures to institute internet censorship (Gebhart, Anonymous, & Kohno, 2017, p. 418).

[134] Each transition was precipitated by unstable societal conditions inextricably tied to polarized political discourse in the media and cyberspace concerning the King, royal family of Thailand, and the lèse majesté laws (Gebhart, Anonymous, & Kohno, 2017; Pinkaew, 2016; Sinpeng, 2013). In both cases, the polarized political discourse involved dueling narratives, one supporting the constitutional monarch and the other supporting the former Prime Minister Thaksin Shinawatra, deposed in the 2006 coup, his followers support a more democratic form of government. Article 112 of the Thai Penal Code prohibits any insults or defamation of the King or any Thai Royal in acts, speech, or writing, commonly referred to as lèse majesté (Gebhart, Anonymous, & Kohno, 2017; Pinkaew, 2016; Sinpeng, 2013).

On the other end of the spectrum resided the state of Tunisia. After 24 years as an anocracy, in the throes of the January 2011 Arab Spring and immediately following the departure of their despotic President, the Tunisian transitional government sought to quickly gain control of the situation and buy time to figure out how to meet the demands of the population and ultimately transition to democracy (Chakchouk, Kehl, Ben-Avie, & Coyer, 2013; Freedom House, 2017; Hinnebusch, 2015; Marshall & Cole, 2014; Marshall & Elzinga-Marshall, 2017). Amongst the foremost challenges, the fledgling regime inherited a pervasive internet construct with censorship and surveillance engineered into every aspect of access to monitor content and push their pro-government narrative (Chakchouk, Kehl, Ben-Avie, & Coyer, 2013; Hinnebusch, 2015; Ruijgrok, 2017). Nevertheless, Tunisia became a democracy in 2013 moving towards an open media environment and internet freedoms (Marshall & Elzinga-Marshall, 2017; Polity IV, 2018).[135]

This leads the discussion to Russia, which seems stuck, perhaps intentionally, in anocratic stasis. Within this category, Russia is the most active in cyberspace (Valeriano & Maness, 2014; Valeriano & Maness, 2015; Valeriano, Jensen, & Maness, 2018). Turkey's interaction in this arena seems focused on gaining control of their domestic internet. Both Russia and Turkey have frequent and ongoing contact with the U.S. across all domains and each wields the instruments of national power in uniquely different ways. Russia is a locked in, longtime rival of the U.S., who remains quite active in cyberspace (Valeriano & Maness, 2014; Valeriano & Maness, 2015; Valeriano, Jensen, & Maness, 2018). Turkey, seemingly friendly toward the U.S., a NATO partner, and a once secular democracy, appears to be drifting towards autocratic, Islamic fundamentalism and at present appears to focus its resources in cyberspace internally. (Akgül & Kirlidoğ, 2015). Of the two, Russia's level of sophistication reflects the sheer breadth of their internal digital panopticon built intentionally to control the domestic narrative through censorship, propaganda, and surveillance, while influencing the international narrative. The Russian

[135] Tunisia's strong civil society made this possible by working diligently to strike a polyarchic balance, conscientiously seeking compromises with Islamic groups to assuage their religious concerns (Hinnebusch, 2015, p. 359).

digital panopticon remains unparalleled and even superior, in some aspects, to that of China (Akgül & Kırlıdoğ, 2015; Asmolov, 2016; Baarda, 2017; Duffy, 2015; Freedom House, 2020; Gabdulhakov, 2020; Marcellino et al., 2020; Nocetti, 2015; Ognyanova, 2018; Paul & Matthews, 2017; Snegovaya, 2015; Strovsky, 2015; Zhukov & Baum, 2016).

1. Russia in the Third Wave

Russia stands as the most threatening anocracy in the international realm of cyberspace, largely due to its capabilities and presence in cyberspace, as discussed earlier (Valeriano & Maness, 2014; Valeriano & Maness, 2015; Valeriano, Jensen, & Maness, 2018). Russia appears to be following the monarchist—anocratic model—attempting to stabilize as an anocracy accruing the economic benefits of a democracy while maintaining the control, censorship, and surveillance characteristics of an autocracy, as a hedge against the Dictator's dilemma (Freedom House, 2017; Gunitsky, 2015; Hussain M. M., 2016; MacKinnon, 2012; Marshall & Elzinga-Marshall, 2017; Morozov, 2011; Zittrain, et al., 2017). In effect, a populist monarch has ruled Russia since 2007, indulging in what MacKinnon termed as Digital Bonapartism (MacKinnon, 2012; Marshall & Elzinga-Marshall, 2017).[136]

Vladimir Putin, backed by the Duma, various government ministries and loyal elite oligarchs, has essentially locked down all digital media, networks, and platforms inside Russia with the intent of controlling the ongoing narrative, ultimately, to ensure public opinion remains positively disposed toward the regime (Akgül & Kirlidoğ, 2015; Baarda, 2017; Duffy, 2015; Freedom House, 2020; Gabdulhakov, 2020; Marcellino, Marcinek, Pezard, & Matthews, 2020; Nocetti, 2015; Ognyanova, 2018; Snegovaya, 2015).[137] Vaulting over first-generation media content controls to focus its efforts on second and

[136] Digital Bonapartism – essentially a populist demagogue, who uses democratic oratory and symbolism to legitimize their rule and political leadership through the manipulation of public opinion by controlling digital media, networks, or platforms (MacKinnon, 2012, pp.66-67).

[137] A 2018 survey of Russian citizens queried those who knew that their personal correspondence sent via on-line services (i.e. Telegram, e-mails, etc.) could be monitored by law enforcement officials, nearly 59% stated that this was done to combat crime or terrorism (Levada Center, 2019, p. 114). Only, 11% stated that this was done as a means of censorship or to limit freedom (Levada Center, 2019, p. 114). Both of which are testament to the effectiveness of Russian domestic propaganda.

third-generation domestically and to use the Fourth-gen to gain traction internationally (Deibert & Rohozinski, 2010; Deibert R. , 2015). Consequently, the regime leverages its monopoly on media outlets (i.e., Channel One, NTV, RT, or Sputnik) and the absolute control of the internet via the .ru domain to push that narrative both inside and outside their physical borders (Freedom House, 2017; Gabdulhakov, 2020; MacKinnon, 2012; Marcellino, Marcinek, Pezard, & Matthews, 2020; Morozov, 2011; Nocetti, 2015; Ognyanova, 2018; Paul & Matthews, 2017; Snegovaya, 2015). Indeed, it appears that nearly 90% of Russian citizens consume media from these sources, with RT being the most-watched news source on the internet (Freedom House, 2020; Levada Center, 2019; Ognyanova, 2018; Paul & Matthews, 2017; Snegovaya, 2015). In addition, the regime uses the internet's efficient surveillance capability to monitor, to trace, and, if necessary, to physically target individuals through judicial or extra-judicial arrest, assault, or intimidation to quash their dissenting opinions (Freedom House, 2020; Gabdulhakov, 2020; MacKinnon, 2012; Maréchal, 2017; Morozov, 2011; Strovsky, 2015). Certainly, Russia's appetite to use intimidation tactics, along with the time honored censorship, propaganda, and surveillance, to control its population appears more effective, expansive, and pervasive than in other anocracies.[138] To this point, the Duma has enacted laws, similar to Iran, which prohibit criticism of senior political figures (i.e., the president, the prime minister, or the cabinet of ministers) (Gabdulhakov, 2020; Hussain, 2016; Maréchal, 2017; Nocetti, 2015; Ognyanova, 2018). While this may seem quite draconian on its face, if one considers Russia's history, specifically the leadership of czars, one first secretary, several general secretaries, and now a mixture of seemingly democratic titles, who appear bent on regaining the status of their formers, it does fit quite nicely (Best & Higley, 2018;

[138] Indeed, Russia's system of judicial and extra-judicial intimidation by far surpasses all anocracies and most autocracies (Freedom House, 2020; Gabdulhakov, 2020; MacKinnon, 2012; Maréchal, 2017; Morozov, 2011; Nocetti, 2015). Gabdulhakov (2020) describes the Russian system as rhizomatic using a botanical comparison of a mass of plant life that appears on the surface to be multiple distinct plants; yet, beneath the surface exists a network of roots connecting the plants together as one, not the many discrete set of plants one might observe from the surface. This metaphor describes the Russian digital panopticon surveilling and tracing their population using a conjoining labyrinth of civil servants, citizen vigilantes, and state police enabled by information technology undergirded by an intentionally vague legal system, which enables the total control of civil society and the domestic narrative (Asmolov, 2016; Baarba 2017, Baum & Zhukov, 2015; Freedom House, 2017, 2020; Gabdulhakov, 2020; Mackinnon, 2012; Marcellino et al., 2020; Maréchal, 2017; Nocetti, 2015; Ognyanova, 2018; Paul & Matthews, 2017; Romanyuk, 2011; Snegovaya, 2015; Strovsky, 2015; Zhukov & Baum, 2016).

Colomer, Banerjea, & Mello, 2016; Maréchal, 2017; Nocetti, 2015; Ognyanova, 2018). Nevertheless, their control over the narrative, the media, and the internet remains absolute, effective, and panoptic (Asmolov, 2016; Baarda, 2017; Duffy, 2015; Freedom House, 2020; Gabdulhakov, 2020; Nocetti, 2015; Ognyanova, 2018; Paul & Matthews, 2017; Snegovaya, 2015; Zhukov & Baum, 2016).

Russia's swift employment of second and third-generatoin content controls appear to be the result of three near simultaneous events occurring on the global stage with distinct cyber overtones: the Arab Spring (2011); the Russian Presidential and Parliamentary elections (2012), which led to mass protests in their largest cities; and the leaking of classified National Security Agency (NSA) files describing U.S. surveillance practices of foreign governments (2013) (Akgül & Kırlıdoğ, 2015; Asmolov, 2016; Duffy, 2015; Maréchal, 2017; Nocetti, 2015; Ognyanova, 2018).[139] Although all of the pieces had been in place prior to 2011, the domino effect of those events brought the specter of a digitally enabled panopticon in Russia to the fore. The Russian people, wishing to avoid any legal or extra-legal entanglements, engage in what has been widely recorded as self-censorship because of the omnipresent gaze of the digital panopticon existing within the .ru domain (Asmolov, 2016; Baarda, 2017; Deibert & Rohozinski, 2010; Gabdulhakov, 2020; Galič, Timan, & Koops, 2017; Manokha, 2018; Maréchal, 2017; Nocetti, 2015; Ognyanova, 2018; Zhukov & Baum, 2016). Thus, creating the embodiment of Foucault's prediction in modern day Russia (Asmolov, 2016; Bentham, 2012; Foucault, 1977; Gabdulhakov, 2020; Galič et al., 2017; Loadenthal, 2018; Mackinnon, 2012; Morozov 2012; Manokha, 2018).

In international affairs, like Iran, Russia displays a similar quasi-phobic distrust toward the U.S. and western democracies. However, its phobia exists for different reasons. Russian leadership views the internet as a domain similar to air, land, sea, and space, a domain where the state must control, maintain, and secure all aspects of it, as a means of maintaining Russian sovereignty (Choucri, 2012; Deibert & Rohozinski, 2010; Deibert,

[139] A month before the 2012 Presidential Election, Putin declared “the Internet doesn't deserve any real attention, and it's the place where pornography dominates” (Duffy, 2015; Northam, 2012). Then just over two years later in 2014, Putin declared the internet “special project of the Central Intelligence Agency (CIA)” (Duffy, 2015; Maréchal, 2017; Nocetti, 2015; Ognyanova, 2018)

2015; Maréchal, 2017; Nocetti, 2015; Valeriano & Maness, 2015; Valeriano, Jensen, & Maness, 2018). This domain is where the terms information security and information space possess *important* philosophical and political meanings for the Russian state—itself (Deibert & Rohozinski, 2010; Jaitner & Mattsson, 2015; Maréchal, 2017; Nocetti, 2015; Ognyanova, 2018). This domain is where state sovereignty, as set forth in the Treaty of Westphalia, must be respected (Deibert & Rohozinski, 2010; Duffy, 2015; Maréchal, 2017; Nocetti, 2015). This domain is where the U.S., throughout the Post-Soviet era, has demonstrated a pervasive, seemingly inexorable expansion into Russian spheres of influence and control, thereby, trampling upon their state sovereignty and threatening their national security (Deibert & Rohozinski, 2010; Duffy, 2015; Maréchal, 2017; Nocetti, 2015; Ognyanova, 2018; Valeriano, Jensen, & Maness, 2018).

Consequently, on the international stage, Russia ranks highest amongst the anocracies that engage in rivalrous cyber dispute activity between 2000–2014 (Valeriano & Maness, 2015). Within the Russian anocracy, the line between the intelligence services and cyber criminals remains blurred; some scholars describe the relationship as historically symbiotic (Kello, 2013; Valeriano, Jensen, & Maness, 2018). This trait gains currency when scholars empirically review Russian cyber tactics. Inherently, Russian initiated cyber incidents use the malicious intent vector to achieve a primarily subversive objective (~ 56%) while secondarily seeking other pertinent information about the target state (~ 44%) (Snegovaya, 2015; Valeriano, Jensen, & Maness, 2018, pp. 110-142).[140] The Russians tend to definitively use these cyber tactics in an attempt to intimidate or coerce its former satellites into aligning with their national security objectives as in Estonia (2007), Georgia (2008), Lithuania (2009), and Ukraine (2014) (Farwell & Rohozinski, 2011; Gartzke, 2013; Jaitner & Mattsson, 2015; Lindsay J. , 2015; Nye J. S., 2017; Snegovaya, 2015; Valeriano, Jensen, & Maness, 2018). Regardless of their subversive intent bent on coercion, they have yet to succeed in coercing any of the states targeted (Valeriano, Jensen, & Maness, 2018, p. 118). Essentially, Russia uses its cyber abilities, often wielded by *patriotic* hacktivists,

[140] Malicious intent calculation equates to 32 out of 45 incidents equating to 0.711 or approximately 71% (Valeriano, Jensen, & Maness, 2018, p. 120). Subversive intent and Information seeking intent calculations equate to 25 out of 45 incidents equaling 0.555 (~ 56%) and 20 out of 45 incidents equaling 0.444 (~ 44%), respectively (Valeriano, Jensen, & Maness, 2018, p. 119).

to advance a very specific narrative designed to create bedlam and undermine public confidence in the targeted countries governance structures (Calamur, 2017; Farwell & Rohozinski, 2011; Gartzke, 2013; Jaitner & Mattsson, 2015; Kello, 2013; Nye J. S., 2017; Thornton & Miron, 2019).

Largely, Russia or its proxies use several Soviet era operational concepts namely *active measures* and *reflexive control* in tandem to an attempt to coerce, influence, or compel another state to yield. *Active measures* describes the use of an array of operant covert and overt psychological methods intent on influencing the opinion-making process of an adversary (Metzl, 1974, p. 921; Valeriano, Jensen, & Maness, 2018, pp. 113-115).[141] Active measures operate through the disruption or manipulation of information. The manipulation occurs by creating and then grafting a competing narrative onto existing media events to bend the message into a theme that achieves Russia's purpose (Inkster, 2016; Snegovaya, 2015; Valeriano, Jensen, & Maness, 2018).

Reflexive control, while similar to perception management in the West, focuses on control of the subject, in this case public opinion of a state or the civil society within a target country (Thomas, 2004, p. 237). *Reflexive control* explains the use of specifically tailored information that would influence a rival to voluntarily make the pre-determined decision framed and preferred by the preparer or originator (a.k.a. the opposing state in dyad) (Thomas, 2004, pp. 237-238; Valeriano, Jensen, & Maness, 2018, pp. 113-114). Ostensibly, the Russians attempt to use active measures through their crafted narrative to achieve reflexive control of their target using their cyber capabilities. Domestically, these tactics appear to have had a dramatic effect. On the international stage these stratagems have caused and continue to cause much consternation throughout the world; yet, any exploration of this lies beyond the scope of this research. Finally, Russia's ability to

[141] Active measures – describes the employment of an array of operationally covert and overt psychological methods intent on polluting and subverting the opinion-making process of an adversary (Inkster, 2016, pp. 28-29; Metzl, 1974, p. 921; Snegovaya, 2015, pp. 14-15; Valeriano, Jensen, & Maness, 2018, pp. 114-115).

compel, influence, or coerce an adversary or target country remains suspect (Valeriano, Jensen, & Maness, 2018, pp. 110–142).[142]

Hence, it appears that the Russian state has locked its citizens behind a digital Iron Curtain (Gabdulhakov, 2020, pp. 4-5). Beyond the brief opportunity between the fall of the Soviet Union (~ 1991) and Vladimir Putin's assumption of the Presidency (~ 1999), Russian media remains under the strict control of the state (Asmolov, 2016; Baarda, 2017; Buckley, 2004; Maréchal, 2017; Nocetti, 2015; Ognyanova, 2018; Strovsky, 2015). Further, the internet prior to the events of 2011–2013 remained relatively open and uncontested (Deibert & Rohozinski, 2010, Duffy, 2015; Maréchal, 2017; Nocetti, 2015; Ognyanova, 2018). However, the combined effects of the Arab Spring (2011), the social unrest caused by the presidential and parliamentary elections (2012), and the Snowden affair (2013) became the catalyst for the drastic increase in censorship (often self-censorship), surveillance, and propaganda of the internet within Russia.[143] As such, both the media and the internet are controlled and monitored quite extensively; thus, both sides of the equation that forms the model in this research may be affected. Therefore, based on this and other information contained in this section, these hypotheses (i.e., H15, H16, and H17) are provided.

[142] Yet, the evidence surrounding the U.S. Election of 2016 remains firm. Some have conjectured that Russian agents armed with their bots and trolls, spending between $150,000 and $247,000 on fake Facebook and Twitter accounts, swayed 62.9M American citizens to vote for the 45th President (Lazer et al., 2018; Maréchal, 2017; Valeriano, Jensen, & Maness, 2018). It seems difficult to make such an assumption or conjecture—particularly if one adheres to the scientific method. Yet, scholarship and science appear simply carried away by their sheer disdain for an Executive who is entirely different from past Presidents (Lazer et al., 2018; Maréchal, 2017; Valeriano, Maness, & Jensen, 2017). Perhaps, scholarship and science should focus on what they do best—scholarship and science—and refrain from analysis based on the cacophony of emotional opinions.

[143] Recent research conducted on Democracies shows that in those states where confidence in traditional media sources is low—substitutes emerge and where censorship of offline media is high the disparity in information between offline and online media is high (Baum & Zhukov, 2015; Romanyuk, 2011).

Hypothesis #15 (H15): *Increasingly* conflictual (i.e. negative) *material* and *verbal* interactions reported in Russian media narratives directed at the United States (U.S.) and its interests—yesterday, results in *decreased* cyber intrusion activity, emanating from Russia, on U.S. networks—today.

Hypothesis #16 (H16): *Increases* in the variation of negative narrative tone, indicating an increased level of media polarization, across media stories originating from Russia directed at the U.S. and its interest—yesterday, results in *decreased* cyber intrusion activity on U.S. networks—today.

Hypothesis #17 (H17): *Increases* in the conflictual or negative *tone* of interactions reported in media narratives from Russia directed at the United States (U.S.) and its interests—yesterday, results in *decreased* cyber intrusion activity on U.S. networks—today.

Figure 21. Russia – Case Study Hypotheses

2. Turkey in the Third Wave

Turkey, after an unbroken 28 years as a secular democracy, began to transition in 2014 from an open to a closed anocracy, ultimately becoming one in 2016 (Freedom House, 2017; Marshall & Cole, 2014; Marshall & Elzinga-Marshall, 2017). This in effect closed anocracy displays some sectarian leanings and employs methods of censorship and surveillance very similar to those seen in autocracies. Turkey intends to design and develop a domestic version of the Google search engine and e-mail service. These efforts align with its internet censorship laws, which rest on the pretext of providing its population with culturally pure content, an action promptly followed by Iran and Russia (Akgül & Kirlidoğ, 2015; Morozov, 2011, p. 237; Rød & Weidmann, 2015; Zittrain, et al., 2017).[144] Further, Turkey enacted new laws to protect national security interests because of the failed 2016 coup attempt that greatly expanded powers of the state to censor, surveil, detain, or arrest individuals suspected of creating subversive content, specifically media content (Akgül & Kirlidoğ, 2015; Deibert, 2015; Freedom House, 2017; Levin, 2016).[145] As such, this once thriving secular democracy seems destined to become an autocracy, in time, with all of its

[144] https://turkeyblocks.org/2017/01/06/turkey-building-domestic-search-engine-and-email/

[145] In December 2016, Turkey jailed 81 journalists – the highest number in the world at the time (Freedom House, 2017, p. 12).

incumbent cyber control mechanisms set on the creation of a digitally panoptic society (Foucault, 1977).

Turkey’s slide into anocracy began in 2002, when the Justice and Development Party (AKP)[146] won a landslide election led by Recep Tayyip Erdoğan and was swept into power. Abdullah Gül, a co-founder of AKP, became Prime Minister as Erdoğan, years earlier, had been legally censured by a Turkish Security Court for a speech given with religious overtones and was prohibited from participating in politics for life (Shambayati, 2004, pp. 266-267).[147] Shortly after assuming office, Gül and the AKP dominated Turkish Parliament amended the constitution, effectively annulling Erdoğan’s legal banishment from politics, allowing him to become Turkey’s Prime Minister in March of 2003 (Shambayati, 2004, p. 269). He held this position he held until assuming the Presidency of Turkey in 2014, which he holds to this day and uses to effectively subsume the powers of the Prime Minister, making him the most powerful person in the country (Akgül & Kirlidoğ, 2015; Esen & Gumuscu, 2016). However, the rise of AKP did not happen unilaterally; they gained and maintained powerful allies within the Gülen movement (Akgül & Kirlidoğ, 2015; Altiparmak & Gürol, 2017; Bilgiç, 2018; Esen & Gumuscu, 2016; Hussain & Hussain, 2017; Rodrik, 2014).[148]

In 2002 and 2003, the relationship between AKP and the Gülen movement began out of their mutual disdain and distrust for the military and secular elites, who were solely

[146] All acronyms used in this section will use the Turkish convention for abbreviations.

[147] In a speech given in 1997, Erdoğan evoked several lines from a poem written by Ziya Gokalp (1876-1924), a famous Turkish Poet and Intellectual, describing a fictious conversation between an ancient Turkish Sultan and an Emperor of the Byzantine Empire. In the dialog, the Emperor affronts the Sultan by declaring that he will “burn the Koran and the Kaba,” both of which are deeply sacred to the Islamic Faith. The Sultan responds to the insult by stating: “*minarets are [our] bayonets, domes helmets; mosques are our barracks, and the believers are [our] soldiers.*” Erdoğan, then the Mayor of Istanbul, used the Sultan’s statement in a speech to a political gathering in the primarily Kurdish city of Siirt. Turkish secularists found his use of these words profoundly offensive and alleged that they constituted a threat to the secular state and institutions of Turkey. Subsequently, Erdoğan was charged and convicted. His sentence constituted ten months in jail, of which he only served four, a fine, and from that point on prohibited from participating in politics for life (Shambayati, 2004, pp. 266-269).

[148] The Islamic scholar and Imam, Fethullah Gülen who has resided in the U.S. since 1999, founded the Gülen Movement. The movement is based on Islamic teaching, supports religious instruction at private schools and universities in over 180 countries through the world, and possesses substantial assets in the media, finance, and health sectors (Altiparmak & Gürol, 2017; Esen & Gumuscu, 2016).

responsible for the four previous (i.e., 1960, 1971, 1980, & 1997) coup d'états (Al Jazeera, 2016; Bilgiç, 2018; Hussain & Hussain, 2017; Polity IV, 2018). Effectively, each of the previous coup d'états ended the rule of the four previous instantiations of the Islamic leaning AK Party in Turkey (Al Jazeera, 2016; Bilgiç, 2018; Esen & Gumuscu, 2016; Hussain & Hussain, 2017; Rodrik, 2014). However, it is important to point out that the Turkish military and judiciary saw themselves as the *Guardians of Democracy* and were responsible for the 49 out of 54 years of democratic rule of the Republic since 1960 (Polity IV, 2018). Further, five of those 54 years bracketed periods of societal unrest and martial law characterized by executions, mass arrests, and disappearances, some of which are described as extra-judicial (Al Jazeera, 2018; Altiparmak & Gürol, 2017; Polity IV, 2018). Nevertheless, in each case within a few years of the successful coup, Turkey saw the return of order and democracy enabled by their military's actions (Al Jazeera, 2016; Bilgiç, 2018; Hussain & Hussain, 2017; Polity IV, 2018; Shambayati, 2004). Also, in each case, those removed from office sought to curtail or even end the military oversight of the Turkish government, wrest control from the conservative Kemalist elites, and ring in an era of Islamic renewal (Al Jazeera, 2016; Altiparmak & Gürol, 2017; Bilgiç, 2018, Esen & Gumuscu, 2016 Hussain & Hussain, 2017; Rodrik, 2014). Thus, the period covered under this research amounts to the culmination of a decades-long struggle between the Secularists and the Islamists battling for the control and direction of the Republic of Turkey.

After wresting control from the Kemalist Secularists in 2002, Erdoğan, the AKP, and their Gülenist allies began expanding their influence in the judiciary, military, police, and the ministerial functions of Turkey (Akgül & Kirlidoğ, 2015, p. 15; Altiparmak & Gürol, 2017, p. 101; Gurdeniz, 2020, p. 83; Hussain & Hussain, 2017, p. 75; Rodrik, 2014). Further, AKP extensively leveraged Gülen followers in positions of influence throughout academia, the state bureaucracies, and the judiciary system, as well as, their extensive network in business, finance, journalism, and the media (Akgül & Kirlidoğ, 2015; Altiparmak & Gürol, 2017; Gurdeniz, 2020; Hussain & Hussain, 2017; Rodrik, 2014). Essentially, after years of strife with the military and their secularist allies, learning from their prior abortive attempts at obtaining control, AKP had finally attained control and open access to all the levers necessary to gain and maintain rule over Turkey. They were not about to let it slip away again.

First, they began building digital panoptic capabilities by tapping into the knowledge of the best—China and Russia (Akgül & Kirlidoğ, 2015; Eldem, 2020; Yesil, Sözeri, & Khazraee, 2017). Initially, through their acolytes in the judiciary and with a majority in parliament, AKP began placing the legal parameters necessary to deploy second-generation content controls tying internet censorship to existing vaguely written laws in the penal code (Akgül & Kirlidoğ, 2015; Deibert & Rohozinski, 2010; Deibert, 2015; Eldem, 2020; Yesil, Sözeri, & Khazraee, 2017). They placed these new internet laws atop imprecisely written regulations that broadly criminalized any speech that insults Turkish ethnicity, government institutions, or the nation itself. The AKP enshrined these laws under the rubric of public health, order, safety, and morality, which ties directly to the coup de grace that will sound familiar-*national security* (Akgül & Kirlidoğ, 2015; Arsan, 2013; Deibert & Rohozinski, 2010; Deibert, 2015; Eldem, 2020; Yesil, Sözeri, & Khazraee, 2017).

In 2007, the AKP regime legalized governmental use of first-generational content controls (i.e., deep packet inspection, throttling, and filtering) through the Parliament by enacting Law No. 5651 and other internet laws to the Turkish penal code, criminalizing discrete types of internet content and allowing for enhanced internet censorship and surveillance, each of which enabled them to gain control of the narrative (Akgül & Kirlidoğ, 2015; Deibert & Rohozinski, 2010; Deibert, 2015; Eldem, 2020).[149] Over the ensuing years, as a result of a series of tumultuous, perhaps AKP orchestrated domestic events, these authorities expanded greatly from first to second-generation allowing the state

[149] The regime authorized implementation of internet law #5651 under a branch of the Information and Communication Technologies Authority (BTK)–the regulatory agency responsible for the telecom sector , the Presidency of Telecommunications and Communications (TIB) (Akgül & Kirlidoğ, 2015; Eldem, 2020; Esen & Gumuscu, 2016). As such, TIB, the BTK division, that had been given the legal mandate to execute telephone taps without a legal warrant, found its authorities greatly expanded from tapping telephones to blocking websites with no judicial oversight and broadened even further by legislative expansion of the laws authorities in 2014 (Akgül & Kirlidoğ, 2015, pp. 4-6; Saka, 2018). Law #5651 introduced the term *sufficient suspicion*. If authorities had sufficient suspicion that an internet content offense was committed, gave the TIB adequate grounds to block, throttle, or remove content (Akgül & Kirlidoğ, 2015; Deibert & Rohozinski, 2010; Esen & Gumuscu, 2016; Saka, 2018).

to censor and surveil its population with impunity (Deibert & Rohozinski, 2010; Deibert, 2015; Eldem, 2020; Yesil, Sözeri, & Khazraee, 2017). Ultimately, these authorities have grown into the domestic elements of third-generation internet content controls under the guise of national security and the requirement for domestic safety of the population (Akgül & Kirlidoğ, 2015; Deibert & Rohozinski, 2010; Deibert, 2015; Eldem, 2020; Yesil, Sözeri, & Khazraee, 2017).

This growth allowed the AKP to gain and maintain control of the domestic narrative becoming the new elite and dominating all media within Turkey, metaphorically shouting down any opposition from the former elites, namely the secularists and their advocates in the military (Arsan, 2013; Bilgiç, 2018; Eldem, 2020; Esen & Gumuscu, 2016; Saka, 2018; Yesil, Sözeri, & Khazraee, 2017; Zittrain, et al., 2017). Further, during the same timeframe, the AKP enacted a series of reforms that criminalized any overt or covert intervention in Turkish politics by the military (Bardakçi, 2013, pp. 421-423; Esen & Gumuscu, 2016, pp. 1585-1586). This huge development, especially when one considers the number of coup d'états executed by the secular Guardians of Democracy since 1960, essentially returned the Republic to Kemal Atatürk's vision of a staunch non-religious democracy.[150] By this action, the AKP laid the legal foundations that outlawed any future coup d'états led by the military and any future involvement of the military in Turkish politics, dealing a major blow to Atatürk's secular military powerbase, the avowed political rivals of the AKP.

Swiftly thereafter in late 2007, the AKP and their Gülen allies in the Presidency of Telecommunications and Communications (TIB), the national police, and the judiciary used their oversized domestic second-generation authorities to surveil, prosecute, and jail hundreds of military officers suspected to have secularist, western leanings, who were suspected of conspiring to overthrow the duly elected AKP government (Akgül & Kirlidoğ,

[150] Mustafa Kemal Ataturk came to power 1923 as the President of Turkey, following the disastrous defeat of the Central Powers in World War I and the subsequent dissolution of the Ottoman Empire (Gurdeniz, 2020). Ataturk envisioned a predominately secular, industrially modern Turkey, which he did not inherit from the Ottoman Islamic Caliphate that he deposed (Al Jazeera, 2016). Ataturk's policies were staunchly secular, western leaning policies intent on tying Turkey to its European roots dominated its domestic and foreign policy for 79 years until AKP was swept into power in the democratically election of 2002 (Al Jazeera, 2016; Bilgiç, 2018; Gurdeniz, 2020; Hussain & Hussain, 2017; Yesil, Sözeri, & Khazraee, 2017).

2015; Arsan, 2013; Bilgiç, 2018; Biçakci, Doruk, & Mitat, 2015; Esen & Gumuscu, 2016; Gurdeniz, 2020; Rodrik, 2014; Yesil, Sözeri, & Khazraee, 2017). The dragnet of prosecutions that surrounded the Ergenekon, Balyoz, or Sledgehammer trials (2008–2012) encompassed not only military officers, but intellectuals, politicians, and journalists (Akgül & Kirlidoğ, 2015; Arsan, 2013; Bilgiç, 2018; Esen & Gumuscu, 2016; Rodrik, 2014). The defendants' main defense was that the electronic records used by the prosecution had been fabricated, which was roundly disregarded by the Gülenist prosecutors and judges presiding over the trials (Akgül & Kirlidoğ, 2015; Arsan, 2013; Bilgiç, 2018; Esen & Gumuscu, 2016; Gurdeniz, 2020, Rodrik, 2014). The court cases concluded in September of 2012, convicting 331 of 365 of plotting the coup attempt (Rodrik, 2014). Thus, at the end of 2012, the main guardians of democracy, the Turkish military, had been sufficiently silenced.

Then came the next struggle for power in Turkey between the AKP and their former Gülenists allies, the latter of which, as it was subsequently discovered in December 2013, had engineered the military plot *narrative* and fabricated most of the electronic evidence used in the Ergenekon trials (Akgül & Kirlidoğ, 2015; Bilgiç, 2018; Esen & Gumuscu, 2016; Gurdeniz, 2020, Rodrik, 2014; Yesil, Sözeri, & Khazraee, 2017). It came to be known that the Gülenists leveraging their vast network were able to use their henchmen in the Presidency of Telecommunications and Communications (TIB), various government funded cyber organizations,[151] the national police, the judiciary, and the media to execute the full array of offensive direct action capabilities resident in third-generation content controls to surveil, confuse, entrap, and disgrace their secular-military opponents (Akgül & Kirlidoğ, 2015; Deibert & Rohozinski, 2010; Deibert, 2015; Eldem, 2020; Rodrik, 2014; Yesil, Sözeri, & Khazraee, 2017).

Suddenly in 2013, Erdoğan declared that the Gülenists had formed a dangerous "parallel state" bureaucracy within the state of Turkey that must be dealt with (Akgül & Kirlidoğ, 2015; Bilgiç, 2018; Esen & Gumuscu, 2016; Gurdeniz, 2020, Rodrik, 2014;

[151] Mainly the Technological Research Council of Turkey (TÜBİTAK), which in 2010, merged with Informatics and Information Security Research Center (BILGEM).

Yesil, Sözeri, & Khazraee, 2017). Multiple AKP members openly professed that they had been misled by the Gülenists during the Ergenekon, Balyoz, and Sledgehammer trials (Rodrik, 2014). The judiciary reopened the cases in 2015, leading to dismissal of most if not all the charges fraudulently levied against those accused (Akgül & Kirlidoğ, 2015; Arsan, 2013; Bilgiç, 2018; Esen & Gumuscu, 2016; Rodrik, 2014). Simultaneously, Erdoğan's AKP majority began the systematic post-Soviet style lustration of Gülenists embedded throughout the Turkish bureaucracy, media, and military (Altiparmak & Gürol, 2017). The AKP purge fell particularly hard on several of the cyber ministries and centers, severely hampering Turkey's cyber capabilities going forward.[152]

Subsequently, the coup attempt in July 2016 led to a two-year state of emergency, which presented Erdoğan and the AKP with almost unlimited power to settle all scores against the secularists, the military, and their latest rival, the Gülenists (Altiparmak & Gürol, 2017; Bilgiç, 2018; Eldem, 2020; Freedom House, 2020; Yesil, Sözeri, & Khazraee, 2017). The narrative engineered by the AKP blamed Gülenists embedded in the military for the abortive coup (Altiparmak & Gürol, 2017; Bilgiç, 2018; Eldem, 2020; Freedom House, 2020; Yesil, Sözeri, & Khazraee, 2017). By laying the blame on their arch-rival the Turkish military and their newfound rival the Gülenists, Erdoğan and the AKP gained and used their free hand in Turkey to eradicate any and all resistance, all the while, leveraging their well-cultivated control of the media to ensure their narrative painted these Gülenists as the traitors of the Republic. Thus, Erdoğan and the AKP used their preeminent command of domestic first, second, and third-generation content controls to ensure their rivals were effectively silenced internally, while broadcasting their message internationally, to the skepticism of some (Eldem, 2020; Yesil, Sözeri, & Khazraee, 2017). By July 2018, Erdoğan and the AKP cemented their control of the domestic narrative and all elements of

[152] Of particular interest in this research was the purge of their cyber expertise within Technological Research Council of Turkey (TÜBİTAK), Informatics and Information Security Research Center (BILGEM), and TIB losing nearly 1,000 scientist and researchers in 2015 and 80% of their administrative staff in 2014 (Akgül & Kirlidoğ, 2015; Bilgiç, 2018; Biçakci, Doruk, & Mitat, 2015, p. 35; Eldem, 2020; Esen & Gumuscu, 2016; Yesil, Sözeri, & Khazraee, 2017). In fact, in 2015, BILGEM declined a Turkish law enforcement agency request to conduct digital forensic analysis on four hard drives because they lacked the expertise to do so due to personnel turbulence (Biçakci, Doruk, & Mitat, 2015, pp. 35-36). Thus, the AKP devised purge of Turkish Cyber ministries created a gaping hole in Turkey's cyber capabilities.

cyberspace in the country devolving from a democracy in 2014 to a closed anocracy in 2016 (Freedom House, 2020; Marshall & Elzinga-Marshall, 2017; Polity IV, 2018).

Therefore, the intrusion data used in this research covered the period from right before the coup in early 2015 to right after the coup attempt 2016–2017, essentially covering part of the state of emergency. Further, the media coded events appear quite sensitive to Turkish reporting. Specifically, the event coders found that Turkish reporting was distinctively different from other Middle Eastern countries, as such, they created a set of unique dictionary protocols to account for Turkey's media events (Schrodt P. A., 2012, pp. 177-181).

Hypothesis #18 (H18): *Increasingly* conflictual (i.e., negative) *material* interactions reported in Turkish media narratives directed at the United States (U.S.) or its interests—yesterday, results in *increased* cyber intrusion activity, emanating from Turkey, on U.S. networks—today.

Hypothesis #19 (H19): *Increasingly* conflictual (i.e., negative) *verbal* interactions reported in Turkish media narratives directed at the United States (U.S.) and its interests—yesterday, results in *decreased* cyber intrusion activity, emanating from Turkey, on U.S. networks—today.

Hypothesis #20 (H20): *Increases* in the variation of negative narrative tone, indicating an increased level of media polarization, across media stories originating from Turkey directed at the U.S. and its interests—yesterday, results in *increased* cyber intrusion activity on U.S. networks—today.

Hypothesis #21 (H21): *Increases* in the accumulated conflictual or negative *tone* of interactions reported in media narratives from Turkey directed towards the United States (U.S.) and its interests—yesterday, results in *increased* cyber intrusion activity on U.S. networks—today, with the effect becoming stronger as Turkey's level of democracy *decreases*.

Figure 22. Turkey – Case Study Hypotheses

This taken together with the data used in the regression equation covered highly mediatized events in Turkey from the reopening of the Ergenekon trials in 2015 to the state of emergency following the coup attempt. A period when the narrative would be tightly controlled by the AKP regime and the population would look to AKP elites for interpretation of the domestic narrative, shifting away from the secular elites. Thus, Turkey was enduring a turbulent time of shifting allegiances, internal strife, and AKP consolidation of power. As such, the two-step process may have been operating and reinforcing the level-two narrative in certain corners of Turkish society allowing the AKP regime to dictate the interpretation of the domestic storyline, while, the effect in others may be diminished. Further, the lustrating purge of the Gülenists and military from their governmental cyber centers, councils, and ministries no doubt led to a colossal loss in cyber expertise (see footnotes 152 & 153). The culminating impact of all of these factors most likely led Turkey's leadership and population to focus internally, with the former consolidating power and the later paralyzed with doubt facing an uncertain future.

Next, over the period of analysis, Turkey slid to opposite ends of the anocratic polity range allowing for the observation of negative tone interaction variable at the country-level of analysis. As the AKP would have dominated the level-two domestic narrative, which was well known by the population, consequently, the reaction would be expected to track as predicted by the anocracy model analyzed in Chapter III and shown graphically in Figure 11. Finally, while Turkey has yet to manifest its cyber prowess on the world stage as cataloged by Valeriano and Maness (2014, 2015, & 2016), ample evidence has been provided above that indicates the Turkish regime possesses and wields significant expertise in the cyber realm with 93% of their intrusions coming in at the highest average risk level shown in Appendix J. Over this period, their cyber prowess appears to have been focused internally. As such, the author proposes to test the above hypotheses in Figure 22 employing the same model used throughout this research.

C. EVIDENCE OF MEDIA EFFECTS IN CYBERSPACE

Again, a review of the research findings covering anocracies discussed in Chapter III appears practical at this point. Like autocracies, the research granted the acceptance of H1, H3, and H5 revealing that two-step [media] flow operates and reinforces regime narratives at level-two of international relations.[153] The anocracies model tracks closely

[153] **Hypothesis #1 (H1):** *Increases* in the number of conflictual *material* interactions reported in the media narratives of other sovereign states directed at the United States (U.S.) and its interests—yesterday, regardless of regime type, results in *increased* cyber intrusion activity on U.S. networks—today.

Hypothesis #3 (H3): *Increases* in the number of conflictual *verbal* interactions reported in the media narratives of anocratic states directed at the United States (U.S.) and its interests—yesterday, results in *no change* in cyber intrusion activity on U.S. networks—today.

with All-Regimes model, both of which are depicted in Figure 12 (Chapter III), each coefficient mirrors the other in direction and narrative type and media polarization. Specifically, this demonstrates that when the number of negative material narratives increase on a given day, a corresponding increase in the number of cyber intrusion attempts occurs on the following day in each model. Next, the All-Regimes model records a strong dampening effect resulting from yesterday's negative verbal narratives, whereas anocracies *yesterday's* negative verbal narratives result in the neutral impact on *today's* intrusions. Finally, the given day's NN polarization coefficient records a reduced effect on the following day's intrusions. When considered comprehensively, these findings provide quantitative evidence of the operation of the two-step flow within level-two of domestic politics during international negotiations between anocratic regimes and the U.S. at level-one.

Interestingly, the interactive coefficient of today's NN tone and level of democracy continues the trend established by the All-Regimes model, which allowed for the acceptance of H7, but notably was rejected for autocracies and democracies.[154] Figure 11 (Chapter III) graphically represents this interaction showing how today's intrusions increase as yesterday's NN tone becomes more conflictual and the level of democracy decreases—consisting of a *doubling* of intrusions per day from the green to red lines. Yet, for the purposes of this case study, Figure 11 supports the argument for the direction of the NN tone coefficient in the Russian models, because their level of democracy does not vary across this period of analysis, which is similar to China and Iran. Yet, as Turkey was enduring a rather tumultuous period of governmental change over this period of analysis, their level of democracy did vary beginning at +3 in 2014 drifting to a –4 in 2016. As such, the regression model calculates a coefficient for this interactive term.

Hypothesis #5 (H5): *Increases* in the variation of negative narrative tone, indicating an increased level of media polarization, across media stories originating from democratic and anocratic states directed at the U.S. and its interest—yesterday, results in *decreased* cyber intrusion activity on U.S. networks—today.

[154] **Hypothesis #7 (H7)**: *Increases* in the aggregate conflictual or negative *tone* of interactions reported in media narratives from democracies, anocracies, and autocracies directed at the United States (U.S.) and its interests—yesterday, will result in *decreased* cyber intrusion activity on U.S. networks—today, with the effect becoming stronger as the level of democracy of the originating state *increases*.

As stated in the hypotheses for both Russia and Turkey, it should be expected that each country may well react differently to the model. Russia's use of second and third-generation internet content controls, regime ownership and control of all domestic mainstream media outlets, and extensive use of propaganda may impact the connection between negative media narratives *today* influencing the cyber intrusion activity *tomorrow*. Further, Turkey's activities seem to be primarily focused on getting their regime's business in order, appearing to focus its internet efforts domestically, at least for now, but it does possess a burgeoning capability, if one considers its level of intrusion capability as shown in Appendix J. As such, the model's results may not parallel the anocracies model, which stands as the reasons for the conjectured hypotheses in Figures 21 and 22. Thus, the research analysis will expose Russia and then Turkey to the model to test the conjectured hypotheses.

1. Russian Evidence

As depicted in Table 7, coefficients derived by the Russia model score differently than those of the All-Regimes and anocracies models. These results reveal that yesterday's negative material narratives coefficient track negatively with today's cyber intrusion activity emanating from Russia, similar to the Iranian model. While the negative verbal narratives tack closely to the All-Regimes model, with yesterday's NN polarization coefficient tracking consistently in direction with the other models, recording a dampening effect on intrusions the following day. Taken as a whole, these terms appear to validate the strong grip the Russian government has over their indigenous internet and media space. Preferring to maintain sovereign control of their domestic internet space to leverage it both internally and externally for their chosen purpose, while manipulating the media message to placate the population with pro-regime narratives. Again, viewing the .ru net as their sovereign territory similar to that of the physical land, sea, and air domains.

Table 7. Results of Negative Narratives Models for Russia and Turkey.

CYBER INTRUSION ATTEMPTS (Anocracy Comparison)				
	Dependent Variable			
	TotalIntrusions – Today			
	Poisson Model			
Independent Variable (Yesterday) / Model	All-Regimes	All Anocracies	**Russia**	**Turkey**
Negative Material Narratives	**0.03*****	**0.10*****	**–0.11*****	**0.03**
	(0.002)	**(0.005)**	**(0.01)**	**(0.03)**
Negative Verbal Narrative	–0.24***	0.0000	–0.12***	–0.41***
	(0.002)	(0.005)	(0.01)	(0.02)
NN Gold_Mean (Tone)	**–0.003*****	**–0.001**	**0.001**	**0.01**
	(0.001)	**(0.001)**	**(0.003)**	**(0.02)**
NN Gold_SD	–0.01***	–0.02***	–0.03***	0.02**
	(0.001)	(0.002)	(0.004)	(0.01)
Polity	**–0.01*****	**–0.01*****		**–0.08*****
	(0.0001)	**(0.001)**		**(0.01)**
Polity squared	–0.001***	–0.01***		
	(0.0000)	(0.001)		
Internet Not Free	**0.12*****	**–0.29*****		
	(0.003)	**(0.01)**		
Media Not Free	–0.21***			
	(0.003)			
Media Self-Censorship	**0.08*****	**3.50*****		
	(0.003)	**(0.45)**		
Friday	0.22***	0.56***	0.42***	0.48***
	(0.002)	(0.01)	(0.01)	(0.01)
Saturday	**0.12*****	**0.28*****	**0.32*****	**0.32*****
	(0.002)	**(0.01)**	**(0.01)**	**(0.01)**
Sunday	–0.32***	–0.29***	–0.25***	0.02
	(0.003)	(0.01)	(0.01)	(0.02)
NN Gold_Mean *x* Polity	**0.002*****	**0.01*****		**0.01****
	(0.0001)	**(0.0004)**		**(0.004)**
Constant	–4.49***	–11.69***	–47,474.37***	1.86***
	(0.03)	(0.47)	(976.82)	(0.20)
Observations	40,608	10,071	288	288
MAE	36.9	15.7	146.5	96.7
RMSE	581.0	118.9	250.5	323.0
AIC	2,512,547.6	192,375.2	33,555.2	37,022.5
Log Likelihood	–1,256,240.8	–96,155.6	–16,753.6	–18,486.3
Notes:				*p<0.1; **p<0.05; ***p<0.01

Next, notice the NN tone variable, which is consistent in positive value with the first-order interaction (i.e., negative tone interaction) shown in the two other models. However, scores no statistical significance, consider the graphical depiction of this multiplicative interaction in the anocracies model and the NN tone for Russia shown in Figure 23 below. Notice how all the lines similarly colored with variations of green track together, with the Russian NN tone discretely broken out at the top of the chart, scoring a decrease in today's intrusions as yesterday's NN tone becomes increasingly negative. Nevertheless, when analyzed together, due to the coefficient's lack of statistical significance and the large standard error range H17 lacks support and stands as rejected in favor of the null hypothesis.[155] Indeed, for Russia, increases in a given day's NN tone has little to no influence on intrusions on U.S. networks the following day.

Observe how yesterday's negative material and verbal narratives and NN polarization terms track in the negative direction with their consistent lack of variation indicted by the tight standard error values of each. The parallels between these three variables as well as the NN tone coefficient above, each resulting in a dampening effect on U.S. networks –today. Hence, the negative direction of these coefficients in the Russian model provides evidence of the effective employment of second and third-generation internet content controls, often resulting in self-censoring behavior.[156]

Additionally, note that most Russians receive their news from state-run internet or television sources both of which are *not* captured in the Phoenix media events data, meaning that the media variables, though significant, may not exemplify the optimal data source to provide evidence of two-step process operating within level-two domestic narrative when Russia is exchanging narratives with its principal rival the U.S. As in the case of Iran, this reveals that Russia views the domestic internet space as its sovereign domain as posited by many scholars (Choucri, 2012; Deibert & Rohozinski, 2010; Deibert R. , 2015; Maréchal, 2017; Nocetti, 2015; Valeriano & Maness, 2015; Valeriano, Jensen,

[155] **Hypothesis #17 (H17):** *Increases* in the conflictual or negative tone of interactions reported in media narratives from Russia directed at the United States (U.S.) and its interests—yesterday, results in *decreased* cyber intrusion activity on U.S. networks—today.

[156] In 2019, the V-Dem project scored Russia's media censorship as direct and routine, while scoring their media's self-censorship as common, but incomplete (V-Dem Institute, 2019, pp. 185-188).

& Maness, 2018). Thus, those who operate out of the Russian *.ru* space do so at the will of the regime and also possess the skill set to intrude using a greater level of sophistication, recording 72% of intrusions emanating from Russia clocking in at the highest level of average intrusion risk, as shown in Appendix J.

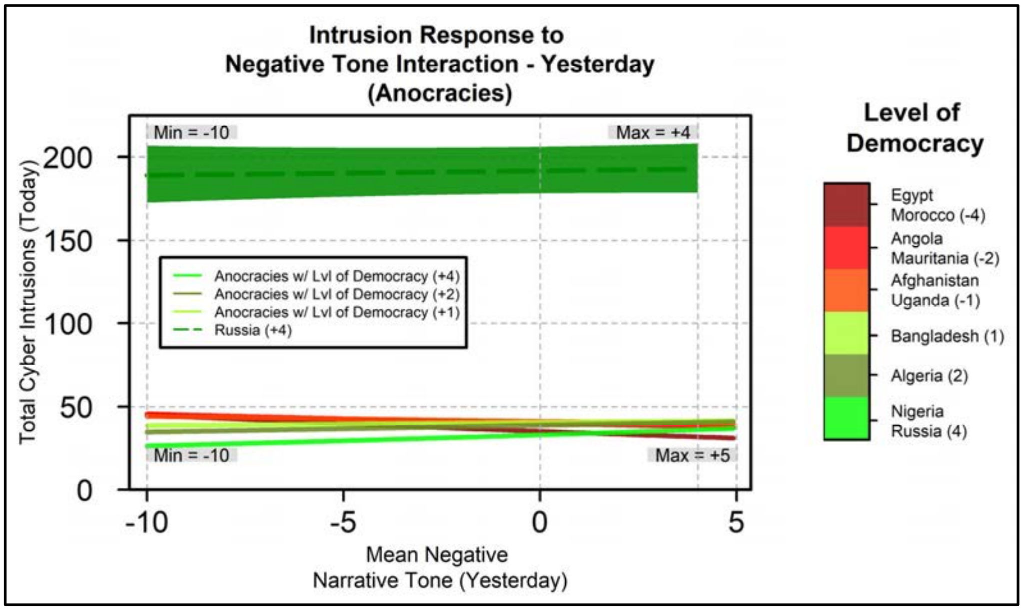
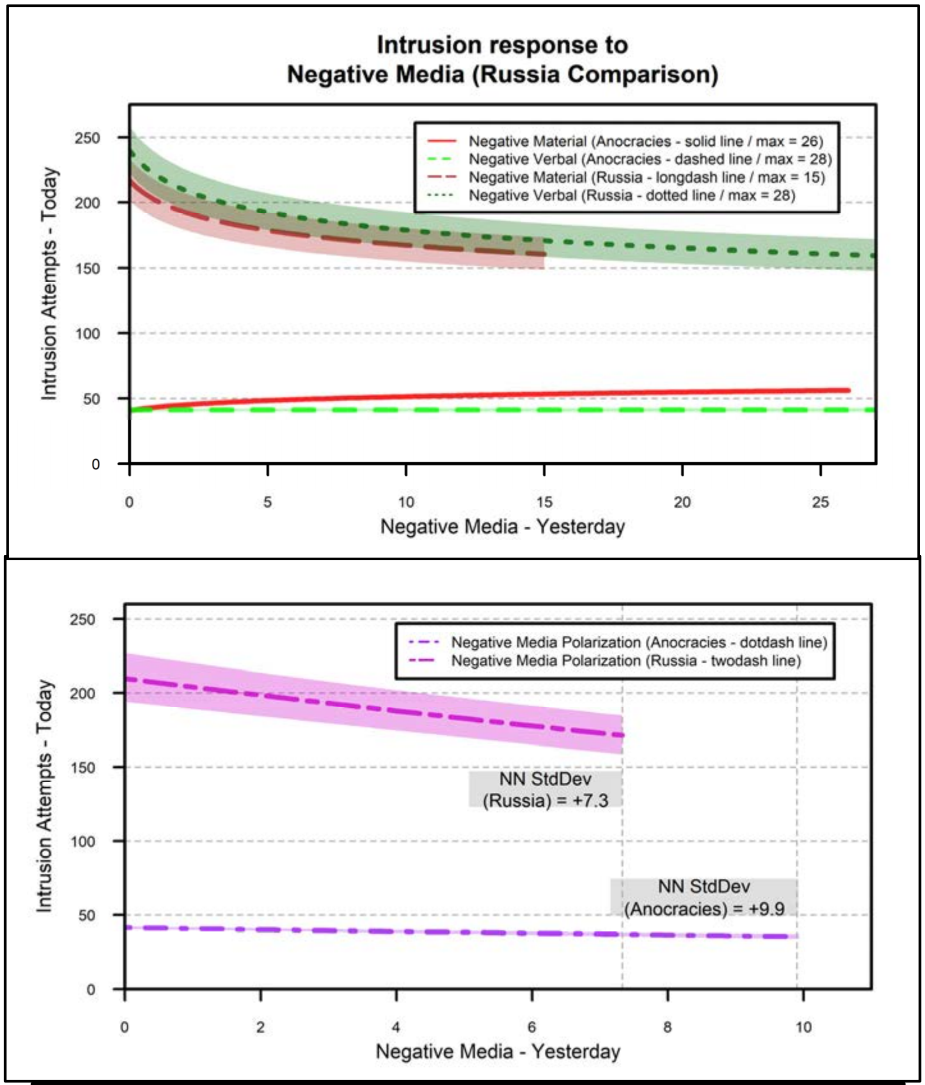


Figure 23. Negative Narrative Tone Results: Russia.

This signifies that those Russians who indulge in intrusive behavior, do so at a higher skill level, as stated. First, the Russian regime's preferred use of *patriotic hackers* to perform acts via a malicious vector to realize either subversive or information-seeking objectives appears to be operating here. Russia employs these active measures for two reasons, one to apply pressure on the U.S. during negotiations and second, the exercise of their state-sponsored *patriotic hackers*, which also provides them with a level of plausible deniability (Calamur, 2017; Jaitner & Mattsson, 2015; MacKinnon, 2012; Snegovaya, 2015; B. Valeriano, Jensen, & Maness, 2018). Further, as a practical matter, hackers need to maintain their hacktivist skills in preparation for employment during times of need such as, Estonia (2007), Georgia (2008), Lithuania (2009), and Ukraine (2014)



Media Variable Prediction Comparison Table: Russia

Model or Regime Type / **Calculated Variable**	**Anocracies**	**Russia**	**Difference from** **Anocracies**
NmN: **AME on Intrusions** +/- **/** (SE)	0.6260*** (0.0333)	-6.7657*** (0.3405)	-7.3917*** (0.3421)
NvN: **AME on Intrusions** +/- **/** (SE)	0.0153 (0.0251)	-5.3221*** (0.2986)	-5.3068*** (0.2997)
NNp: **AME on Intrusions** +/- **/** (SE)	-0.6321*** (0.0833)	-9.2744*** (1.2271)	-8.6423*** (1.2299)

Notes:
Average Marginal Effect (AME)
Negative Material Narrative (NmN)
Negative Verbal Narrative (NvN)
Negative Narrative Polarization (NNp)
Standard Error (SE)

Statistical Significance – p-Level:
***p < 0.01; **p < 0.001; ***p < 0.0001**

Figure 24. Media Results Comparison: Russia.

(Farwell & Rohozinski, 2011; Gartzke, 2013; Jaitner & Mattsson, 2015; Lindsay, 2015; Nye, 2017; Snegovaya, 2015; Valeriano, Jensen, & Maness, 2018). As such, the number of high-risk intrusions emanating from this regime, as indicated in Appendix J, provides further quantitative evidence that this type of patriotic hacktivist behavior may operate in Russia.

Thus, as shown in Figure 24, the Russian regime exercises significant control over the internet, using second and third-generation content controls, which appears to cause many in their media to self-censor. Observe Russia's material and verbal NN records a precipitously faster decrease than anocracies, recording a marginal effect of *twelve* and whopping *347 times* below anocracies' AME, respectively. Notice, how Russia's maximum NN polarization varies *26% less* than that of other anocracies across the x-axis in the middle portion of Figure 24.[157] Next, observe how the yesterday's Russian NN polarization average marginal effect on today's intrusions decreases approximately *fourteen times* faster than the anocracies model over the x-axis count range, as derived by using the values from the table at the bottom of Figure 24 and Figure 35 of Appendix F. Further, the fact that nearly 90% of Russian citizens consume news from state-run media organizations that are not included in this study's data and given the models statistical significance, discussed above, provide ample evidence to support acceptance of H15 and H16, rejecting the null in each case.[158]

2. Turkish Evidence

The statistical coefficient comparison chart in Table 7 reveals how Turkey differs in most respects from other anocracies. First, notice the negative material narratives that scores a 0.3, but scores *no* statistical significance, unlike the All-Regimes and the

[157] Per Figure 24, the maximum variation in Russia's NN Polarization score clocks in at +7.3, while the max for anocracies comes in at +9.9 – a difference of 2.6. Thus, the calculated percentage difference would be (2.6 / 9.9 = .26 ~ 26% less than anocracies.

[158] **Hypothesis #15 (H15):** *Increasingly* conflictual (i.e., negative) *material* and *verbal* interactions reported in Russian media narratives directed at the United States (U.S.) and its interests—yesterday, results in *decreased* cyber intrusion activity, emanating from Russia, on U.S. networks—today.

Hypothesis #16 (H16): *Increases* in the variation of negative narrative tone, indicating an increased level of media polarization, across media stories originating from Russia directed at the U.S. and its interest—yesterday, results in *decreased* cyber intrusion activity on U.S. networks—today.

anocracies models. Secondly, observe how the negative verbal narratives remain consistent in direction with the All-Regimes, differing from anocracies in that the coefficient records a negative statistically significant value. Thirdly, note how the NN polarization coefficient value swings opposite in sign direction from the other models and clocks in at a lower level of statistical significance (p-value < 0.05). Figure 26 and Appendix I reveals the magnitude, sign direction, and predicted value differences for these coefficients between Turkey and the anocracies models.

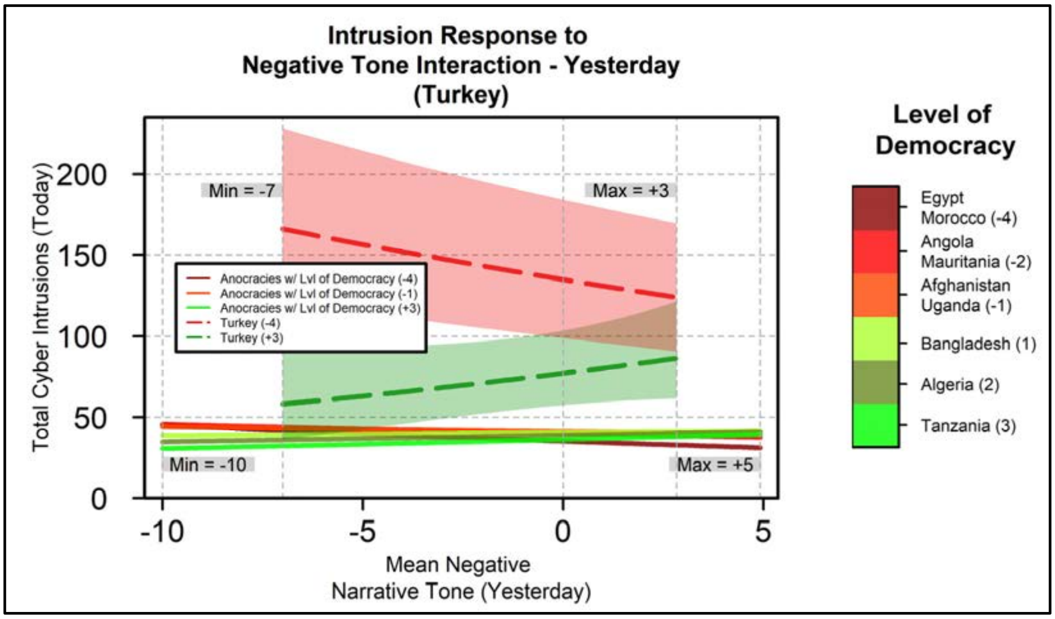


Figure 25. Negative Narrative Tone Results: Turkey

Fourth, as stated earlier Turkey swung from being an open anocracy (+3) in 2014 to a closed anocracy (–4) in 2016. Observe, how Turkey's NN tone interaction coefficient tracks precisely in direction and varies slightly more than the other anocracies across their shift in level of democracy as indicated by the reduced p-value less than 0.05 a gauge of the models reduced predictive confidence for this coefficient. Figure 25 depicts both the similarities in sign direction and magnitude of differences for this interactive variable. Nevertheless, as Turkey's polity score shifts lower shown in red and as *yesterday's* NN tone increases more intrusion occur on U.S. networks *today*, as shown in Figure 25. This finding runs parallel to that of the anocracies model. Further, note the tighter NN maximum tone range (–7 to +3), which appears to signify the regime's restraint or internally focused rhetoric toward the U.S. during period of governmental transition. Certainly, analyzing Turkey in this context provides a unique opportunity to observe the intrusion response resulting from this coefficient at the country level. Taken together, this provides the support necessary to accept H21 and reject the null.[159]

This provides another indication of transitional turbulence facing Turkey over this period, Erdoğan declared a State of Emergency that lasted for two years from 20 July 2016 to 20 July 2018 (Altiparmak & Gürol, 2017; Eldem, 2020, p. 461). The coup attempt that spawned the State of Emergency furnished Erdoğan and the AKP with optimal control of the internet and the media allowing them to leverage second and third-generation content controls to dominate the Turkish domestic narrative.[160] Further consider how the freshly spurned, but cyber competent, Gülenists and Kemalist secularists, may be using their abilities to circumvent these controls turning to information seeking to gain some understanding of events beyond the NN tone fed to them by the recently dominant AKP regime.

Also, the diminished statistical significance recorded by the NN polarization and NN tone interaction coefficients may indicate that Turkey's internet and media space over this period of analysis was *hotly contested*. To state more clearly, the tech savvy Gülenists, banished from government positions, indulging in information seeking behavior, looking for information on the AKP controlled internet may have had a difficult time as well as AKP may have encountered difficulties in preventing the expelled Gülenists from gaining access to that information. Yet, externally Turkey's presence and response appears more restrained.

[159] **Hypothesis #21 (H21):** *Increases* in the accumulated conflictual or negative *tone* of interactions reported in media narratives from Turkey directed towards the United States (U.S.) and its interests—yesterday, results in *increased* cyber intrusion activity on U.S. networks—today, with the effect becoming stronger as Turkey's level of democracy *decreases*.

[160] A year after the end of the State of Emergency (2019), the V-Dem project scored Turkey's media censorship as indirect, but routine, while scoring their media's self-censorship as common, but incomplete (V-Dem Institute, 2019, pp. 185-188). Additionally, Turkey's internet censorship recorded a level denoting the government's consistent attempts to block internet access, except for pro-regime or content devoid of political connotations, but allowing for possible circumvention of these controls.

Turkey has attained and maintains a significant proficiency in cyberspace as shown in the intrusion risk factor counts in Appendix J; yet, the regime appears to refrain from wielding it in any cyber conflicts, disputes, or incidents recorded by Valeriano and Maness (2014, 2015, and 2016) to date. Perhaps, this is because Erdoğan and the AKP have chosen to modify their foreign policy strategy. Turning away from the age-old policy of viewing Turkey as a bridge between the East and West, shifting to a tiered policy employing *zero problems with neighbors* and *rhythmic diplomacy* focused first regionally and second internationally (Dedeoglu, 2016; Hussain & Hussain, 2017; Tabansky, 2016).[161] Finally, this noteworthy finding may not only signify a shift in Turkey's foreign policy going forward, but also provide evidence to buttress the theory of cyber restraint, wherein Turkey chooses a more restrained posture in cyberspace so as to avoid misinterpretation of intent leading to miscalculation (Valeriano & Maness, 2015).

Thus, returning to the analysis of yesterday's negative material and verbal narratives and NN tone polarization values gauging their impacts on today's intrusion attempts. Interestingly, the material narrative coefficient scores a positive value but shows *no* statistical significance, while the negative verbal narratives score a negative value with a higher level of statistical significance of p-value < 0.01 as shown in Table 7. The former could be the result of the smaller number of negative material narratives showing a max of eight on any given day with verbal storylines clocking in at a max of 14, 75% higher. Further, this coupled with regime's apparent shift in strategy, discussed above, and the fact that Turkey remains an ally of the U.S. may result in a greater level of cyber restraint, which may contribute to the material narrative coefficient's lack of significance.

Yet, the negative verbal narratives score a solid, statistically significant, negative impact on tomorrow's intrusions, recording an average marginal drop of 14 intrusions across the x-axis count range considerably below anocracies, which essentially scored zero coefficient value with *no* statistical significance. Perhaps, an indication of the freshly

[161] Ahmet Davutoglu, the foreign policy adviser to both Presidents Gul and Erdoğan, adjusted the state's foreign policy arguing that Turkey's historical legacy and geographic position made it indispensable to regional affairs and stability. This regional focus, as he envisioned, would enhance Turkish influence and gravitas globally (Hussain & Hussain, 2017).

dominant AKP elites use of their near total control of the domestic level-two narrative via the two-step flow. Further, this finding would be reinforced by the discussion above pertaining to Turkey's policy of cyber restraint and the internal focus of the regime.

Lastly, observe the NN media polarization scoring an increase in today's intrusions at an albeit with minimal statistically significant at p-value < 0.05. Next, consider that Turkey's maximum NN media polarization clocks in at a rate 22% *less* than other anocracies, which could be seen as an indicator of AKP's control over variation in media message.[162] Further, observe the table at the bottom of Figure 26 below, which records Turkey's average marginal intrusion value *seven times* greater in today's intrusions over that of anocracies resulting from rises in yesterday's NN media polarity with a minimum p-value < 0.01.

These values and their statistical significance are noteworthy, because they indicate that NN polarization in the AKP controlled press does result in an amount of curiosity leading to information seeking behavior—albeit constrained. Thus, much of Turkey's governmental cyber expertise may have been purged during the Gülenists lustration, which sent these expert hackers into the private sector. Leading, these spurned professionally trained hacktivists and other members of the population to be triggered by media NN polarization and choose to satiate their curiosity of its origin by engaging in latent information seeking behavior. Particularly, in a government controlled, or at least heavily influenced, media environment, any variation in media messaging could activate Turkey's spurned hacktivists. Appendix J records the Turkish intruder's level of expertise with 93% of intrusions clocking in at the highest level of intrusion risk. Certainly, the coefficient value, the constrained media polarization, the average marginal effect difference in intrusions, and their collectively moderate level statistical of significance could indicate

[162] The same model was used to derive the AME for each country removing all non-fluctuating variables (i.e., polity, Internet and Media Not Free, Media self-censorship, internet penetration rate, population, and GDP) because their values do not change except for Turkey and the UK in this study. As such, the predicted values of NmN, NvN, and NNP are being used holding all of the other variables constant at their mean values, while the prediction estimate is derived, very little, if any, change was observed as a result of the removal of these control variables, which allows for prediction of the AME in this case. Per Figure 26, the maximum variation in Turkey's NN Polarization score clocks in at +7.7, while the max for anocracies comes in at +9.9 – a difference of 2.2. Thus, the calculated percentage difference would be (2.2/9.9 = .22) ~ 22% less than anocracies.

that these former AKP allies may be engaging in information seeking behavior to find out the rest of the story. Each of these effects are graphically depicted in Figure 26 and in Figure 35 of Appendix F.

Essentially, these findings depict how Turkey's population over this period came to rely on fewer and fewer elites. As Erdoğan and the AKP had previously removed the military and secularists as prominent elite voices and then within this period of analysis was in the process of purging the Gülenists from their prominent positions in the government, the military, and private sector. As such, the Turkish population had *no* other choice but to rely on the AKP elites, who they had elected in 2002, when they were a democracy, ultimately leading to Turkey's fall into the anocratic realm, which may only be a waypoint to a Neo-Ottoman autocracy. Nevertheless, these fewer voices, as in autocracies, enjoy outsized influence, which can be viewed in Figure 26. Thus, these newly minted AKP elites successfully neutralized the negative material narrative effect, enhanced the diminishing impact of negative verbal narratives, and caused their banished expert hacktivist to seek to assuage their curiosity resulting from NN media polarization.

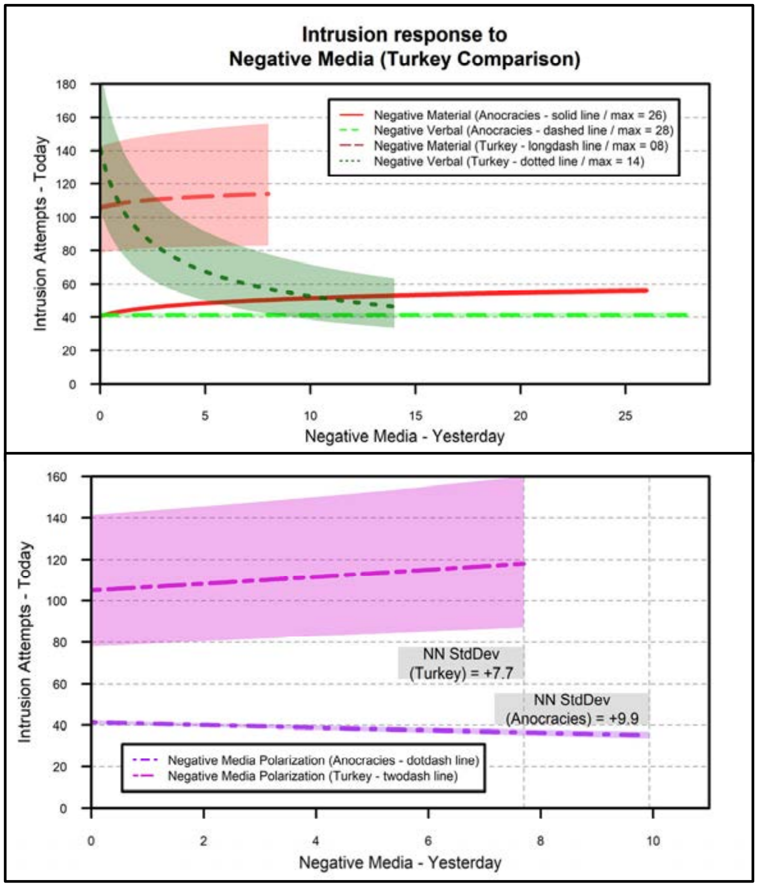
Figure 26 acutely shows this outsized influence by the dark green dotted line describing how drastically today's intrusions fall, while the Erdoğan regime engages in yesterday's negative verbal jousting with the U.S. as interpreted for them by the AKP elites. Then internally muffling any negative material rhetoric effect as depicted in the orange red long-dashed line. Finally, the uptick in today's intrusions following increases in NN polarization in the Turkish media. Thus, while the model's evidence does not support the acceptance of H18, the combination of empirical and statistical evidence does support the acceptance of H19 and H20, rejecting the null in each case.[163] The latter two may indicate

[163] **Hypothesis #18 (H18):** *Increasingly* conflictual (i.e., negative) *material* interactions reported in Turkish media narratives directed at the United States (U.S.) or its interests—yesterday, results in *increased* cyber intrusion activity, emanating from Turkey, on U.S. networks—today.

Hypothesis #19 (H19): *Increasingly* conflictual (i.e., negative) *verbal* interactions reported in Turkish media narratives directed at the United States (U.S.) and its interests—yesterday, results in *decreased* cyber intrusion activity, emanating from Turkey, on U.S. networks—today.

Hypothesis #20 (H20): *Increases* in the variation of negative narrative tone, indicating an increased level of media polarization, across media stories originating from Turkey directed at the U.S. and its interest—yesterday, results in *increased* cyber intrusion activity on U.S. networks—today.

that the two-step flow operates and reinforces level-two (i.e., domestic politics) for the negative verbal narrative type and polarization in Turkey over this period of analysis.



Media Variable Prediction Comparison Table: Turkey

Model or Regime Type / Calculated Variable	Anocracies	Turkey	Difference from Anocracies
NmN: **AME on Intrusions** +/- / (SE)	0.6260*** (0.0333)	1.9624 (1.7102)	1.3364 (1.7105)
NvN: **AME on Intrusions** +/- / (SE)	0.0153 (0.0251)	-14.0860*** (0.7801)	-14.0707*** (0.7805)
NNp: **AME on Intrusions** +/- / (SE)	-0.6321*** (0.0833)	3.4468· (1.4354)	4.0789* (1.4378)

Notes:
Average Marginal Effect (AME)
Negative Material Narrative (NmN)
Negative Verbal Narrative (NvN)
Negative Narrative Polarization (NNp)
Standard Error (SE)

Statistical Significance – p-Level:
·p < 0.05; *p < 0.01; **p < 0.001; ***p < 0.0001

Figure 26. Media Results Comparison: Turkey.

D. CONCLUSION

Over this period of analysis, these anocracies experienced different national settings. Russia sought to maintain its position as an open anocracy, while tightening its grip over the information residing in cyberspace within its sovereign borders treating cyberspace as just an additional domain to the air, land, sea, and space. Using second and third-generation content controls to sustain their age-old grasp on internal information, as captured by yesterday's NN material, verbal, and polarization tone coefficients indicating the Russian regimes firm grasp over their domestic internet and media resulting in a uniformly diminishing effect on today's intrusions. The regime employs the doctrines of active measures and reflexive control in an attempt to project influence beyond Russia's sovereign borders, seeing the intended coercive impact of each fall terribly short abroad, while appearing quite effective domestically.

On the other hand, over this period, Turkey was experiencing a convulsive transition through the anocratic realm apparently bound to end up as an autocracy. The analysis pointed out how beginning in 2002, Erdoğan and the AKP set upon a deliberate campaign to wrest power from the Guardians of Democracy (i.e., the military and secularists) seeking to set Turkey on a path towards a Neo-Ottoman future. After denuding Turkey's military and their secularist allies through the use of powerful second and third-generation content controls intent upon tracing, confusing, entrapping, and disgracing their intended targets, subsequently, the AKP shifted the aim of this cyber arsenal on their former Gülenists allies achieving the same effect. This left Erdoğan and his AKP elites as the only credible leaders remaining in Turkey, with a cyber arsenal at their disposal. Through the control of the media, which is quantified by the negative values of the negative verbal narrative and tone interaction coefficients, they appear to have consolidated their position within Turkey. This can be seen in these two variables and the muting effect on the NN material values, with NN verbal narratives scoring the highest diminishing effect on the following days intrusions across this analysis, as shown in Appendix I.

Finally, by viewing the total counts of daily average intrusions risk types in Appendix J, one can see that both Russia and Turkey possess significant cyber expertise. However, each chooses to wield their cyber capabilities differently. Russia chooses to consistently employ its cyber prowess both regionally and abroad, while Turkey prefers to hone their cyber skills leveraging them internally but choosing to constrain their provocative use beyond their borders. However, this could be a distinct result of Turkey's tumultuous domestic affairs during the period of analysis.

Nevertheless, as in Chapter IV, countries, like individuals, choose to operate in cyberspace in different ways, where context, culture, and political setting matter. Some seek to gain control of the internet within their borders to provide them with some amount of societal control, while others use the WWW to push back against their regional, international, or internal rivals. Regardless, cyberspace appears to be a dynamic environment, where countries and regime types manifest behaviors uniquely their own, yet similarities *do indeed* abound.

VI. CASE STUDY: DEMOCRACIES IN CYBERSPACE

A. INTRODUCTION

This final case study covers democracies. The democratic regime type encompasses countries such as the United States, Sweden, Germany, Mexico, Chile, Japan, Mongolia, and Nigeria to name a few. Appendix G contains the complete list of the democracies included in this study. Yet, most of the studies on regime type and the internet revolve around what some refer to as the cyber hegemon-the United States (Valeriano, Jensen, & Maness, 2018).[164] Nevertheless, this research studies the U.S. as the target of intrusions and has shown that, for some, a country's negative media narratives about the U.S. *yesterday* may result in intrusions *today*. As such, the thrust of this chapter will focus on the United Kingdom and India, one a former rival, but after the late-1800s became a solid ally of the U.S. weathering two World Wars and the other a former colonial protectorate of the United Kingdom (UK), which became a Republic in 1949. India has generally maintained a friendly relationship toward the U.S. since gaining its sovereignty.

The chapter will progress as did the last two case studies. First, a short survey of how democracies generally view cyberspace and their position within the WWW. Second, the research will empirically explore how both the UK (Britain) and India control, monitor, or police their internal internets, leading to a series of hypotheses for each country. Third, the researcher will use the existing model to test each hypothesis and the chapter will concluded by comparing these two democracies' media and cyber-space environments.

[164] As the principal state that won two world wars, propagated democracy across the globe, and developed the internet, all in the last century, has made the U.S. the most likely democratic regime to incur cyber intrusions on its networks (Axelrod & Iliev, 2014; Choucri, 2012; Gartzke & Lindsay, 2015; Kello, 2013; Lindsay J. , 2013; Nye J. S., 2017; Valeriano, Jensen, & Maness, 2018). The U.S. prescribes certain agencies to handle different threats (i.e., incursions, infiltrations, exploitations, etc.) within cyberspace leveraging a whole of government approach. Additional, doctrine of how the U.S. intends to use and respond to potential threats in cyberspace is well documented its cyber strategy and joint publications, described as a combination of stealth and surgical strikes (Carter, 2015; Joint Chiefs of Staff, 2014; Valeriano, Jensen, & Maness, 2018, p. 179).

B. DEMOCRACY RIDING THE THIRD WAVE

Certainly, democracies embody some of the most politically messy regime types on the planet. Considering their open internet space, manipulation of the media riding on and through the WWW can originate from state, non-state, or even transnational actors all with different intentions and means to act upon those intentions. After the terrorist attacks on the U.S. in 2001, democracies became increasingly aware of enemies that might be residing in or moving through their populations, enemies who bore malice towards the state as a whole. As such, many enacted laws allowing for the prosecution, surveilling, and tracing of individuals involved in terrorist recruitment, planning, or propaganda on the internet (Deibert & Rohozinski, 2010). Terrorist acts, plus, the exploitation of children and copyright infringement mark the main thrusts of democratic censorship in cyberspace (Deibert, 2015; Goodman, 2015; MacKinnon, 2012; Morozov, 2011). All the while, democracies continue attempting to maintain a balance between protection of their country and the right to freedom of speech and assembly.

As such, many democracies enhanced their pre-existing laws or, as did the U.S., enacted new laws providing the government with the right to surveil its population using delayed notice, sneak-a-peek, or no-warrant at all (Chesterman, 2011; Freedom House, 2017; MacKinnon, 2012; McHugh & Ramirez, 2018; Morozov, 2011). Yet, most democracies, most anocracies, and even some autocracies seem to outsource censorship to third party companies, holding the likes of Apple, Facebook, and Google accountable for the content or narratives authored by their users. However, this policy outsourcing both causes and enables these companies to respond to the issue of the day, with very little thought going into a given censoring decision besides how it will affect their profit margin (Chesterman, 2011; Freedom House, 2017; Goodman, 2015; MacKinnon, 2012; McHugh & Ramirez, 2018; Morozov, 2011; Shahin & Zheng, 2020).

Some countries within the European Union, India, and South Korea, placed the responsibility on these companies using broad, ill-defined terms such as *spreading false information*, *grossly harmful*, *harassing*, or *ethically objectionable* to describe illegal internet content (MacKinnon, 2012). Many others have adopted state-level filtering protocols directing ISPs to block certain illicit content (MacKinnon, 2012; pp. 95–96).

However, one state's harmful, misleading content is another's right to free speech or artistic expression. On the internet the culture of the state matters when it comes to the amount of censorship their population may expect or tolerate—democracies epitomize this fact in the extreme (Morozov, 2011).

Thus, democracies may possess significant surveillance structures as a hedge against crime and terrorism, but their media spaces, with their manifold competing narratives, may appear to some anocracies and autocracies as sheer and utter chaos.[165] For western democracies, as many scholars have theorized and others have observed using communications, chaos, or systems dynamic theories, order *emerges* out of an apparently amorphous, chaotic system of systems (SOS) (Barabasi, 2003; Barabasi, 2016; Capra, 1996; Johnson IV, Tolk, & Sousa-Poza, 2013; Sterman, 2010).[166] While some autocracies and anocracies may not understand democracy's media bedlam, they certainly manifest a respect for its capabilities and do, as recent U.S. presidential elections have shown, attempt

[165] Recently, in a journal article concerning media bias during the Libyan Civil War during (2010-2011), Matthew Baum and Yuri Zhukov (2015) conjectured that during times of conflict, either internal to or between states, democratic media outlets tend to engage in a "*framing* war," which coincides with the "shooting war." The authors discovered that the media narrative in democracies, being *independent* from government influence and driven by commercial preferences to maximize profits, tend to favor rebel – anti-regime forces (Baum & Zhukov, 2015). Further, they describes democratic media biases that emphasize originality, conflict, proximity, and drama as basic criteria for newsworthiness (Baum & Zhukov, 2015, p. 397). These biases seem to drive the media narrative. For example, democratic media appears to *under* report rebel atrocities, while *over* reporting regime violence, whereas, media in non-democracies (i.e., Autocracies and possibly Anocracies) the opposite is true (Baum & Zhukov, 2015). Further, the authors conjectured that anti-regime, democratic media bias *could pressure* western leaders to contemplate foreign intervention, particularly in cases of civil war, which empirically occurred in this case (Baum & Zhukov, 2015, p. 397).

[166] System of Systems (SOS) – a super system or meta system comprised of elements which themselves are independent systems, and interact among themselves to achieve, either wittingly or unwittingly, a common goal (Johnson IV, Tolk, & Sousa-Poza, 2013, p. 284). Emergence of patterns/properties in a complex system will come about (emerge) through operation of the system (Keating, 2009, p. 170).

to influence it, perhaps out of their respect or fear of it (Inkster, 2016; Maréchal, 2017; Morozov, 2011; Valeriano, Jensen, & Maness, 2018).[167]

1. United Kingdom in the Third Wave

As in most other case studies of the different regime types—culture matters. Consequently, Britain is no different. The United Kingdom is a long standing ally and has, in the recent century, enjoyed, what some describe, as a special, close, or intimate relations with the U.S. (Bull, 2012, p. 167; Marsh, 2012; Oliver & Williams, 2016; Treharne, 2015). Since, the late 1800s early 1900s, the U.S. and the UK have been on a non-rivalrous path (Millett & Maslowski, 1984). Both have endured and created a lot together as allies in last century's two World Wars and one Cold War, strong trading partners for over a century, founding members of the post WW II North Atlantic Treaty Organization (NATO), and signals intelligence partnership known as the Five Eyes (Buckley, 2004; Millett & Maslowski, 1984; Nye, 2007; Nye, 2014; Valeriano, Jensen, & Maness, 2018).[168] Finally, both hung together through the post September 11, 2001 (9/11) period, working through the difficult and protracted wars in Iraq and Afghanistan (Marsh, 2012; Oliver & Williams, 2016; Strong, 2017). Perhaps, no two other countries personify the theory of democratic

[167] This respect or fear stems from the Radio Free Europe or Voice of America narrative, which attributed some or most of the responsibility for the fall of the Berlin Wall to democratic media programming beamed into the former satellites of the Soviet Union. As the story goes positive, media narratives broadcast into the Eastern bloc countries made that populations aware of freedoms and standard of living their western European brothers and sisters enjoyed under democratic forms of government. Some qualitative scholars theorized that West German Television (WGTV) broadcast into East Germany near the end of the Cold War, circa 1989, assisted in the coordination of anti-regime protests (Grix, 2000, pp. 32-33; Jarausch, 1994, p. 44; Kuran, 1991, p. 37; Opp & Gern, 1993, pp. 675-676). Crabtree, et.al. (2015), building on the work of other scholars in this arena, realized that WGTV was able to broadcast to *some* but *not all* of East Germany; thus, matching signal strength to spatial protest location found no statistical evidence that WGTV had an impact on anti-government protests in East Germany (Crabtree, Darmofal, & Kern, 2015; Grdesic, 2014; Kern, 2011). Out of this awareness sprang the distribution of clandestine samizdat materials, within eastern Europe, demanding increased freedoms and better standards of living conditions, ultimately, leading to the fall of the Berlin Wall and subsequently, the collapse of the Soviet Union (Buckley, 2004; Crabtree, Darmofal, & Kern, 2015).

[168] Sometimes referred to as the allied cyber [intelligence] network, the Five Eye countries include; Australia, Canada, United Kingdom, United States, and New Zealand (Deibert R. J., 2013, p. 252; Eldem, 2020; Nicholson, 2019; Nye J. , 2014; Valeriano, Jensen, & Maness, 2018, p. 195).

peace and its special relationship more than the U.S.-UK dyad (Buckley, 2004; Bull, 2012; McDonald, 2015; Strong, 2017).[169]

This special relationship may indeed lead to the indexing of U.S. opinion leaders or elites in UK media, which results in reverberation (Putnam, 1988; Strong, 2017).[170] Strong (2017) provided evidence of this phenomenon specifically in the U.S.-UK dialog leading up to the wars in Afghanistan and Iraq as well as the Libyan intervention, positing a third level to the original two-level process of domestic and international relations. This level-three process is best captured as foreign-domestic interaction as described in media reports about foreign, in this case U.S., elites' or actors' statements or actions, which reverberate in the target country's media, in this case the UK, resulting in a modification of their international policy. (Conceição-Heldt & Mello, 2017; Putnam, 1988; Strong, 2017). Indeed, the research done here may buttress Strong's conjectures, but cannot provide sufficient evidence beyond level-one and two.

Further, Reifler et al. (2014) in their analysis of public opinion surrounding Britain's participation in the Afghanistan surge and in the Libyan intervention found Briton's decisions in matters of foreign affairs to be decisively prudent and morally principled (Tomz & Weeks, 2013). Prudent in their war or intervention cost-benefit calculus as to whether either would damage their national interests or literally cost too much (Reifler, et al., 2014). Additionally, in each case Briton's public opinion remained consistently *against* war and intervention, breaking sharply with their Members of Parliament (MPs) who remained staunchly supportive, indicating a disregard for elite cues (Reifler, et al., 2014). Indeed, in domestic matters, British public opinion tends to align generally with their leadership and party affiliation, vis-à-vis their political elites (Newton, 1999; Reifler, et al., 2014, p. 50). Certainly, over the centuries, the relationship between

[169] Further, Tomz and Weeks (2013) indicate in their research that public opinion shows a special zone of peace amongst democracies. Their study found that democratic states were less likely to use military force against other democracies and regard such use as immoral (Tomz & Weeks, 2013). Conversely, a democratic state using force against an autocracy was more likely and perceived as just (Tomz & Weeks, 2013). Obviously, buttressing the democratic peace theoretic.

[170] Reverberation – how statements and actions of foreign actors (i.e., elites) reported by media sources can affect the domestic politics of another state, thereby, influencing the foreign policy decisions of that state (Putnam R. D., 1988; Strong, 2017)

British elites and publics has stood as distinctively different from other European countries.[171]

Thus, the two-step flow may operate within Britain as it pertains to domestic issues; however, in the international affairs arena British publics appear to manifest an independence of mind separate from their elites (Best & Higley, 2018; Newton, 1999; Reifler, et al., 2014; Tomz & Weeks, 2013).[172] This pattern of behavior displayed by their citizenry may manifest itself in the intrusive behavior of the would be British hacker. Indeed, their penchant for prudence and morality, particularly in their foreign interventions, may present itself in their intrusive activity (Reifler, et al., 2014; Tomz & Weeks, 2013). Further, as Tomz and Weeks (2013) discovered in their research, Brits find it morally wrong to *attack* another democracy. Particularly, a democracy whose relations with Britain is considered to be close, special, or unique such as their relationship with the U.S. (Bull, 2012; Marsh, 2012; Oliver & Williams, 2016; Strong, 2017; Treharne, 2015). Since, as pointed out in the literature review, the media's use of the term *cyber-attack* with all of its weaponized baggage may in this British case assist in deterring or dissuading the UK hacker population from intruding in U.S. networks (BBC, 2017; Kroft, 2015; Czosseck, Ottis, & Taliharm, 2013; FireEye, M-Trends, 2016; Gandhi, et al., 2011; Harris, 2017; Stavridis, 2015; Valeriano & Maness, 2015). Finally, as stated when one considers this evidence alongside the US–UK special relationship rubric, British hacker behavior could sharply break with that of the ordinary democratic intruder captured by the democracies

[171] Britain's elites seem to possess an exceptionalism unique to others in Europe. Since the observations made by Alex de Tocqueville in the late-1700s, Britain's nobles displayed uniquely different characteristics from their marriage practices to the ways in which elites treated their subjects (De Tocqueville, 1856). Britain was able to deftly weather the tumultuous era of the French Revolution, the deposing of the French monarchy, the rise of Napoleon Bonaparte and an almost decade and half of constant war that followed (Best & Higley, 2018; Connolly, 1979; De Tocqueville, 1856). Further, the UK was able to soldier through the various exogenous shocks of the nineteenth and twentieth centuries managing internal social issues along the way through evolution not revolution. Indeed, British elites appear quite capable of skillfully making inclusive concessions (i.e., rights to citizenship) to previously disenfranchised elements of their population and by doing so avoiding the terribly destructive tendencies that personified the French Revolution (Best & Higley, 2018; Connolly, 1979; De Tocqueville, 1856). Thereby, British elites have created a stronger bond of trust with their population, beyond that of most modern-day democracies. The most recent populist Brexit movement continues to highlight how British elites lack political trust in concept of the European Union, showing a continued trend of distrust in the continental elites and their methods (Best & Higley, 2018, p. 453).

[172] The most recent instantiation being the 2016 Brexit vote (Best & Higley, 2018).

model, where increases in NN material and verbal daily counts on a given day result in increasing intrusions on U.S. networks the next day. This British model may reflect an opposite reaction to these NN types.

Further, reverberation may manifest itself as well. Meaning, increases in yesterday's negative media polarization, resulting from differing views of U.S. elites' opinions concerning British policies around some issue, could lead to increased intrusions today. As these British hackers' resort to information seeking behavior to discern, for themselves, the reality of the issue at hand.

Finally, over this period of analysis the UK drifted to a lower level of democracy from +10 to +8 (Freedom House, 2017; Freedom House, 2020). Due to the British government's revision of their authority to surveil the population, because the previous laws governing these authorities were deemed illegal by the European Court of Justice (ECJ). These revisions coupled with the rise of anti-immigration sentiment, which ultimately led to the Brexit vote, to leave the European Union in 2016, taken together were viewed as a degradation of Britain's position as a liberal democracy.[173] As such, this provides another unique opportunity to observe how yesterday's NN tone at varying levels of democracy leads to changes in today's intrusions coming from Britain, in this case. Thus, similar to Turkey, one would expect at this discrete country-level of analysis that Britain's response to increases in *yesterday's* NN tone as their level of democracy decreases to result in increases in intrusions *today*. Further, as shown in Appendix J, British intruders tend to manifest a level of cyber sophistication similar to that of Turkey—intruding at the higher average risk level. Next, the research turns to reviewing the British version of the digital panopticon.

The British appear to have avoided many of the negative aspects of employing the digital panopticon. Indeed, the main visual tell of the existence of the digital panopticon in Britain resides in the form of the ubiquitous closed-circuit television (CCTV) cameras across the UK. The UK's CCTV network is vast, numbering approximately 4.2 million

[173] Brexit was the British colloquialism used to describe the populist referendum to exit the EU (Freedom House, 2017).

devices (Deibert & Rohozinski, 2010). To place this in context, that is approximately one camera for every 14 UK citizens, which accounts for approximately 20% of the global CCTV installation (Morgan, 2013; Wu, Tao, & Chang, 2017). Impressive considering that Britain possesses roughly 0.86% of the earth's population (CIA, 2019).

Structurally, the UK has been able to avoid the incumbent suspicion of their ubiquitous use of public surveillance systems. Norris and Armstrong (1999) recorded that 90% of Brits agreed with the use of CCTV systems. Further, many in Britain regard those who oppose CCTV's use as *heartless,* perhaps due to the brutal murder of two children in Liverpool (1993), which may have been prevented, if this system had been in place (Wu, Tao, & Chang, 2017). Although, the British authorities have encountered some setbacks support for these types of automated system when used for police purposes, support remains solid amongst the general public in most locations.[174]

Additionally, the British government's common practice of conducting community audits that are intended to hear from and involve the local citizens in the planned use of public CCTV systems prior to its introduction certainly engenders public buy-in for deployment of these systems (Zurawski, 2004). Further, concerns that Britain will become an *Orwellian surveillance state* continually resonates across British media and their political spectrum with some periodicity (BBC, 2009; Deibert & Rohozinski, 2010; Orwell, 1949). Yet, Britain possesses a robust legal system resting on laws concerning surveillance that date back to 1990s and is strictly adhered to by government entities (Deibert & Rohozinski, 2010; Wu, Tao, & Chang, 2017; Zurawski, 2004). Perhaps their CCTV

[174] The *troubles* in the British province of Northern Ireland spanning from 1969 to 2007 provide the case in point. Centuries before, the British government established the province's economic and governmental power structures, which strongly favored and benefitted the minority Protestants over the majority Catholics. In 1969, age old grievances borne out of existing systematic power structures boiled over leading to violent clashes between the two groups. The government immediately deployed military units to separate the two and keep the peace. As the *troubles* wore on, the Catholics and the Protestants created sophisticated surveillance networks to monitor each other and their intergroup members, while the British military attempted to surveil both to keep the peace using existing mechanisms of social control (Zurawski, 2004). Gradually, the military began emplacing CCTV towers, primarily surveilling the Catholic areas, revealing their government's lack of neutrality in the *troubles* (Zurawski, 2004). Ultimately, as the 1998 peace initiatives began to gain traction and the military units began to withdraw, control of the state-of-the-art CCTV surveillance infrastructure devolved to the local police for crime prevention and security purposes. Nevertheless, due to the nearly thirty years of ubiquitous physical or virtual surveillance and control, the Catholic community in Northern Ireland still view the CCTV systems with disdain and suspicion (Zurawski, 2004).

deployment policies, their societal anxiety over becoming a surveillance state, and their robust structure of laws protecting individual rights and civil liberties produces a level of assurance that the British government will use these CCTV systems for crime prevention and security and not for societal control (Deibert & Rohozinski, 2010; Freedom House, 2020; Wu, Tao, & Chang, 2017).

Hypothesis #22 (H22): *Increasingly* conflictual (i.e. negative) *material* and *verbal* interactions reported in British media narratives directed at the United States (U.S.) or its interests—yesterday, results in *decreased* cyber intrusion activity, emanating from the UK, on U.S. networks—today.

Hypothesis #23 (H23): *Increases* in the variation of negative narrative tone, indicating an increased level of media polarization, across media stories originating from the UK directed at the US and its interest—yesterday, results in *increased* in cyber intrusion activity on U.S. networks—today.

Hypothesis #24 (H24): *Increases* in the accumulated conflictual or negative *tone* of interactions reported in media narratives from the UK directed towards the United States (U.S.) and its interests—yesterday, results in *increased* cyber intrusion activity on U.S. networks—today, with the effect becoming stronger as Britain's level of democracy *decreases*.

Figure 27. United Kingdom – Case Study Hypotheses

Finally, while there is evidence of the UK's presence in cyberspace, overt action in what Valeriano and Maness (2015) would describe as cyber conflicts, disputes, or incidences remains non-existent. Although a Russian target of cyber incidences in 2011 and 2014, any evidence of British retaliation remains muted (Valeriano, Jensen, & Maness, 2018). Even though Britain's cyber sophistication exists at a level on par with that of the other Five Eyes members, they apparently prefer to constrain their employment of it or clandestinely channel their cyber retaliations through the Five Eyes infrastructure, thereby, masking their capability and intent. Thus, just as Valeriano, Jensen, and Maness (2018) propose that the Five Eyes mechanisms and cooperative activities extend the US's cyber capabilities, so to, the alliance may offer certain advantages to Britain as a silent partner in cyber conflicts, disputes, and incidence. Certainly, an unverifiable conjecture at the unclassified level of analysis, but entirely plausible. Accordingly, by considering all of the information provided about Britain in this section, the hypotheses delineated in Figure 27 below are provided for testing by the statistical model used throughout this research project. Now the research changes focus to the other democracy in this study—India.

2. India in the Third Wave

India stands as the world's largest democracy with a population of 1.3 billion citizens, with 72% primarily Indian with 80% practicing the Hindu faith (CIA, 2019). India's large predominantly homogenous population tend to be voracious consumers of media from diverse sources with 90% checking news sources at least once a day (Aneez, Neyazi, Kalogeropoulos, & Nielsen, 2018; CIA, 2019). However, with a 32% internet penetration rate, television and broad sheet newspapers still dominate, but their rate of growth continues to decrease (Aneez, Neyazi, Kalogeropoulos, & Nielsen, 2018). Further, Indian's media consumers continue to use news from diverse sources numbering between 11.2 to 5.7 outlets per media consumer—a rate higher than most peer countries (Aneez, Neyazi, Kalogeropoulos, & Nielsen, 2018, p. 13; Freedom House, 2019). Thus, while Indians are voracious consumers of diverse news sources, the population still looks to the old-guard or more recently the nouveau—elites for their interpretation of policy and media stories to gauge their potential reactions on a given subject as drawn out in the V–Dem and other research (Mechkova & Lindberg, 2016; Mohan, 2015; Natarajan, 2014; Oldenburg, 2018). As such, India, most likely more properly aligns with the All-Regimes, autocracies, and anocracies models; thus, it should be expected that *yesterday's* negative material narratives will correlate positively, while the verbal narratives clock a diminishing impact for intrusions on U.S. networks *today*.

Along with this information, India manifests a labyrinth of elites spanning from National, to State, and to the local village level (Oldenburg, 2018). Consequently, India's population, more so than other democracies, looks to either their time-honored elites or neo-elites involved in social movements to interpret contemporary events (Bjola & Manor, 2018, Conceição-Heldt & Mello, 2017; Higley & Burton, 2006; Mechkova & Lindberg, 2016; Mohan, 2015; Natarajan, 2014; Oldenburg, 2018; Putnam, 1988; Strong, 2017; Trumbore, Boyer, Gibson, Harvey, & Wilkenfeld, 2000). Further, like most other democracies, the Indian media exemplifies the cacophony of voices that make up the competing narratives as the country attempts to influence another nation in diplomatic negotiations (Bjola & Manor, 2018, Conceição-Heldt & Mello, 2017; Mechkova & Lindberg, 2016; Natarajan, 2014; Oldenburg, 2018; Putnam, 1988; Strong, 2017; Trumbore, Boyer, Gibson, Harvey, & Wilkenfeld, 2000). So, after initial increases in NN tone leading to increases in Indian media polarization, the population increasingly looks to their elite structure in the two-step process, operating within level-two of domestic politics to make sense of international events. So, increases in yesterday’s NN tone in Indian narratives about the U.S. may cause an increase in today’s intrusions—initially. But, the much more dominant effects expected out of the India model will result from the two-step flows operation as manifested by negative material and verbal narratives and NN media polarization.

Certainly their citizens’ attempts to tease out the truth as may be indicated by changes in NN tone, but at times, the Indian government and the courts have blocked information considered politically sensitive, which allows the government to control the narrative surrounding such issues (Aneez, Neyazi, Kalogeropoulos, & Nielsen, 2018; Freedom House, 2019). All of these elements come together causing Indian citizens to look to their elites for their opinions on events, which subsequently, influences their actions. This became acutely apparent with the 2009 roll out of the technologically enabled unique identification project (UID), known as Aadhaar (in the Hindi language the word means foundation) (Goodman, 2015; Rao & Nair, 2019, p. 469; Shahin & Zheng, 2020, p. 25).

Domestically, a few years earlier than China’s Social Credit System (SCS), and for different reasons, India embarked on development of the Aadhaar system in an attempt to take account of everyone in their population (Goodman, 2015; Rao & Nair, 2019, p. 469; Shahin & Zheng, 2020, p. 25). The Unique Identification Authority of India (UIDAI) began and currently runs the Aadhaar program, which was originally envisioned to end the chain of corruption endemic to the Indian social welfare system (Shahin & Zheng, 2020).[175]

Enter Aadhaar, which was envisioned to register every one of India's 1.3 billion citizens, attempting to capture unique attributes of each individual's identity, thereby allowing welfare payments to be made directly into the recipient's bank account, thus cutting many elements in the bureaucracy out of the transfer chain (Rao & Nair, 2019). Ostensibly, this was indeed the intended purpose of this biometric system to ensure their unique identity.[176] Indian media and elites used Foucault's argument that without the ability to discretely identify each individual in society any government system would be rife with corruption, thereby hampering planned growth and development (Foucault & Ewald, 2003; Rao & Nair, 2019). As of 2019, the UIDAI had nearly completed registering the entire population and each citizen had knowingly exchanged their name, age, gender, address fingerprints, iris scan, and facial photograph for a twelve-digit unique identification code (Rao & Nair, 2019; Shahin & Zheng, 2020). Next, the Indian government made it *mandatory* for their citizens to possess this code to gain access to a variety of financial, governmental, and social services such as bank accounts, insurance policies, gas subsidies, tax payments, etc. (Rao & Nair, 2019, p. 476; Shahin & Zheng, 2020).

Further, Indian media coverage and elite voices, at the beginning, tended to focus initially on the benefits of the program to the average citizen, while blithely vaulting over the fundamentally obvious privacy issues brought about by the collection of each citizen's biometric and personal data (Shahin & Zheng, 2020). It was not until the 2013–2014 time frame, after the project was well underway that India's news media began reporting and

[175] Previously, welfare payments or transfers made by the India government to poorer citizens flowed through the nation's massive bureaucracy; however, as the money flowed through the system, bureaucrats or other nefarious characters along the way would take their cut of the payment ending up with the average beneficiary receiving very little of the dedicated subsidy (Rao & Nair, 2019; Shahin & Zheng, 2020). Policy Officials in India estimate that only about 15% of each rupee (i.e. India's currency) spent makes it to the intended welfare beneficiary (Rao & Nair, 2019, p. 473). Blunting the intended effect of the social welfare systems, which was intended to assist the poor in India society, not facilitate corruption within the bureaucracy.

[176] Initially, the UIDAI used fingerprints alone as the biometric of choice to ensure individual identity; however, in India where most labor in done by hand, fingerprint quality can be of quite low quality (Rao & Nair, 2019, p. 475). Thus, UIDAI decided to add iris scan into the unique set of biometrics collected on each individual (Rao & Nair, 2019, p. 475).

Indian elites began voicing concerns about the privacy issues inherent to this type of mandatory data collection (Dixon, 2017; Goodman, 2015; Rao & Nair, 2019; Shahin & Zheng, 2020).

Subsequently, as in all these cases technology moved faster than government policy. Elements of the government began to find uses for Aadhaar to ostensibly track criminals, illegal immigrants, and other people within the population who were not citizens of India. As recent as 2017, the Indian legislature had enacted very few laws to protect the data much less the citizens against the wrongful use of their data by *rogue* government employees or the technology companies that made Aadhaar a reality (Dixon, 2017; Goodman, 2015; Shahin & Zheng, 2020). All the while, the government continued to build out their version of the digital panopticon, even as evidence of Aadhaar's abuses continued to mount (Dixon, 2017; Goodman, 2015; Shahin & Zheng, 2020).

Indeed, India, unlike China's SCS, had unwittingly created the means to achieve the digital panopticon via Aadhaar to fix the governmental problem of a citizen's physical identity, while simultaneously and perhaps unintentionally creating a sophisticated system to surveil and track its own population. Now to adjust the focus, turn to India's external cyber presence.

The 2008 terrorist attacks in Mumbai shook the very foundations of the Indian government, pointing to their collective ineptitude in cyberspace (Deibert R. J., 2013, pp. 92-94). As such, this singular event, coinciding with a spate of corrosive hacks originating from China, propelled India into the expansive use of second-generation content controls in the name of none other than *national security* concerns (Deibert R. J., 2013; Deibert R. , 2015). Indeed, the Indian administration followed the well-worn path of multiple other states across the regime spectrum by enacting vaguely written laws to compel commercial vendors such as Facebook, Google, Microsoft, Research in Motion (RIM), and Yahoo to establish a *proactive prescreening system* to ferret out any objectionable content and remove it (Deibert R. J., 2013, pp. 92-94).[177] Again, as in many other cases, this directive to remove internet content was accompanied by exceedingly broad and imprecise language of what constituted *objectionable content*, coupled with precisely targeted legal ramifications for non-compliance.[178] As a case in point, executives would be subject to fines and up to seven years in jail for not complying (Deibert, 2013, pp. 92–94).

To address India's internal lack of cyber acumen, the government created the National Technical Research Organization (NTRO), their version of the NSA in the U.S., to reach out virtually to an interdisciplinary group specializing in cyber espionage at the University of Toronto known as Citizen Lab run by Dr. Ronald Deibert (Deibert, 2013). The Lab found their request simultaneously astonishing and illuminating. The requested revealed India's lack of cyber prowess, their willingness to accept outside help, and their readiness to outsource cyber issues, if necessary, to handle the Chinese threat (Deibert, 2013). While the author found the events surrounding these incidents as chronicled by Deibert (2013) profoundly riveting, a complete rendering here lies well beyond the scope of this research.

Suffice it to say, that even though this research has discovered that the Chinese prefer mass over sophistication in their intrusion tactics, their penetration into India networks prior to 2010 was vast, thorough, and complete. Subsequently in 2013, India set upon an ambitious plan to quickly develop a cyber capability to include ethical hacking techniques and a half a million strong cyber army (Deibert, 2015; Ministry of Electronics and Information Technology, Government of India, 2020). This evidence supports what many scholars and world leaders have posited over the centuries: quantity does, indeed,

[177] The most infamous was India's aggressive pursuit of RIM to comply with their "lawful access" demands. These demands required RIM to host their data on servers within India and assist the government in its surveillance requirements (Deibert R. J., 2013, p. 94 & 109; Deibert R. , 2015, p. 67). At times, even threated to expel RIM from India entirely if the company chose not to comply with their requirements (Deibert R. J., 2013, p. 109; Deibert R. , 2015, p. 67). Ultimately, this relentless pressure led RIM to acquiesce to India's cyber mandates. Even agreeing to train Indian cyber experts in specialized surveillance techniques (Sharma, 2011).

[178] The mixture of laws resides in India's Information and Technology Act of 2008, specifically Section 69, and the Information Technology (Intermediate Guidelines) of 2011 (Deibert R. J., 2013). Explicitly in Section 69 of the 2008 Act, the government is empowered to act in the sovereignty, integrity, defence, and security of India, which provides quite expansive legal authorities that the Indian regime appears intent on using extensively (Deibert R. J., 2013).

have a quality all its own (Lipow, 2016). Next, to wrap up this section, the research will offer a few hypotheses about India.

Hypothesis #25 (H25): *Increasingly* conflictual (i.e. negative) *material* interactions reported in Indian media narratives directed at the United States (U.S.) or its interests—yesterday, results in *increased* on cyber intrusion activity, emanating from the India, on US networks—today.

Hypothesis #26 (H26): *Increasingly* conflictual (i.e. negative) *verbal* interactions reported in Indian media narratives directed at the United States (U.S.) or its interests—yesterday, results in *decreased* on cyber intrusion activity, emanating from the India, on US networks—today.

Hypothesis #27 (H27): Increases in the variation of negative narrative tone, indicating an increased level of media polarization, across media stories originating from India, directed at the US and its interests—yesterday, results in *decreased* cyber intrusion activity on U.S. networks—today.

Hypothesis #28 (H28): *Increases* in the conflictual or negative tone of interactions reported in media narratives from India directed at the U.S. and its interests—yesterday, results in *increased* cyber intrusions on U.S. networks—today.

Figure 28. India – Case Study Hypotheses

Nevertheless, India swiftly built a largely defensive cyber infrastructure, restrained and regional in its use. Valeriano, Jensen, and Maness (2018) counted only 7 cyber incidents with India as the antagonist between 2000 and 2014. All of these incidents proceeded through a malicious vector seeking to achieve their primary objective of subversion (~86%) with the remainder focused on an information seeking intent (~14%) (Valeriano, Jensen, & Maness, 2018). India reached their objective in each case but may not have achieved their attempt to coerce their dyadic adversary; however, coercion may not have been their goal. Their goal appears more to push back against regional rivals and to defend their country's public and private enterprises in cyberspace.

First, as the empirical evidence indicated, India should exemplify the impact of *yesterday's* negative media events on *today's* intrusions on U.S. networks, tracking closely with the All-Regimes, autocracies, and anocracies model as posited in H25 and H26 above. Second, NN polarization in the Indian media should produce a dampening effect on today's intrusions, as the population looks to the elites for answers, as conjectured in H27. Third, increases in yesterday's NN tone in Indian media in reference to the U.S. is expected to increase cyber intrusions on U.S. networks today as per H28 above. Again, running opposite to democracies in this aspect. Next, a short review of democracies and the model evidence previously discussed.

C. EVIDENCE OF MEDIA EFFECTS IN CYBERSPACE

A quick review of Chapter Three's finding about democracies seems prudent at this point. First, as with the All-Regimes, autocracies and anocracies models, negative material narratives *yesterday* result in a rise in cyber intrusions on U.S. networks *today*. However, unlike the three previous models, *yesterday's* negative verbal narratives do not produce a subsequent decrease in *today's* intrusions on U.S. networks. The reader can find both results graphically depicted in Figure 10 in Chapter III. Second, NN polarization within democracies seems to track in sign direction consistent with All-Regimes and anocracies, but opposite of autocracies. This finding results from the fact that some democracies may lack confidence in the veracity of their country's media outlets, as discussed in the India section above (Aneez, Neyazi, Kalogeropoulos, & Nielsen, 2018; CIA, 2019).

As previously posited, this could be the result of the sheer cacophony of partisan arguments, opinions, and voices emanating from manifold elite groups reported in democratic media environments (Bjola & Manor, 2018; Conceição-Heldt & Mello, 2017; Putnam, 1988; Strong, 2017; Trumbore, Boyer, Gibson, Harvey, & Wilkenfeld, 2000). As such, the theoretical linkage between the two-step process and level-two, while it may exist for democracies, cannot be as clearly explained here as in the other models. While the democracies model allows for the acceptance of H1, H2, and H5—explanatory nuances beyond these remain as qualitative conjectures.[179]

[179] **Hypothesis #1 (H1):** *Increases* in the number of conflictual *material* interactions reported in the media narratives of other sovereign states directed at the United States (U.S.) and its interests—yesterday, regardless of regime type, results in *increased* cyber intrusion activity on U.S. networks—today.

Hypothesis #2 (H2): *Increases* in the number of conflictual *verbal* interactions reported in the media narratives of democratic states directed at the United States (U.S.) and its interests—yesterday, results in *increased* cyber intrusion activity on U.S. networks—today.

Hypothesis #5 (H5): *Increases* in the variation of negative narrative tone, indicating an increased level of media polarization, across media stories originating from **democratic** and **anocratic** states directed at the U.S. and its interest—yesterday, results in *decreased* cyber intrusion activity on U.S. networks—today.

Third, the first-order interactive variable depicts the relationship between NN tone *yesterday* and, in this case, the democratic countries at varying levels of democracy as shown in Figure 9 of Chapter III. In the evidence sections below, the research will ascribe each country to their given polity score broken out on the z-axis, representing each level of democracy. For example, India represents those democracies scoring 9 on the scale and is but one of the eighteen countries with that score Appendix G contains a complete listing of the eighty-eight democracies considered in this study.

Nevertheless, the graphic provides evidence for rejection of H7, because even though all of the lines for democracies at polity levels of 7, 8, and 9 record decreasing intrusions *today* as *yesterday's* NN tone increases, the line depicting the higher democracy countries does not decrease as rapidly with a higher mean value above that of lower-level democracies. Thus, Figure 9 shows how those +7 countries represented by the red line record a drastic decrease in today's intrusions, dropping –40 per day across the x-axis from right to left. Today's intrusions for those +9 countries captured by the green line score a drop of only –3 per day at that democracy scale, which appears almost flat. The analysis will return to this interesting aspect in the country case studies below.

1. British Evidence

Interestingly, like Iran and Russia both the negative material and verbal narratives record a negative coefficient value. Both are depicted in comparison to the All-democracies model in Figure 30 and Table 8. Very interesting findings indeed, which deserve some exploration and explanation. Rarely, if ever, has a material negotiation within this dyad not resulted in a win-set suitable to both these long-standing allies (Buckley, 2004; Marsh, 2012; Nicholson, 2019; Oliver & Williams, 2016; Reifler, et al., 2014; Stoddart, 2016; Strong, 2017; Tomz & Weeks, 2013; Treharne, 2015). Further, it appears by the negativity of the coefficient and its statistical significance indicates that any negative verbal rhetoric used by the UK toward the U.S. is viewed by its hacker population as posturing by their leadership to achieve some marginal gain in the win-set. Thus, taken together this provides further evidence that these long-standing allies rarely get cross and that the United Kingdom's intrusion community is not mobilized by negative verbal rhetoric unlike other

Democracies as shown in Figure 30. This explanation, coupled with the Third Wave discussion above, the negative coefficients and, the statistical significance, allows for the acceptance of H21 and the rejection of the null.[180]

Next, observe that NN polarization coefficient positively correlates with subsequent intrusions. A finding similar in sign direction to both Turkey and China. Yet, the explanation for this finding tracks closer to Turkey than China, which will be drawn out later.

Now, observe the negative tone interaction coefficient, which is recorded in this analysis manifesting the UK's drop in level of democracy in 2016 from +10 to +8. As discussed earlier, this was precipitated by the UK government's revision of surveillance policy, rising anti-immigrant sentiment resulting in the Brexit referendum, all of which were viewed as symptoms of the deterioration of their liberal democracy. Like Turkey, this provides yet another unique opportunity to analyze this variable at the country-level and the results as hypothesized run similar to Turkey's. Notice in Figure 29, how Britain's polity score of +10, depicted by the dark green dashed line, records a –496 drop in today's intrusions across the x-axis range as a result of the increases in yesterday's NN tone, while the dark red dotted line indicating Britain's decrease in score to +8 clocks an increase of +332 in today's intrusions across the x-axis as a result of yesterday's increase in NN tone. This finding is consistent with the UK discussion above and the conjectured hypothesis, but inconsistent with democracies as a whole.

[180] **Hypothesis #21 (H21):** *Increasingly* conflictual (i.e., negative) *material* and *verbal* interactions reported in British media narratives directed at the United States (U.S.) or its interests—yesterday, results in *decreased* cyber intrusion activity, emanating from the UK, on U.S. networks—today.

Table 8. Results of Negatives Narratives Models for the United Kingdom and India

CYBER INTRUSION ATTEMPTS (Democracy Comparison)				
	Dependent Variable			
	TotalIntrusions – Today			
	Poisson Model			
Yesterday's Independent Variables / Model	All Regimes	All Democracies	**United Kingdom**	**India**
Negative Material Narratives	**0.03*****	**0.03*****	**–0.27*****	**0.22*****
	(0.002)	**(0.004)**	**(0.01)**	**(0.01)**
Negative Verbal Narrative	–0.24***	0.08***	–0.19***	–0.18***
	(0.002)	(0.004)	(0.01)	(0.01)
NN Gold_Mean (Tone)	**–0.003*****	**0.23*****	**–0.63*****	**–0.01****
	(0.001)	**(0.01)**	**(0.06)**	**(0.003)**
NN Gold_SD	–0.01***	–0.03***	0.06***	–0.20***
	(0.001)	(0.001)	(0.004)	(0.003)
Polity	**–0.01*****	**0.77*****	**–0.02**	
	(0.0001)	**(0.02)**	**(0.02)**	
Internet Not Free	0.12***	0.08***		
	(0.003)	(0.005)		
Media Not Free	**–0.21*****	**–0.12*****		
	(0.003)	**(0.003)**		
Media Self-Censorship	0.08***	0.04***		
	(0.003)	(0.003)		
Friday	**0.22*****	**0.29*****	**0.53*****	**–0.91*****
	(0.002)	**(0.003)**	**(0.01)**	**(0.01)**
Saturday	0.12***	0.07***	0.07***	–0.25***
	(0.002)	(0.003)	(0.01)	(0.01)
Sunday	**–0.32*****	**–0.27*****	**–0.31*****	**–0.15*****
	(0.003)	**(0.004)**	**(0.01)**	**(0.01)**
NN Gold_Mean *x* Polity	0.002***	–0.03***	0.07***	
	(0.0001)	(0.001)	(0.01)	
Constant	**–4.49*****	**–5.99*****	**–0.67**	**–11,174.95*****
	(0.03)	**(0.10)**	**(0.65)**	**(337.85)**
Observations	40,608	24,126	288	288
MAE	36.9	22.2	140.2	399.0
RMSE	581.0	202.8	432.0	1,176.5
AIC	2,512,547.6	767,059.7	35,507.4	108,732.1
Log Likelihood	–1,256,240.8	–383,496.8	–17,728.7	–54,342.1
Notes:				*p<0.1; **p<0.05; ***p<0.01

Further, Britain possesses a sophisticated cyber population with a 95% internet penetration rate, and their hacktivists chose to salve their curiosity to find out what they are missing, due to this manifest reduction in freedoms, as the NN tone increases. As their level of cyber sophistication indicates in Appendix J, intruding at the highest level of intrusion risk 68% of the time. As such, this supports the acceptance of H24, showing that increases in NN tone of yesterday's UK narratives about the U.S. results in an increase in today's intrusions, as their polity score decreases.[181]

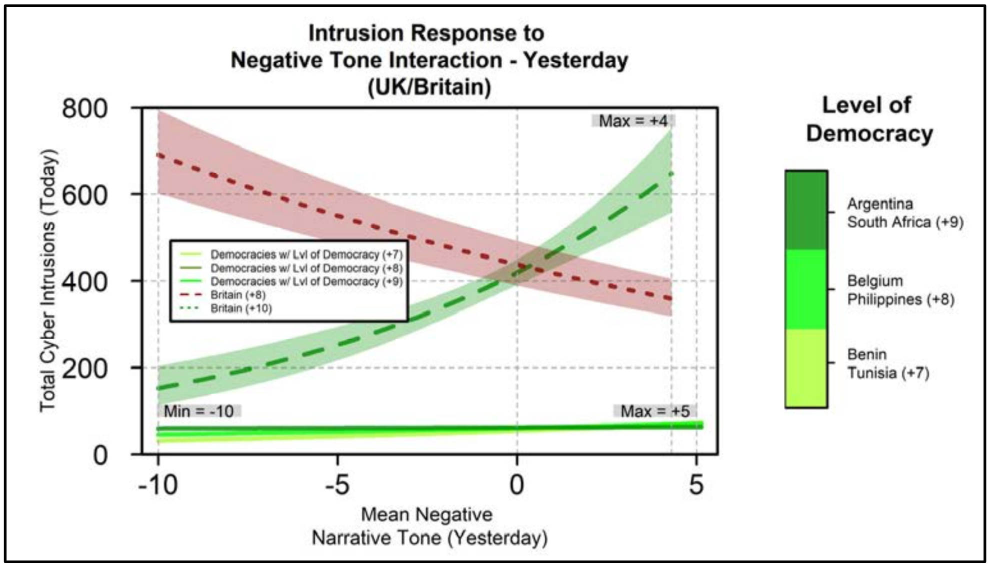
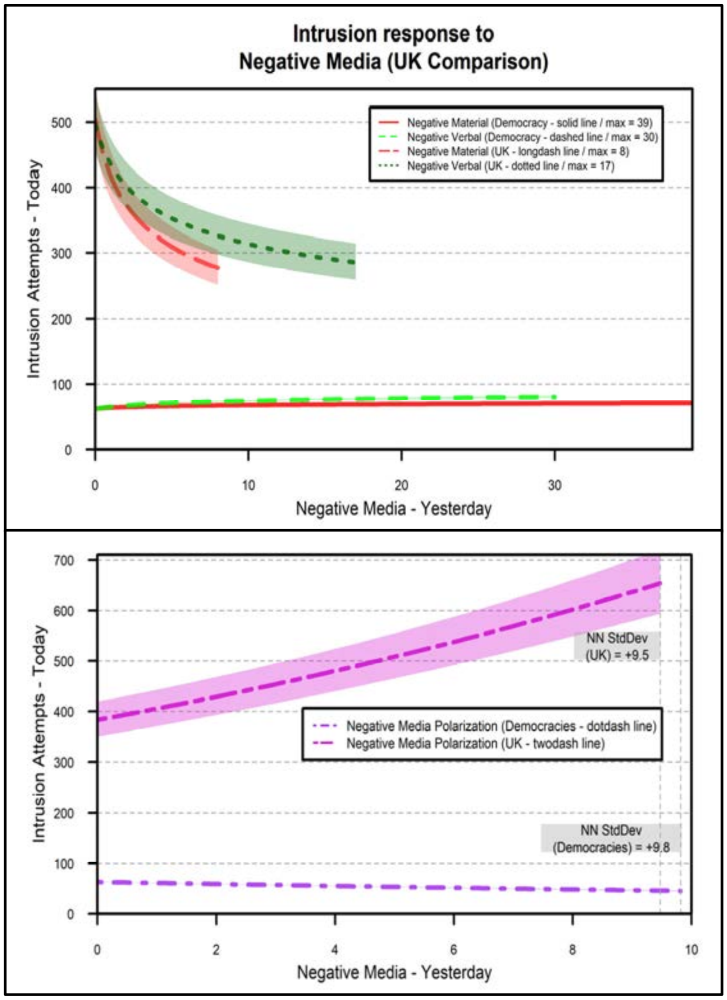


Figure 29. Negative Narrative Tone Results: United Kingdom.

Finally, notice the line depictions of the material and verbal negative daily narrative counts and average marginal effects table in Figure 30. Observe how both lines trends negative as discussed and posited. Both predicted values swing to the negative direction with material scoring a marginal decrease across the x-axis range *125 times* below and verbal recording a marginal drop *twenty-one times* faster than the predicted values for democracies. Perhaps, a real indicator of Briton's belief in their close relationship with the

[181] **Hypothesis #24 (H24):** *Increases* in the accumulated conflictual or negative *tone* of interactions reported in media narratives from the UK directed towards the United States (U.S.) and its interests—yesterday, results in *increased* cyber intrusion activity on U.S. networks—today, with the effect becoming stronger as Britain's level of democracy *decreases*.

U.S. and their disdain for aggression toward other democracies as posited by Tomz and Weeks (2013).



Media Variable Prediction Comparison Table: United Kingdom

Model or Regime Type / Calculated Variable	**Democracies**	**United Kingdom**	**Difference from Democracies**
NmN: **AME on Intrusions** +/- / (SE)	0.2286*** (0.0286)	-28.3537*** (1.3741)	-28.5823*** (1.3744)
NvN: **AME on Intrusions** +/- / (SE)	0.6541*** (0.0328)	-12.8629*** (0.7605)	-13.5170*** (0.7612)
NNp: **AME on Intrusions** +/- / (SE)	-1.8194*** (0.0519)	29.3307*** (2.1118)	31.1501*** (2.1124)

Notes:
Average Marginal Effect (AME)
Negative Material Narrative (NmN)
Negative Verbal Narrative (NvN)
Negative Narrative Polarization (NNp)
Standard Error (SE)

Statistical Significance – p-Level:
***p < 0.01; **p < 0.001; ***p < 0.0001**

Figure 30. Media Results Comparison: United Kingdom.

Next, notice how the magenta line, characterizing the effect of yesterday's NN polarization in the UK media, pitches up scoring a dramatic increase in today's intrusions, *seventeen* times greater than the predicted marginal effect for democracies, as quantified in the table at the bottom of Figure 30.[182] Further, consider the UK's tolerance for NN media polarization tracking in variation range at 3% less than democracies as a group.[183] Perhaps, as discussed in the UK section above this could be an indication of the impact of media reverberation. As, *yesterday's* media stories become more negatively polarized, increases in intrusions occur the following day because the polarization creates cognitive dissonance causing the astute UK hacktivist community to salve their curiosity online. Thus, as each of these coefficients are statistically significance in Table 8 and align with the evidence provided in Figure 30, when viewed together, this provides evidence in support of H21 and H22, allowing for their combined acceptance and rejection of the null.[184] Now to analyze India in the same manner.

2. Indian Evidence

First, notice the negative material and verbal coefficients for India in Table 8. The negative material narratives coefficient tracks in sign value clocking a marginal increase in forecasted intrusions nearly *twenty-seven times* higher than democracies across the x-axis range, as shown in the table at the bottom of Figure 32. Secondly, the negative verbal narratives coefficient in the table tracks opposite in direction scoring a marginal drop in today's forecasted intrusions over the range, *six times* less than the aggregated democracies model. Interestingly, India tracks in negative sign for verbal narrative effects with all the other countries in the study, except China.

[182] Change in average marginal effect on intrusions today resulting from yesterday's NN polarization scores a –1.82 for democracies and a +29.33 for Britain clocking a difference of +31.15 as shown in Figure 30. Consequently, the magnitude of the change between the two is 31.15 / 1.82] = 17.1 ~ 17.

[183] Drawn from the middle frame of Figure 32 [(9.8 – 9.5) / 9.8 = .03 ~ 3%.

[184] **Hypothesis #21 (H21):** *Increasingly* conflictual (i.e., negative) *material* and *verbal* interactions reported in British media narratives directed at the United States (U.S.) or its interests—yesterday, results in *decreased* cyber intrusion activity, emanating from the UK, on U.S. networks—today.

Hypothesis #22 (H22): *Increases* in the variation of negative narrative tone, indicating an increased level of media polarization, across media stories originating from the UK directed at the U.S. and its interest—yesterday, results in *increased* cyber intrusion activity on U.S. networks—today.

Next, notice how yesterday's NN tone variable scores a negative coefficient (–0.01), which equates to an amplifying effect over the NN tone range and comes in at a lower ($p < 0.05$) level of statistical significance. Further, observe how the green dashed line, in Figure 31, for India stands atop the other green lines for the countries captured by the democracies interactive coefficient combining NN tone and level of democracy, rising at a rate *four times* higher than the other democracies with a polity score of +9. One can easily discern how India, as compared to the twenty other countries depicted in the solid dark green line, scores an increase in intrusions *today* as *yesterday's* NN tone about the U.S. increases. This differs in impact and sign value from media sources residing in those countries scoring a +9 level of democracy. Thus, even when considering the lower level of statistical significance for this coefficient, in view of this statistical and graphical evidence, presented in Table 8 and Figure 31 respectively, H27 can be accepted and the null rejected.[185] These findings seem to validate the conclusion made in the Reuters Institute report on India indicating that *90%* of those surveyed accessed news media reports at least *once a day*, which implies, based on the below depicted result, that Indians are quite sensitive to media tone (Aneez, Neyazi, Kalogeropoulos, & Nielsen, 2018). Also, this may provide evidence of the operation of the two-step process within level-two of domestic politics within India.

[185] **Hypothesis #27 (H27):** *Increases* in the conflictual or negative tone of interactions reported in media narratives from India directed at the U.S. and its interested—yesterday, results in *increased* cyber intrusions on U.S. networks—today.

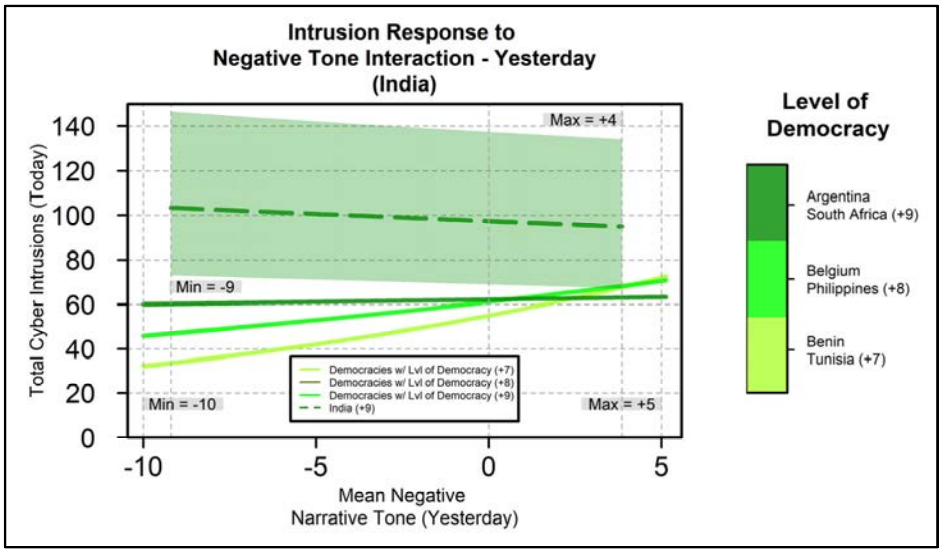
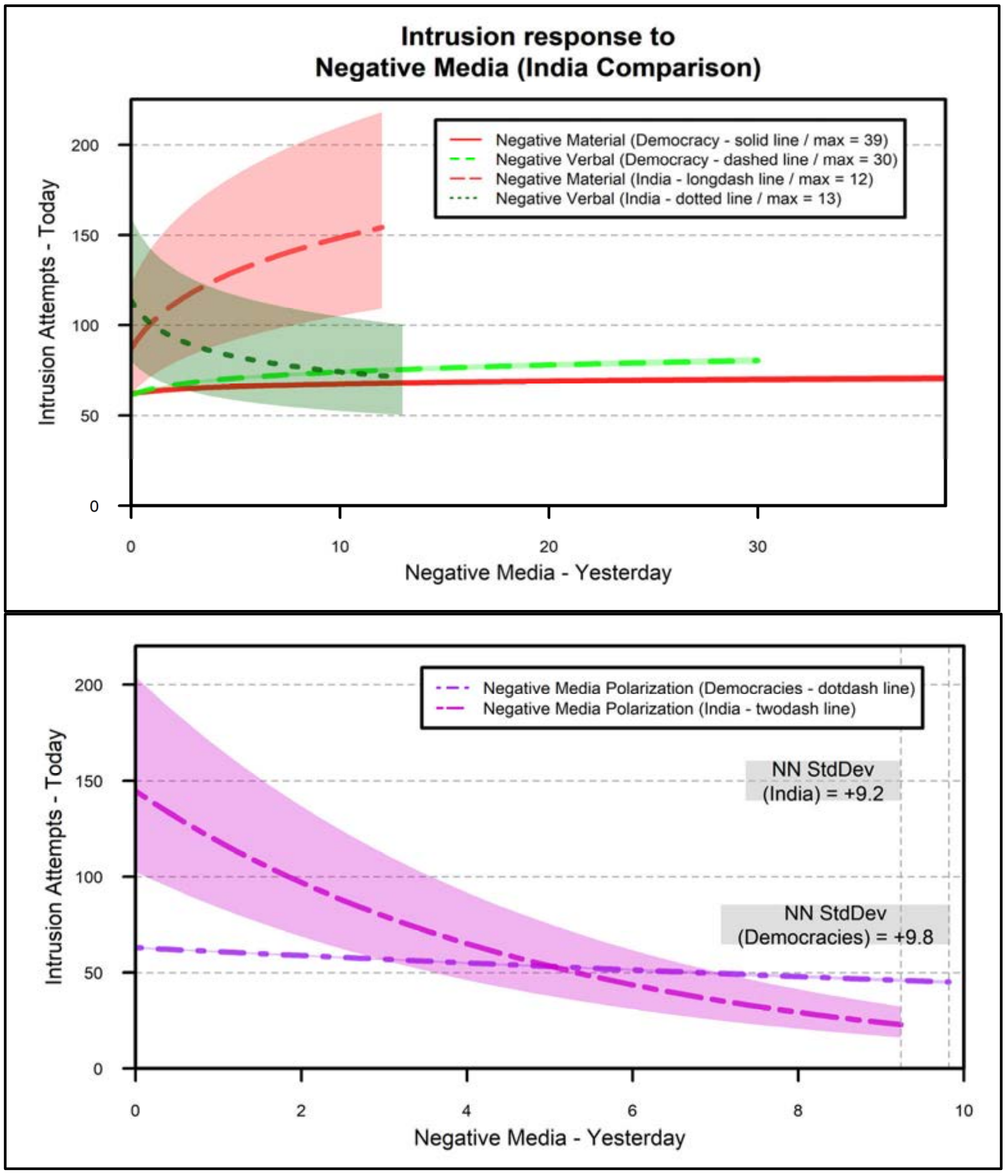


Figure 31. Negative Narrative Tone Results: India.

Now, returning to *yesterday's* negative material and verbal narrative coefficients as show in Figure 32. Notice, how they are both graphically correlated with intrusion's today. Further, by observing their values in Table 8 with NN material and verbal scoring +0.22 and –0.18, respectively, one can see that India tracks precisely in sign with democracies, but at an incremental rate *137 times* higher for material narratives. India's negative verbal marginal effect drops nearly *193 times* faster over the predicted intrusion range, as depicted in the table at the bottom of Figure 32.

Indeed, India, like Turkey for anocracies, seems to epitomize what has been posited in this research that for certain regime types and countries the two-step flow process seems operate within level-two of domestic politics as depicted in the logic map in Appendix C. Thus, while India's leadership is engaged negotiations with the U.S. in level-one of international politics, the labyrinth of India elites signal to the population to give their leadership room to negotiate, which is indicated in the drop of intrusions *today* based on *yesterday's* negative verbal narratives.



Media Variable Prediction Comparison Table: India

Model or Regime Type / Calculated Variable	**Democracies**	**India**	**Difference from Democracies**
NmN: **AME on Intrusions** +/- **/** (SE)	0.2286*** (0.0286)	150.8314*** (5.5767)	150.6028*** (5.5768)
NvN: **AME on Intrusions** +/- **/** (SE)	0.6541*** (0.0328)	-88.8759*** (3.2088)	-89.5300*** (3.2090)
NNp: **AME on Intrusions** +/- **/** (SE)	-1.8194*** (0.0519)	-352.5411*** (4.5320)	-350.7217*** (4.5323)

Notes:
Average Marginal Effect (AME)
Negative Material Narrative (NmN)
Negative Verbal Narrative (NvN)
Negative Narrative Polarization (NNp)
Standard Error (SE)

Statistical Significance – p-Level:
***p < 0.01; **p < 0.001; ***p < 0.0001**

Figure 32. Media Results Comparison: India.

Subsequently, when a tangible result is realized, the elites, either themselves or possibly through social movement affiliations, signal to resume or increase intrusion activity, as indicated by the rise of intrusions resulting from yesterday's negative material narratives. Again, this is not to indicate directionality of these effects. Certainly, material can precede verbal or vice versa. Nevertheless, increases in the number of *yesterday's* negative material and verbal narratives expressed by India about the U.S. results in an increased or decrease in the level of intrusions, respectively, on U.S. networks *today*. Thus, this finding provides the requisite support for the acceptance of H25 and H26, rejecting the null in each case.[186]

Next, observe the NN media variance or polarization coefficient notching the highest negative value (–0.20) which tracks in sign direction with the democracies model, dropping at an average marginal rate *193 times* faster than democracies, as depicted in the table at the bottom of Figure 32. Further, note how India's NN polarization variation range scores only 3% less than democracies as a group.[187] As for India, this appears to showcase their population's tendency to absorb media content from a diversity of sources; yet, tending not to react to the NN polarization of yesterday's narrative. To some this may stand in stark contrast to the effects of NN tone above; however, each variable measures different things. NN tone measures tenor of media stories, while NN polarization gauges the divergence of media narratives, which buttresses the acceptance of H27.[188]

D. CONCLUSION

This chapter began with an overview of democracies and how they view the use of cyberspace—free and open. Surveillance of actions on the internet is governed by legal

[186] **Hypothesis #25 (H25):** *Increasingly* conflictual (i.e., negative) *material* interactions reported in Indian media narratives directed at the United States (U.S.) or its interests—yesterday, results in *increased* on cyber intrusion activity, emanating from the India, on U.S. networks—today.

Hypothesis #26 (H26): *Increasingly* conflictual (i.e., negative) *verbal* interactions reported in Indian media narratives directed at the United States (U.S.) or its interests—yesterday, results in *decreased* on cyber intrusion activity, emanating from the India, on U.S. networks—today.

[187] Drawn from the middle frame of Figure 32 [(9.8 – 9.2) / 9.8 = .06 ~ 6%.

[188] **Hypothesis #27 (H27):** Increases in the variation of negative narrative tone, indicating an increased level of media polarization, across media stories originating from India, directed at the U.S. and its interests—yesterday, results in *decreased* cyber intrusion activity on U.S. networks—today.

frameworks mainly focused on terrorism, the protection of children from exploitation, and the theft of intellectual property or copyrights (Deibert, 2015; Goodman, 2015; MacKinnon, 2012; Morozov, 2011). Certainly, some democracies employ first-generation internet content controls but rarely resort to second-generation controls, mostly in those cases outlined above (Deibert & Rohozinski, 2010; Deibert R. J., 2013). Yet, some democratic policy makers have fallen into the seductive policy heuristic (i.e., thought trap) of outsourcing policing of internet content to third party providers, who, driven by the profit motive may quickly censor the issue du jour, which could lead to censoring of democratic voices on a larger scale (MacKinnon, 2012; Morozov, 2011).

Yet, in this research, Britain stands out as applying the rule of law to their citizens' cyber interactions over outsourcing their responsibilities to police content to private sector ISPs, regardless of their colossal use of CCTV across the country. Their citizens remain confident in the government's just use of their CCTV surveillance methods. Further, the average British citizen appears to exercise an independence of mind different from most other countries on the planet, usually sharply breaking with the aristocratic elites on foreign affairs issues. Most Britons find it immoral to attack other democratic countries, particularly the U.S., with which Britain has enjoyed a manifestly special relationship for over a century.

These findings play out quite nicely in the research conducted here. NN material and verbal stories in *yesterday's* UK press, about the U.S., both result in negative correlation by this set of coefficients on *today's* intrusions. This set of results are uniquely different from democracies. Further, yesterday's NN tone negatively correlates with *today's* intrusions when Britain's scored a +10 in level of democracy, but then shifted to positive correlation when they incurred a drop in polity score to +8. This parallels the findings for Turkey showing how shifts in level of democracy can impact intrusions as the effect of NN tone becomes progressively more negative. Finally, the intrusion risk factor counts, shown in Appendix J, reveal that the British do possess a high level of cyber sophistication, when they choose to exercise it. Thus, providing evidence that high penetration rate democracies possess high end cyber capabilities. Yet, on the international stage Britain remains silent, perhaps relying on their Five Eyes partners to respond on their behalf.

At the other end of the democratic spectrum lies India, which stands out as discretely different, in most respects, from the UK but seems to closely align with democracies in negative material narrative and NN polarization impact on intrusions. Each recording a magnifying or dampening effect, respectively.

Thus, India, whose population dwarfs the UK by comparison, catalogues many of the issues incumbent with having so many citizens. First, creating a unique identification system (i.e., Aadhaar) to account for its vast inhabitants attempting to fix existing welfare corruption issues. Creating an IT system (Aadhaar) that seems to address the main issue, but simultaneously results in the creation of a digital panopticon. This fact in conjunction with their V–Dem (2019) scoring internet and media as not free, and Freedom House (2020) scoring as partially free highlights India's differences and challenges.

Yet, India tracks precisely in direction aligning with democracies for *yesterday's* negative material narratives and NN polarizations influence on *today's* intrusions on U.S. networks. Further, India's NN tone *yesterday* trends negative producing a positive impact on *today's* intrusions. These findings provide evidence of how India's population manifests diverse media consumption habits; yet, their elaborate elite structure, based in the caste system, still holds sway over their reactions to media narratives. This research provides evidence of the operation of the two-step process within level-two of domestic politics within India, as *yesterday's* negative verbal media narratives and NN polarization show dampening effects on *today's* intrusions. The Indian elites signal their population to reduce intrusion activity to provide their leadership with room to negotiate at level-one of international politics or attempt to make sense of the diverse media space *rife* with NN polarization. However, once the result of the level-one negotiations becomes known, elites signal a return to normal or even a heightened level of intrusions as indicated by the effects of negative material narratives and increases in NN tone.

Finally, India appears to lack cyber proficiency, seeking to use low risk intrusion techniques. The values shown in Appendix J indicate this lack of cyber proficiency as India apparently prefers low risk intrusions, choosing quantity over quality. This finding is similar to that of China, where evidence from this research showed that Chinese hackers follow the same methods. This finding sets nicely with India’s minimal involvement in the international aspect of cyberspace, seeking only to push back against its regional rivals.

Therefore, this case study winds to an end with similar discoveries to those made in the previous case study chapters. First, when comparing the individual country to their regime type countries, *culture, political context*, and their *evolutionary setting* matter. Second, unlike the other countries surveyed across this research, democracies appear to manage the domain while simultaneously realizing they *cannot* control it, which allows their civil societies to use it as their populations deem necessary, using generational controls sparingly and only when necessary. Nevertheless, as differences abound, so do parallels and similarities, which were drawn out in this research. Yet, each country, with its own culture and context, arrives at those similarities following, decidedly, very different paths.

THIS PAGE INTENTIONALLY LEFT BLANK

VII. CONCLUSIONS AND RESEARCH RECOMMENDATIONS

A. MEDIA EFFECT IN CYBERSPACE

In this exploration of media effects in cyberspace, the research used discrete country-day counts of the sources of cyber intrusions drawn from a single server on a U.S. network as the dependent variable, with the independent variable drawn primarily from the Phoenix data set, recording the rate of negative media narratives directed by countries toward the United States. The research drew out some interesting differences and similarities between regime types and countries across the breadth and period of analysis.

This chapter will begin by reviewing the conclusions drawn from the variations and parallels across the negative narrative model results. First, this section will analyze the major findings of this research comprising the material and verbal narrative effects on subsequent intrusions on U.S. networks. Second, it will summarize how negative media polarization impacts intrusions on U.S. networks. Third will be the analysis of the multiplicative interaction effects of negative media tone and each country's level of democracy, to include country-level differences and similarities. Finally, the chapter will conclude with recommendations for future research in the media effects and cyberspace arena.

B. CONCLUSIONS: MEDIA EFFECTS IN CYBERSPACE

1. Material and Verbal Negative Narratives

The analysis of the regime-type models for democracies, anocracies, and autocracies drew out some interesting differences and parallels. The first difference surfaced when comparing the types of narratives (i.e., material or verbal) across the regime-type models. Autocracies showed a drop in today's intrusions when compared to an increased number in yesterday's *verbal* negative narratives. The democracies recorded the opposite impact, while anocracies generated *no impact*. This reveals three separate conclusions.

First, autocracies, in general, seem to be able to dampen intrusion activity on U.S. networks, while their leadership is engaged in verbal discourse in level-one negotiations with the U.S. The supposition was that as their country's leadership engaged with the U.S. in level-one dialog, their elites would cue the citizenry at level-two, encouraging them to reduce their intrusions or through the use of generational content controls constrain intrusions on U.S. networks on the following day (Deibert & Rohozinski, 2010; Putnam, 1988). This would indicate that two-step process flow, where elites digest the regime's current narrative and relay its content to the general population, was operating within level-two of domestic politics in autocracies (Lazarsfeld, Berelson, & Gaudet, 1944).

Second, due to this multiplicity of verbal negative narratives in a democracy, the opposite effect occurs. This finding indicates that either two-step flow *does not* operate in democracies within the level-two discussions or there is simply too much media noise generated by the manifold partisan elites within democracies, to produce a discernable signal of the flow's effect within level-two deliberations (Bjola & Manor, 2018; Conceição-Heldt & Mello, 2017; Putnam, 1988; Strong, 2017; Trumbore, Boyer, Gibson, Harvey, & Wilkenfeld, 2000). In contrast, autocracies and anocracies, normally with a single party or group in charge, can and do rheostat the internet and control media messages, thereby cuing their publics to act accordingly.

Thirdly, anocracies score a neutral impact resulting from verbal negative narratives. Coupled with the minimal negative impact of narrative polarization and the moderate growth across the material narrative range, this indicates the strict control anocracies place on their sovereign internet space and media narratives. As pointed out in the model design chapter, anocracies generate a robust coefficient value for media self-censorship with a slope value *ten times* greater than All-Regimes and *thirteen times* greater than democracies, the only other models that estimated a value for this coefficient. These taken together indicate extensive use of generational content controls by anocracies, within their unique digital panopticon structures.

Moreover, yesterday's material negative narratives produce consistently positive effects on succeeding cyber intrusions across the All-Regimes and regime-type models, except for Turkey which produces a positive effect with no statistical significance. Since, Turkey was embroiled in a period of political upheaval and locked in a state of emergency during the period of analysis, this may explain the lack of statistical significance. Yet, the preponderance of these findings supports the conclusions made above.

Anocracies and autocracies each rheostat today's intrusions, either neutralizing or decreasing them as yesterday's level-one verbal negative narratives increase. By allowing subsequent intrusions to increase following the increasing number of yesterday's material negative narratives, this would signify an end to the negotiation and the realization of a negative tangible result. Thus, this negative outcome for the country, as indicated by the negative material narratives, cues the elites to prompt the population to resume or increase today's intrusions on U.S. networks. Secondarily, the regime may ease generational content controls, making it easier for intruders affiliated with either the government or some social movement to ply their tradecraft. Again, this directionality of explanation with verbal proceeding to material is provided here for ease of understanding; certainly, events could happen in the opposite manner.

To further buttress the theoretical evidence of the finding discussed above, democracies track slightly higher and in consistent sign direction with the other two models' material negative narratives. Due to the sheer cacophony of differing media narratives, democratic partisan elites and their audiences cannot discern any unanimity of message. Consequently, democratic hackers manifest very little change in their intrusive practices based on type of narrative (i.e., material vs. verbal).

As the research delved into the country-level case studies, certain differences within regime types and similarities across regime-type boundaries began to surface. Yesterday's material negative narratives effect China and India by tracking quite closely in direction with their corresponding regime-type models. On the other hand, Turkey scores a positive; yet, statistically *insignificant* impact on today's intrusions resulting from yesterday's material negative narratives. This Turkish finding could be a result of the political turmoil discussed above, the fact that Turkey remains an ally of the U.S., the sheer paucity of material observations scoring a maximum of 8 on any given day, or any combination of these explanation could apply.

In contrast, Iran, Russia, and Britain tack opposite in direction to each of their corresponding regime-types. The explanation for Iran and Russia resides in their well-known use of first through third generation content controls coupled with their extensive, manifest use of internet throttling and filtering techniques. To improve the argument, their use of generational controls further demonstrates that the internet residing within their borders is a sovereign domain similar to air, land, sea, and space. Thus, any intrusive actions beyond their sovereign borders in cyberspace could be viewed as state sponsored. As for Britain, this negative coefficient value could be explained by the fact that the U.S. and the UK share a well-documented special relationship and their population's distain for any aggression towards other democracies.

This diversity in trends continues in the effects of verbal negative narratives. Patterns reveal China's ability to subtly rachet down intrusive behavior during verbal jostling with the U.S. at level-one of international politics. Further, the PRC leverages their intergovernmental elite structure coupled with their extensive use of generational content controls. Once the verbal jousting has ended and a tangible result is realized, the PRC uses the same methods to rheostat up their patently intrusive cyber behavior. This finding provides evidence of the operation of the two-step flow within level-two of China's domestic political narrative. Iran and Russia swing consistent with their respective regimes types for the same reasons described above.

Regarding India, Turkey, and the UK, the explanation for the negative coefficient value remains similar because they are all allies of the U.S., even though each has its own discrete culture. As for Britain, the reasoning is similar to the material negative narrative explanation above. India appears to starkly manifest the two-step process operating within level-two of domestic politics as shown by the wide swing from verbal negative narratives resulting in fewer subsequent intrusions, to material negative narratives clocking an increase in ensuing intrusions. These findings point directly to operation of the two-step flow reinforcing the level-two domestic politics narrative for India.

As for Turkey, the explanation is tied to a shift in foreign policy. During this period of analysis, Erdoğan and the AKP steered away from their age-old policy of viewing Turkey as the bridge between the cultures of the east and west to a two-tiered policy. First, regionally Turkey adopted the zero problems with their neighbors policy and secondly, they began to execute a policy of rhythmic diplomacy to maintain their presence internationally (Dedeoglu, 2016; Hussain & Hussain, 2017; Tabansky, 2016). This meant that their NATO allies could no longer rely on Turkey to be a hedge for the west against Chinese or Russian aggression. Further, this positioned Turkey as a more neutral player / partner in the region and internationally. Turkey's shift to a more restrained posture seems to manifest itself in cyberspace with anocracies recording a statistically *insignificant* coefficient close to zero for verbal negative narratives with a marginal effect on today's intrusions *fourteen times* less than the same value of anocracies. Thus, the shift in policy, the rampant political upheaval, the lustration of AKP's ex-domestic allies—the technologically savvy Gülenists—from governmental positions, and the state of emergency all came together positioning the AKP as the reigning elites. AKP elites used this newfound position to buttress their new policy of non-aggression regionally and consistent engagement internationally at level-one by controlling the domestic political narrative at level-two using their now exclusive instrument—the two-step flow.

Finally, to close out the review of negative narrative types, note that Britain stands out as decidedly different from democracies in the effects of both material and verbal negative narratives. The marginal effects of yesterday's material and verbal negative narratives were estimated at *125 times* and *twenty-one times less* than other democracies, respectively. Here the explanation is twofold: the average Briton appears to have a moral aversion to attacking another democracy and the U.S. enjoys a special relationship with Britain both historically and through a multitude of treaties. As such, UK hackers appear disinclined to be mobilized by negative narratives about the U.S., at least in the intrusion realm. Thus, it appears that the special relationship between the U.S. and Britain crosses into the intersection between media events and cyberspace.

2. Negative Narrative Media Polarization

Next the analysis turns to the negative narrative polarization results. As proffered in the hypotheses, democracies and anocracies see a decrease in subsequent intrusions as a result of increases in negative media polarization yesterday. These findings align with the arguments made above for both negative narrative types. Anocracies' tighter control of media messaging and use of generational content controls appears to produce a slight marginal dampening effect, recording a 37% drop below the result seen in the All-Regimes model. Democracies seem to be either reviled or confused by the negative media polarization, resulting in an 87% drop in marginal effects compared to all other regimes.

However, autocracies swing in the opposite direction in response to negative media polarization leading to a *thirty-fold* increase in succeeding intrusions over the predictions of the All-Regimes model. Apparently, autocracies manifest control of the internet and media spaces leaves their technologically savvy hacktivists with little choice other than to indulge in information seeking behavior beyond their borders. Also, this could be the result of a coordinated effort by the regime to rachet up the rhetoric to essentially mobilize their hacktivist population. Either is plausible.

China seems to reflect the latter, leveraging its colossal elite PRC structure to mobilize or demobilize their hacktivists, following similar theoretical mechanisms aligning with the material and verbal explanations above. Iran and Russia oscillate in the opposite direction with the former clocking a *ten-fold* drop and the later scoring *fourteen-fold* drop in marginal effect on today's intrusions resulting from yesterday's media polarization below their respective regime types. Russia follows anocracies in direction; yet, Iran tracks opposite of autocracies with both showing a higher dampening impact on subsequent intrusions. When considering each and the explanations made above concerning material and verbal narratives, this finding appears to further buttress the argument that both countries retain solid control of their internet and media space.

The results for Turkey move in the opposite direction to its regime type, as do the results for Iran and Russia, but for different reasons. Turkey records a *seven-fold* increase in the average marginal impact on intrusions over anocracies resulting from yesterday's NN polarization. Further, Erdoğan and the AKP seems to exercise greater control over their negative media variation, recording a maximum variance 22% less than all anocracies. Nevertheless, this increase in intrusions resulting from increases in media polarization may be emanating from the recently purged, technologically astute Gülenists, or spurned secularists, who are seeking to understand the narrative beyond Turkey's AKP controlled media space. The fact that 93% of the intrusions originating from Turkey come in at the highest intrusion risk level serves to support this argument, as seen in Appendix J.

India aligns with democracies, while Britain runs in the opposite direction. As stated, India's media space is quite diverse with 90% of the population accessing news media reports at least once a day. Thus, their population is firmly engaged in the media space, with manifold diversity, so they simply are not triggered by it and become increasingly disinterested as that polarization increases, showing marginal effects for polarization far smaller than those observed in other democracies.

Britain comes in opposite to both India and democracies, recording an average marginal increase in today's intrusions *seventeen times* higher than that predicted across all democracies. Perhaps this could be a manifestation of the independent-minded Brits who seek to salve the cognitive dissonance created by increasing negative media polarization and indulging in information-seeking behavior. This increase in negative media variability led to a degradation in the UK's liberal democracy due to changes in their surveillance laws, a rise in anti-immigration sentiment, and Brexit, their break with the European Union. These events, occurring over this period of analysis, could have fused together in the minds of independent Brits, leading to a spike in information seeking behavior. Further, evidence of this phenomenon, in regards to Britain, will be provided during the analysis of the first-order interaction between negative narrative tone and level of democracy.

3. Negative Narrative Media Tone and Level of Democracy

The interaction term combining negative narrative tone and level of democracy (i.e., polity score) also records some interesting findings. First, autocracies and democracies saw an increase in the level of intrusions as the level of democracy increased within their discrete regime-types, a finding which ran opposite the conjectured hypothesis. However, the analysis of anocracies bore out where the posited phenomenon occurred, recording findings in-line with hypothetical expectations where decreases in today's intrusions resulted from increases in negative narrative tone as the level of democracy (i.e., polity score) increased. These findings can be reviewed graphically in Appendix H.

Second, Britain and Turkey each provided a unique opportunity to extend this hypothesis and test it at the country-level, because each country experienced a degradation in level of democracy over this period of analysis. The study of each drew out results substantively similar to those predicted for anocracies. Thus, for each country, intrusions on U.S. networks today increased as yesterday's narrative tone became increasingly negative, in combination with the coincidental drop in their level of democracy. All of the other countries showcased in this analysis remained in their distinct level of democracy throughout.

Next, Figures 17 and 19 in the autocracies' case study chapter graphically depict China's and Iran's negative narrative tone effects across the x-axis as compared to the first-order interaction between the two variables for the regime-type. Within these figures, China and Iran are both incorporated in the line scoring –7.[189] As the figures depict, both countries track closely with other autocracies at their level of democracy. Interestingly with this set, it seems that the countries that are more democratic intrude *more*, while those autocrats scoring less than –7 intrude *less*. Perhaps this is a result of these countries having a more rivalrous relationship with U.S. than the more autocratic countries, which includes Bahrain, Qatar, and Saudi Arabia at the extreme –10 polity score.

Whereas India, which is similarly depicted in Figure 31, scores an increase as NN tone becomes increasingly negative at a lower level of statistical significance ($p < 0.05$). Yet, this level of significance rises to a point allowing one to posit that Indians appear to be moderately triggered by increases in NN tone, opposite in direction to NN polarization with a smaller impact. Russia scores a statistically *insignificant* value for this coefficient.

Thus, for autocracies and democracies, regime intrusions may diminish as negative narrative tone increases, but the level of intrusions increases as these countries within each regime-type bin (i.e., –10 to –6 for autocracies) become more democratic. However, for anocracies, the opposite is generally true—more intrusions result today from yesterday's

[189] The other seven include: Azerbaijan, Belarus, Cuba, Eritrea, Kuwait, Laos, and Vietnam (see Appendix G).

negative narrative tone as countries within this bin become less democratic. Certainly, this provides an opportunity for further study.

C. FUTURE RESEARCH OF MEDIA EFFECTS ON CYBER INTRUSIONS

One place to look for evidence of democratic peace in cyberspace might be by applying this model and analysis to other close relationships between democracies. For example, one could analyze Australia, Canada, and New Zealand, as members of the Five Eyes, to discern if they manifest the same type of hacker behavior toward the U.S. This could possibly place a finer point on the broad nature of the theory, which still largely rests mainly on qualitative arguments.

Second, one could proceed by focusing this intrusion research on those states with shifting levels of democracy over a period of analysis to discern if the above findings presented for Turkey and the United Kingdom still hold. Third, by exposing these models to different intrusion data sets, either captured by a different IDS or by an IDS in the private sector, would enhance the reliability and validity of this statistical correlation model in assessing media effects in cyberspace.

Certainly, this dissertation has encountered many twists and turns in the exploration of this phenomenon, unearthing manifold differences and similarities between countries, both across and within regime-types. Ultimately, the outcome of media effects on cyberspace intrusions depends on the given country’s unique culture, political context, and evolutionary setting. Indeed, each country’s behavior, operation, and presence in cyberspace depends on each of these components simultaneously.

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX A. GLOSSARY OF TERMS

The definitions used and created in this research are composed of language that is combined, synthesized, and frequently taken verbatim from the cited source(s). This glossary precisely establishes the terms of reference or terminology in an effort to create general understanding and to standardize the explanations of the amorphous, diverse, ever-changing environment where cyberspace and media events comingle. In doing so, the definitions necessarily draw from established language of expert sources, as cited, to propose recognizable yet directed terminology for the field. When language has been copied verbatim from a source, the page or section number is provided in the citation.

A.

Active measures – describes the employment of an array of operationally covert and overt psychological methods intent on polluting and subverting the opinion-making process of an adversary (Inkster, 2016, pp. 28-29; Metzl, 1974; Snegovaya, 2015, pp. 14-15; Valeriano, Jensen, & Maness, 2018, pp. 114-115)

Activism – a doctrine or practice that emphasizes direct vigorous action especially in support of or opposition to one side of a controversial issue (examples: political *activism or* environmental *activism)* (Webster, 2017, sec. “activism”); to normal, non-disruptive use of the Internet in support of an agenda or cause (Denning, 2001, p. 1).

Activist – a person involved in activism; engaged in activities to include browsing the Web for information, constructing websites and posting materials on them, transmitting electronic publications and letters through e-mail, and using the internet to form coalitions, or to plan and coordinate specific activities (Denning, 2001, p. 1).

Akaike Information Criteria (AIC) is a statistical test approximating the predictive accuracy through the use of out of sample prediction error or deviance

(McElreath, 2016, p. 189). AIC penalizes models that try to overfit the dataset by using too many parameters or explanatory variables.

Anocracy – a form of government that is neither a full democracy nor an autocracy; often times referred to as a mixed democracy or hybrid regime (Marshall & Cole, 2014, p. 21).

Artificial Intelligence (AI) – the theory and development of computer systems able to perform tasks that normally require human intelligence, such as visual perception, speech recognition, decision-making, and translation between languages (Oxford Dictionary, 2015, sec. “artificial intelligence”).

Autocracy – a form of government where citizen participation is severely curtailed, restricted, or suppressed; chief executives are selected according to clearly defined (usually hereditary) rules of succession from within the established political elites; and, once in office, chief executives exercise power over the executive, legislative, and judicial branches of government, most of civil society (Marshall & Cole, 2014, pp. 20-21).

Average Marginal Effect – predicts the marginal change (effect) in a dependent variable, as depicted on a graph’s y-axis, for each per unit change of a given independent variables across the x-axis.

B.

Benign Hacking – hacking motivated by the desire for knowledge (Himma, 2008, p. 200).

Biometric – the measure or analysis of unique physical or behavioral characteristics (i.e., fingerprints, eye scans, voice patterns, keystroke rhythm, etc.) used specifically as a means of verifying personal identity (Webster, 2017, sec. “Biometric”).

Botnet(s) – host of networked computers forced or clandestinely compromised and controlled by a remote user or hacker to perform an array of functions. Botnets constitute free (stolen) computational or network resources leveraged to conduct malicious activity on the internet, such as denial of service, defraud internet advertisers, etc., while masking the identity of the remote operator (Singer & Friedman, 2013, p. 44). Hackers use tailored malware to clandestinely take over and exploit a computer or networks resources for their own purposes (Singer & Friedman, 2013). Hackers use various methods to propagate their customized malware via automated or non-automated means (Shin, Lin, & Guofei, 2011).

Broadband Services – a mass-market retail service by wire or radio that provides the capability to transmit data to and receive data from all or substantially all Internet endpoints, including any capabilities that are incidental to and enable the operation of the communications service, but excluding dial-up Internet access service (Federal Communications Commission, 2020, p. 19741; Jordan S. , 2017, pp. 405-507).

C.

Civil Society – the self-generating and self-supporting communities of people who share a normative order and volunteer to organize political, economic, or cultural activities that are independent from the state or state functions (Diamond, 1994, p.5; Hussain, 2016, p. 7).

Competitive Advantage **–** is the unique ability of a state to utilize its resources effectively, managing to improve its value and position itself ahead of its economic or military rival (Choucri, 2012; Diehl & Goertz, 2001; Porter, 1991; Valeriano, Jensen, & Maness, 2018; Vasquez & Leskiw, 2001)

Computer Worm – stand-alone software, known as Malware that requires no host program to replicate within the information system or execute its intended purpose (Goodman, 2015).

Conflict – is a disagreement on preferred outcomes (Valeriano & Maness, 2015, p. 32).

Cyber – interactions through the use of computers or digital information systems or networks (Committee on National Security Systems, 2015, p. 40; Valeriano & Manness, 2015, p. 22)

Cyber-attack – a cyber-operation, whether offensive or defensive, that is reasonably expected to cause injury or death to persons or damage or destruction to objects (Schmitt, 2013, pp. 91-92).

Cyber conflict – the use of computational technologies in cyberspace for malevolent [or] destructive purposes in order to impact, change, modify diplomatic, economic, [or] military interactions between entities [state or non-state] short of war and non-contiguous to a battlefield (Valeriano & Maness, 2014, pp. 348-351; Valeriano & Maness, 2015, p. 5). Cyber Attacks *occur* within cyber conflicts.

Cyber dispute – specific campaigns between two states using cyber tactics during a particular time-period and contains one to several incidents, often including an initial engagement and responses (Valeriano & Maness, 2014, p. 349). Cyber Attacks *may occur* within cyber disputes.

Cyber domain – see Internet ~ synonymous usage with internet throughout this paper.

Cyber Exploitation – refers to the use of cyber offensive actions-perhaps over an extended period of time-to support the goals and missions of the party conducting the exploitation, usually for the purpose of obtaining information resident on or transiting through an adversary's computer systems or networks (Valeriano & Maness, 2015, pp. 49-50).

Cyber Intrusion – an event or combination of multiple events, that constitutes a cyber-incident in which a hacker or an intruder gains, or attempts to gain, access to information residing on an information system (IT) or networks, without having authorization, in violation of security policies, security procedures, or acceptable use policies (Committee on National Security Systems, 2015, p. 61; Maness & Valeriano, 2016, p. 310; Valeriano & Maness, 2014; Vatis, 2001. pp. 11-12). For example, methods used to remotely accessing a network for the purposes of stealing, gathering, or exfiltrating information.

Cyber Incident – a. an occurrence or set of occurrences that result in an actual or potentially adverse effect on an information system, network, and/or the information residing therein (Committee on National Security Systems, 2015, p. 40). b. an individual action or cyber operation launched against a state, by another state or non-state actor as part of an ongoing cyber dispute or conflict (Valeriano & Maness, 2014, p. 349; Valeriano & Maness, 2015).

Cyberspace – see Internet ~ synonymous usage throughout this paper with internet.

Cyberzone – a sanction electronic space (i.e., state sponsored – intranet), which only can access authorized state provided information (Deibert & Rohozinski, 2010).

D.

Dataveillance – a. surveilling individual behavior through the intensive data trails their digital behavior generates. b. surveilling individuals through computational means and digital information, which has become easier for government entities to trace, an individual or groups behavior, than was possible in the past because of the historical reliance on heavier forms of architectural or institutional surveillance means (Clarke, 1988; Galič, Timan, & Koops, 2017, p. 29).

Dictator's Dilemma – pits the dictator or autocrats desire for control and slow implementation of the internet and associated technologies *against* the fact that any country or state not connected to the internet will fall behind economically and technologically – both of which pose threats to the longevity of an authoritarian regime *(*Al Jazeera, 2018; Shirky, 2011; Morozov, 2011*)*.

Digital Bonapartism – essentially a populist demagogue, who uses democratic oratory and symbolism to legitimize their rule and political leadership through the manipulation of public opinion by controlling digital media, networks, or platforms (MacKinnon, 2012, pp. 66–67).

Digital Panopticon – an internet enabled, digital version of a structural design and theoretical concept that allows a single individual to monitor an entire institution without the observed subject's awareness of their observation. This presumes that if individuals – such as prisoners, students, workers, or citizens – understand that they may be under observation at any time; these individuals will act as though they are under examination; thus, they will self-police (Foucault, 1977, p.216; Loadenthal, 2018 pp.1-3; Manokha, 2018, pp.219-237; Pinkaew, 2016, pp. 195-214).

Direct action – any action that achieves its desired goal (i.e., civil disorder, civil strife, civil disorder, civil violence, or any state sponsor variations thereof) and spans from cyber to kinetic measures (Deibert & Rohozinski, 2010; Deibert, 2015; King M. L., 1963; Keck & Sikkink, 1998; MacKinnon, 2012; McAdams, McCarthy, & Zald, 1999)

Distributed Denial of Service (DDOS) – an attack in which multiple compromised computer systems attack a target, such as a server, website or other network resource, and cause a denial of service for users of the targeted resource. The flood of incoming messages, connection requests or malformed packets to the target system forces it to slow down or even crash and shut down, thereby denying service to legitimate users or systems (Beaver, 2018, sec."DDOS").

Doxing – revealing personal documents publicly, as part of a protest, prank, or vigilante action. Often doxing requires minimal network penetration, relying more on careful research to link hidden personal or embarrassing data to the victim (Singer & Friedman, 2013, p. 46).

Dyad – an interaction between two elements or parts, in this case two states or countries (Oxford Dictionary, 2015, sec. "dyad").

E.

Elite – individuals and small, cohesive groups who wield a disproportionate level of power or influence affecting national and supranational political outcomes in a substantial way on a continuing basis (Best & Higley, 2018, p. 3; Higley & Burton, 2006, p. 14). Throughout this text, elite is synonymous with opinion or proximate leader.

Emergence – a classic systems principle indicating the effectiveness of a Systems of Systems; patterns and properties in a complex system come about (emerge) as the system operates; these patterns and properties cannot be anticipated beforehand or derived from an understanding of system elements or their individual properties (Johnson IV, Tolk, & Sousa-Poza, 2013, p. 284; Keating, 2009, p. 209).

Explain – see Explanatory inference below.

Explanatory inference – to derive and compare hypotheses about the hidden frameworks that may be responsible for the data (i.e., cyber-intrusions), then use an epistemic branch of science, in this case statistical correlation, to test the strength of the hypothesized relationships between the dependent variable and independent or *explanatory* variables (Godfrey-Smith, 2003, pp. 190-201).

F.

Fourth Estate – the idealized role of journalism is that it serves as a "watchdog," keeping government honest and watching out for the interests of people (Kovach & Rosenstiel, 2001, pp. 50-53).

Framing – a. *in the media narrative (effects) context* is defined as deliberate efforts by groups of media professionals (i.e., reporters, journalists, editors, etc.) to mediate a shared understanding of world events by creating a narrative that resonates, and possibly influences, the audience's schemata of an event either experienced or re-counted by a given actor (i.e., politicians, lobbyists, advocates, experts, moral entrepreneurs, intellectuals, elites, witnesses) (Ball-RoKeach & DeFleur, 1976; Benford & Snow, 2000; Carroll & Hackett, 2006; Habermas, 2006; McAdams, McCarthy, & Zald, 1999; Neuman & Guggenheim, 2011; Scheufele & Tewksbury, 2007; Werder, 2009).

Freeware – (a.k.a. Public Domain Software) software not protected by copyright laws of any nation that may be freely used without permission of or payment to the creator, and that carries no warranties from or liabilities to the creator (Committee on National Security Systems, 2015, p. 99).

G.

H.

Hack – a. to gain unauthorized access to computers or to computerized, information systems or networks, (Floridi, 2008, p. 8; Himma, 2008, pp. 191-192; Webster, 2017, sec. “hack”); b. related form – Hacker, noun; c. related form – Hacking, transitive verb.

Hacker – an expert at programming and solving problems with a computer; a person who gains unauthorized access to and sometimes tampers with information in computers, information systems or networks (Committee on National Security Systems, 2015, p. 56; Floridi, 2008, pp. 3-24; Himma, 2008, pp. 191-192; Webster, 2017, sec. “hacker”).

Hacking – refers to acts in which a person or groups of people gain unauthorized access to computers, information systems or networks (Floridi, 2008, p. 8; Himma, 2008, pp. 191-192; Webster, 2017, sec. “hacking”).

Hacktions – actions conducted within an information system (i.e., computer, server, computer network, or through the internet) by a hacker (Samuel, 2004b, pp. 129–130).

Hacktivism – a. refers to the marriage of hacking and activism. It covers operations that use hacking techniques against a targets Internet site with the intent of disrupting normal operations but not causing serious damage. Examples are Web sit-ins and virtual blockades, automated e-mail bombs, Web hacks, computer break-ins, and computer viruses and worms (Denning, 2001a, pp. 70-75); b. the commission of an unauthorized digital intrusion for the purpose of expressing a political or moral position (Himma, 2008, pp. 200-201); c. the (sometimes) clandestine use of computer hacking to help advance political causes (Manion & Goodrum, 2000; pp. 14-19); d. the nonviolent use of illegal or legally ambiguous digital tools in pursuit of political ends, combining the transgressive civil disobedience with the technology and techniques of computer hackers (Samuel, 2004a, p. 2); e. related form Hacktivist, noun or adjective.

Halal – in Arabic means lawful, referring to any object or act considered as permissible under Islamic law (MacKinnon, 2012, p. 55).

I.

Indexing – the way in which journalists write their narratives (i.e., stories) by reporting the voices or viewpoints of prominent officials who because of their position of influence may affect the outcome of the situation (Bennett, 1990; Strong, 2017). Journalist perform the function of indexing to ensure they adhere to professional standards of balanced, fair, and objective reporting, which is reinforced by normative editorial standards (Bennett, 1990; Strong, 2017).

Information Seeking Intent – the active and intentional actions in cyberspace, set upon executing acts of cyber espionage (i.e., intelligence, surveillance, reconnaissance) to exfiltrate or gather information specifically from or out of a target's IT networks (Case & Given, 2016; Clarke & Knake, 2010; Denning, 2011; Gandhi et al., 2011; Gartzke & Lindsay, 2015; Kello, 2013; Samuel, 2004a).

Information System (IS) – a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information (Committee on National Security Systems, 2015, p. 65).

Information Technology (IT) – includes all categories of ubiquitous technology used for the gathering, storing, transmitting, retrieving, or processing of information (e.g., microelectronics, printed circuit boards, computing systems, software, signal processors, mobile telephony, satellite communications, and networks). Synonymous with Information and Communications Technology (ICT) (Committee on National Security Systems, 2015, p. 67).

Instruments of National Power – Diplomacy, Information, Military, and Economic (DIME) (Farlin, 2014, pp. 9-38; Mattis, 2018, p. 4)

Internet Protocol (IP) – standard protocol for transmission of data from source to destinations in packet-switched communications networks and interconnected systems of such networks (Committee on National Security Systems, 2015, p. 70).

Internet – the single, interconnected, worldwide system of commercial, governmental, educational, and other computer or digital information systems or networks that share (a) the protocol suite specified by the Internet Architecture Board (IAB) and (b) the name and address spaces managed by the Internet Corporation for Assigned Names and Numbers (ICANN) (Committee on National Security Systems, 2015, p. 70; Valeriano & Maness, 2015, pp. 9-17). Used throughout this paper as synonymous with the World Wide Web (WWW), cyberspace, or cyber domain.

Internet Service Provider (ISP) – an organization that provides access to the Internet, as well as other services such as web hosting or e-mail. It is a primary control point, since all traffic from an individual or organization flows through its ISP (Singer & Friedman, 2013, p. 47). Synonymous with Internet Provider in this paper.

Intrusion Detection System (IDS): Software that automates the process of monitoring the events occurring in a computer system or network and analyzing them for signs of possible incidents and attempting to stop detected possible incidents (Cichonski, Millar, Grance, & Scarfone, 2012, p.60).

J.

K.

L.

Liberalism – an analytical approach to international relations where states are part of a global society that modulates their interactions based on norms and rules established through interaction, initially through transnational and more recently international trade (Nye, 2007, p. 288). National borders signify moral importance because states represent the collective ideals and rights of the peoples inhabiting them; thus, it follows that respect for the sovereignty and territorial integrity of a given state shows respect for the rights of its citizens (Nye, 2007, pp. 23–24; Walzer, 1977; Walzer, 1980).

M.

Malicious Vector – an intrusion, infiltration, or exploitation of IT systems to steal intellectual property, a person's identity, or execute a *cybercrime* comprise the lattice of cyber actions and goals form its' the boundaries (Choo, 2011; Goodman, 2015; Sharp, 2017; Valeriano & Maness, 2015). These observable actions seem intent on causing financial, psychological, or reputational harm to the target (i.e., individual or government).

Malware –software or firmware intended to perform an unauthorized process that will have adverse impact on the confidentiality, integrity, or availability of an information system. A virus, worm, Trojan horse, or other code-based entity that infects a host. Spyware and some forms of adware are also examples of malicious code, hardware, firmware, or software that is intentionally included or inserted in a system for a harmful purpose (Cichonski, Millar, Grance, & Scarfone, 2012, p. 60; Committee on National Security Systems, 2015, p. 79). Also see *computer worm.*

Material Conflictual (Negative) – physical acts of a conflictual nature, including armed attacks, destruction of property, assassination, embargos, naval blockades, etc. (Schrodt, 2017, p.20).

Material Cooperative (Positive) – physical acts of collaboration or assistance, including receiving or sending aid, reduce bans, reduce sanctions, etc. (Schrodt, 2017p. 20).

Mean Absolute Error (MAE) – is the measure of the average absolute difference between the actual and model calculated residuals over a given time series (Levine, Berenson, & Stephan, 1998, pp. 690-693).

Media-Effects Theory – a. the deliberate and non-deliberate short and long-term within-person changes in cognitions (including beliefs), emotions, attitudes, and behavior that result from media use (Valkenburg, Peter, & Walther, 2016, p. 316). b. Elements of media effects include timing (immediate vs. long-term), duration (temporary vs. permanent), valence (negative or positive), change (difference vs. no difference), intention (or non-intentional), level of effect (macro vs. micro), direct (or indirect), and manifestation (observable vs. latent) (Potter, 2012, pp. 35-36).

N.

Narrative Theory – the institutionalized use of semiotic structures or codes to allow narrators (i.e., authors) and readers to communicate through texts; thereby, allowing the reader to understand and make sense of a given situation described in the story (Barbatsis, 2004; Kearns, 2005). b. information that actively engages the senses using language to create structure that draws in the reader or listener, intentionally, leaving out pieces of information, or the other side of the story, in an effort to engage the reader or listener by inviting them to us their imagination to fill in the missing information and discern what really happened (Wake, 2009, p. 674).

Neo-Liberalism – similar to liberalism except that state actions are constrained by economic interdependence and international institutions (Nye, 2007, p. 288).

Netizen – citizen of the internet (Diamond, 2010; Lindsay, 2014).

Network(s) – Information system(s) implemented with a collection of interconnected components. Such components may include routers, hubs, cabling, telecommunications controllers, key distribution centers, and technical control devices (Committee on National Security Systems, 2015, p. 86).

O.

Opinion Leader – see Elite.

P.

Performative Hacktivist – refers to the use of cyber offensive actions—perhaps over an extended period of time (Samuel, 2004a, pp.129–130).

Polity – the design or constitution of a politically formed state or country; in this context it means to describe the form of governing institutions spanning from Democracies, to mixed governments such as Anocracies, through to totalitarian regimes or Autocracies (Polity IV, 2018; Webster, 2017, sec. "polity")

Polyvocality – means there is *no* objective truth, *no* single official version of a story, *no* preferred interpretation or reading of the events, rather, the story is derived from many voices and multiple differing points of view from which the single narrative is created (Wake, 2009, pp. 673-677).

Q.

R.

Reflexive Control – explains the use of tailored information (i.e., media narratives) that would influence an opponent or rival to voluntarily make the pre-determined decision created, framed, and preferred by the preparer or originator (a.k.a., opposing state in a conflictual dyad) (Thomas, 2004, pp. 237-238; Valeriano, Jensen, & Maness, 2018, pp. 113-114).. While similar to perception management, reflexive control focuses on *control* of the subject – in this case public opinion of a state or the civil society within a target country (Thomas, 2004, p. 237).

Reverberation – how statements and actions of foreign actors (i.e., elites) reported by media sources can affect the domestic politics of another state, thereby, influencing the foreign policy decisions of that state (Putnam,1988, pp. 454–456; Strong, 2017, pp. 293–294).

Root Mean Square Error (RMSE) – is the square root of the model’s variance residuals or the difference between the observed values of the data collected and the model’s predicted values. It provides an indication of how well the model predicts the response. The lower the RMSE the better the explanatory variables predict the response variable (Ludecke, 2019, p. 19).

Router – a device that mediates the transmission routes of data packets over an electronic communications network (i.e., the Internet) (Webster, 2017, sec. “router”).

Rivalry – is a relationship between two states whereby through a series of connected disputes both sides use, with some regularity, their instruments of national power (i.e., diplomatic, informational, military, or economic (DIME)) to telegraph threats, to employ coercion or intimidation tactics in order to gain some competitive advantage over the other (Chairman of the Joint Chiefs of Staff, 2016; Diehl & Goertz, 2001; Farlin, 2014; Porter, 1991; Valeriano, Jensen, & Maness, 2018; Vasquez & Leskiw, 2001). Rivalries take on psychological manifestations of their enmity towards each other, which include suspicion, mistrust, hatred, and demonization (Maoz & Mor, 2002). This psychosis seems to permeate all level of civil societies (i.e., masses to elites) engaged in a rivalrous behavior (Maoz & Mor, 2002). Further, opponents view accommodations, made by the other, in actions, deeds, or statements with bias suspicion, whereas, hostility consistently defines the true essence of a rival’s intentions or attitudes (Jervis, 1976; Heradstveit, 1979; Maoz, 1990; Maoz & Mor, 2002).

S.

Server – a computer in a network that provides services (such as access to files or shared peripherals or the routing of e-mail) to other computers in the network (Webster, 2017, sec. “server”).

Social Control – the rules and standards of society that circumscribe individual action through the inculcation of conventional sanctions and the imposition of formalized mechanisms (Webster, 2017, sec. “social control”). Used in and throughout this text as synonymous with Societal Control.

Social Media – forms of electronic communication (such as websites for social networking and microblogging) through which users create online communities to share information, ideas, personal messages, and other content (such as videos) (Webster, 2017, sec. “social media”).

Semantic substrate – a substratum of the synthetic layer that contains the information and knowledge created, manipulated, and utilized by humans in our day-to-day life. Access to this substrate comes through the physical through the syntactic. Information that is exfiltrated, manipulated, or stolen resides in the semantic substrate (Libicki, 2007, pp.8-10; Valeriano & Maness, 2015, pp. 22-24).

Subversive Intent – the desire to undermine the constitution, the integrity, or the authority embodied in a rival’s ability to exercise control over their established institutions or entities defines *subversive intent (Rid, 2012, p. 22; Valeriano & Maness, 2015, pp. 33-37).*

Surveillance – a. to watch from above; to keep a close watch over someone, b. ‘sur’ to watch from above, ‘veillance’ from above (Galič, Timan, & Koops, 2017; Webster, 2017, sec. “surveillance”).

Syntactic substrate – a substratum of the synthetic layer that contains the computer language, instructions, and syntax, which enables the internet to function. The physical layer, of cyberspace, enables access to the semantic substrate, through the syntactic substrate where the hacking occurs to gain access to the information in the semantic (Libicki, 2007, pp. 8-10; Valeriano & Maness, 2015, pp. 22-24).

System of Systems (SOS) – a super system or meta system comprised of elements which themselves are independent systems, and interact among themselves to achieve, either wittingly or unwittingly, a common goal (Johnson IV, Tolk, & Sousa-Poza, 2013, p. 284). Emergence of patterns/properties in a complex system will come about (emerge) through operation of the system (Keating, 2009, p. 170).

T.

The First Wave – Agrarian Age; the age of the three estates, 1st Estate or the Clergy, 2d Estate or the Nobility, 3d Estate or the Serfs, Peasants, or Commoner. Society revolved around the cultivation of arable land and the security of it. Information circulated by word of mouth orally from person to person. Hence, conflict generally revolved around the protection or acquisition of land or territory (Connolly, 1979; De Tocqueville, 1955; Toffler, 1980; Toffler & Toffler, 1993). Agrarian Age spanned from 8000 – 9000 BC or BCE (Saharan Africans begin to farm and raise cattle for subsistence) to 1770s (Toffler, 1980).

The Second Wave – Industrial Age (i.e., Revolution), the age of mechanization of textiles, transportation, communications, warfare, etc., which created the requisite mass production, mass merchandising, and mass distribution of goods and services (Toffler, 1980; Toffler & Toffler, 1993). Society became dependent on industrial production and the security of materials and means of production. Information passed via word of mouth, written word via print media, or use of telegraph, telephone, and/or radio to transmit information. Agriculture still necessary to sustain the population became increasingly industrialized and more efficient (i.e., Eli Whitney’s Cotton Gin). Conflict between the industrial and agrarian age societies culminated in the U.S. Civil War (1861–1864), with the industrial society firmly supplanting the agrarian (Toffler, 1980). The Industrial Age spanned from approximately 1800 to 1960.

The Third Wave – Third Wave – Information Revolution (current age), the age of digitization and computerization of information through use of interconnected networks spanning the globe (i.e., the internet, World Wide Web, Cyberspace), enabling the nearly instantaneous transfer of information and knowledge, leading to the demassification of society (Nye, 2014; Toffler, 1980; Toffler & Toffler, 1993). Social and political power resides with those creating, innovating, controlling, managing, harnessing information to improve or innovate the use of existing legacy or newly developed systems (Nye, 2014; Toffler, 1980; Toffler & Toffler, 1993). By using information, agriculture and industrial products have become commodities (Toffler, 1980; Toffler & Toffler, 1993). The Information Revolution began in the 1960s and continues in the present era.

Tone – a construct meant to apply a objective scale (i.e., +10 to –10) to media narratives from cooperative (i.e., positive, +10) to conflictual (i.e., negative, –10) (Bi, 2015; Brandt, Colaresi, & Freeman, 2008; Colaresi, 2004; Goldstein, 1992; Goldstein & Pevehouse, 1997; Schrodt & Gerner, 1997; Shellman, Clare Hatfield, & Mills, 2010; Yonamine, 2001).

Throttling – adjusting the amount of bandwidth to or from a server. The term is often associated with Internet Service Providers (ISP)s that limit the speed to users based on the volume or type of traffic being transmitted (PC Mag Digital Group, 2020, sec. “throttling”).

U.

V.

Verbal Conflictual (Negative) **–** a spoken criticism, threat, or accusation, innately rhetorical and often related to past or future potential acts of conflict (Schrodt, 2017, p. 20).

Verbal Cooperative (Positive) – narratives describing dialog-based meeting, such as negotiations or peace talks or statements that express a desire to cooperate or appeal for assistance (other than material aid) for other states (Schrodt, 2017, p. 20).

Virtual Private Network (VPN) – protected information system link utilizing tunneling, security controls, and endpoint address translation giving the impression of a dedicated line (Committee on National Security Systems, 2015, p. 131).

W.

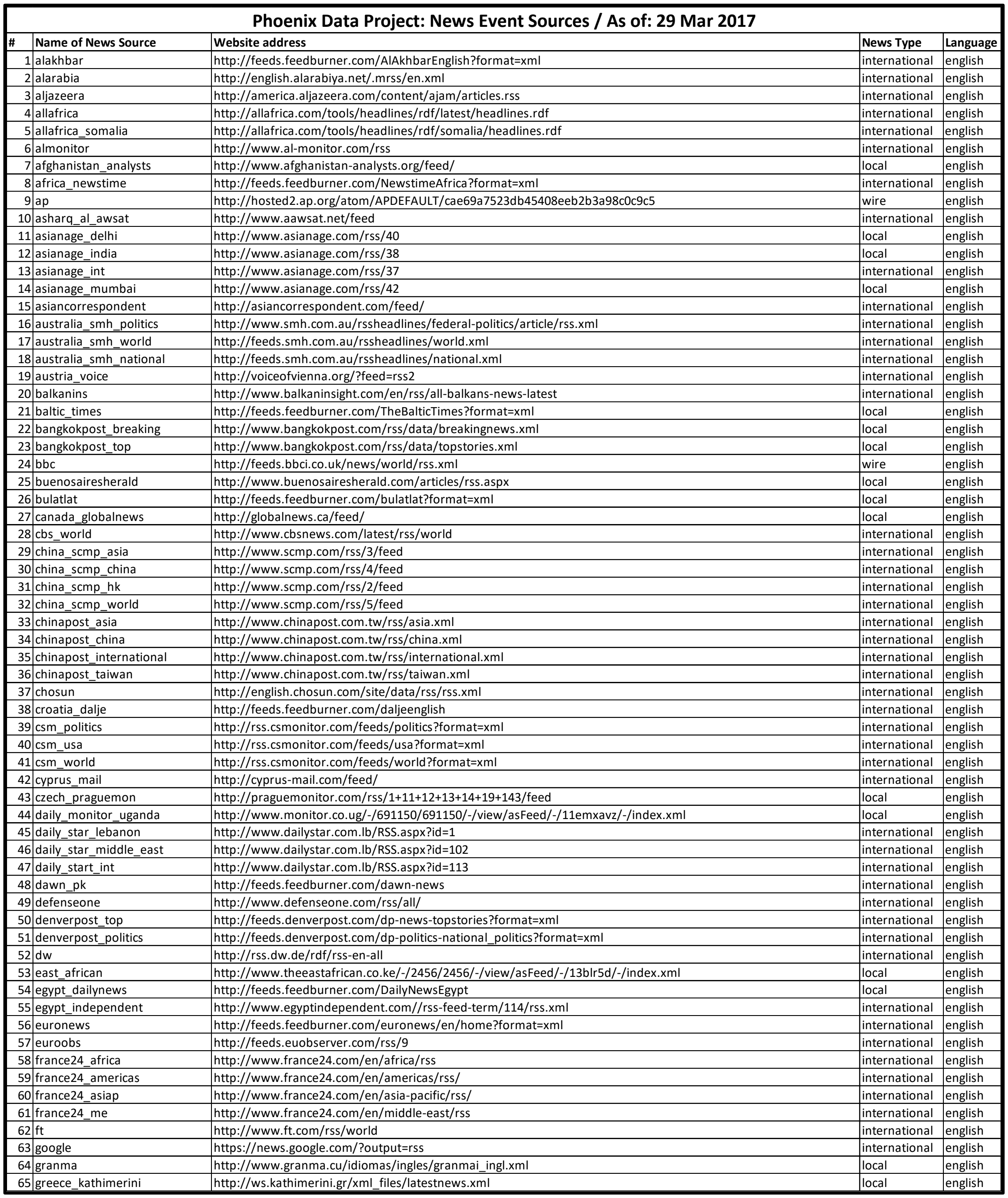
World Wide Web (WWW) – see internet ~ synonymous usage throughout this paper with cyberspace and the internet.

Y.

Z.

APPENDIX B. SOURCES OF NEWS MEDIA EVENTS

1 of 6



Phoenix Data Project: News Event Sources / As of: 29 Mar 2017

#	Name of News Source	Website address	News Type	Language
1	alakhbar	http://feeds.feedburner.com/AlAkhbarEnglish?format=xml	international	english
2	alarabia	http://english.alarabiya.net/.mrss/en.xml	international	english
3	aljazeera	http://america.aljazeera.com/content/ajam/articles.rss	international	english
4	allafrica	http://allafrica.com/tools/headlines/rdf/latest/headlines.rdf	international	english
5	allafrica_somalia	http://allafrica.com/tools/headlines/rdf/somalia/headlines.rdf	international	english
6	almonitor	http://www.al-monitor.com/rss	international	english
7	afghanistan_analysts	http://www.afghanistan-analysts.org/feed/	local	english
8	africa_newstime	http://feeds.feedburner.com/NewstimeAfrica?format=xml	international	english
9	ap	http://hosted2.ap.org/atom/APDEFAULT/cae69a7523db45408eeb2b3a98c0c9c5	wire	english
10	asharq_al_awsat	http://www.aawsat.net/feed	international	english
11	asianage_delhi	http://www.asianage.com/rss/40	local	english
12	asianage_india	http://www.asianage.com/rss/38	local	english
13	asianage_int	http://www.asianage.com/rss/37	international	english
14	asianage_mumbai	http://www.asianage.com/rss/42	local	english
15	asiancorrespondent	http://asiancorrespondent.com/feed/	international	english
16	australia_smh_politics	http://www.smh.com.au/rssheadlines/federal-politics/article/rss.xml	international	english
17	australia_smh_world	http://feeds.smh.com.au/rssheadlines/world.xml	international	english
18	australia_smh_national	http://feeds.smh.com.au/rssheadlines/national.xml	international	english
19	austria_voice	http://voiceofvienna.org/?feed=rss2	international	english
20	balkanins	http://www.balkaninsight.com/en/rss/all-balkans-news-latest	international	english
21	baltic_times	http://feeds.feedburner.com/TheBalticTimes?format=xml	local	english
22	bangkokpost_breaking	http://www.bangkokpost.com/rss/data/breakingnews.xml	local	english
23	bangkokpost_top	http://www.bangkokpost.com/rss/data/topstories.xml	local	english
24	bbc	http://feeds.bbci.co.uk/news/world/rss.xml	wire	english
25	buenosairesherald	http://www.buenosairesherald.com/articles/rss.aspx	local	english
26	bulatlat	http://feeds.feedburner.com/bulatlat?format=xml	local	english
27	canada_globalnews	http://globalnews.ca/feed/	local	english
28	cbs_world	http://www.cbsnews.com/latest/rss/world	international	english
29	china_scmp_asia	http://www.scmp.com/rss/3/feed	international	english
30	china_scmp_china	http://www.scmp.com/rss/4/feed	international	english
31	china_scmp_hk	http://www.scmp.com/rss/2/feed	international	english
32	china_scmp_world	http://www.scmp.com/rss/5/feed	international	english
33	chinapost_asia	http://www.chinapost.com.tw/rss/asia.xml	international	english
34	chinapost_china	http://www.chinapost.com.tw/rss/china.xml	international	english
35	chinapost_international	http://www.chinapost.com.tw/rss/international.xml	international	english
36	chinapost_taiwan	http://www.chinapost.com.tw/rss/taiwan.xml	international	english
37	chosun	http://english.chosun.com/site/data/rss/rss.xml	international	english
38	croatia_dalje	http://feeds.feedburner.com/daljeenglish	international	english
39	csm_politics	http://rss.csmonitor.com/feeds/politics?format=xml	international	english
40	csm_usa	http://rss.csmonitor.com/feeds/usa?format=xml	international	english
41	csm_world	http://rss.csmonitor.com/feeds/world?format=xml	international	english
42	cyprus_mail	http://cyprus-mail.com/feed/	international	english
43	czech_praguemon	http://praguemonitor.com/rss/1+11+12+13+14+19+143/feed	local	english
44	daily_monitor_uganda	http://www.monitor.co.ug/-/691150/691150/-/view/asFeed/-/11emxavz/-/index.xml	local	english
45	daily_star_lebanon	http://www.dailystar.com.lb/RSS.aspx?id=1	international	english
46	daily_star_middle_east	http://www.dailystar.com.lb/RSS.aspx?id=102	international	english
47	daily_start_int	http://www.dailystar.com.lb/RSS.aspx?id=113	international	english
48	dawn_pk	http://feeds.feedburner.com/dawn-news	international	english
49	defenseone	http://www.defenseone.com/rss/all/	international	english
50	denverpost_top	http://feeds.denverpost.com/dp-news-topstories?format=xml	international	english
51	denverpost_politics	http://feeds.denverpost.com/dp-politics-national_politics?format=xml	international	english
52	dw	http://rss.dw.de/rdf/rss-en-all	international	english
53	east_african	http://www.theeastafrican.co.ke/-/2456/2456/-/view/asFeed/-/13blr5d/-/index.xml	local	english
54	egypt_dailynews	http://feeds.feedburner.com/DailyNewsEgypt	local	english
55	egypt_independent	http://www.egyptindependent.com//rss-feed-term/114/rss.xml	international	english
56	euronews	http://feeds.feedburner.com/euronews/en/home?format=xml	international	english
57	euroobs	http://feeds.euobserver.com/rss/9	international	english
58	france24_africa	http://www.france24.com/en/africa/rss	international	english
59	france24_americas	http://www.france24.com/en/americas/rss/	international	english
60	france24_asiap	http://www.france24.com/en/asia-pacific/rss/	international	english
61	france24_me	http://www.france24.com/en/middle-east/rss	international	english
62	ft	http://www.ft.com/rss/world	international	english
63	google	https://news.google.com/?output=rss	international	english
64	granma	http://www.granma.cu/idiomas/ingles/granmai_ingl.xml	local	english
65	greece_kathimerini	http://ws.kathimerini.gr/xml_files/latestnews.xml	local	english

Phoenix Data Project: News Event Sources / As of: 29 Mar 2017

#	Name of News Source	Website address	News Type	Language
66	guardian_africa	http://www.theguardian.com/world/africa/roundup/rss	international	english
67	guardian_americas	http://www.theguardian.com/world/americas/roundup/rss	international	english
68	guardian_china	http://feeds.theguardian.com/theguardian/world/china/rss	international	english
69	guardian_europe	http://www.theguardian.com/world/europe/roundup/rss	international	english
70	guardian_scasia	http://www.theguardian.com/world/southandcentralasia/roundup/rss	international	english
71	haaretz_dd	http://feeds.feedburner.com/DefenseAndDiplomacy?format=xml	international	english
72	haaretz_international	http://feeds.feedburner.com/InternationalRss?format=xml	international	english
73	hindu_cities	http://www.thehindu.com/news/cities/?service=rss	local	english
74	hindu_int	http://www.thehindu.com/news/international/?service=rss	international	english
75	hindu_nat	http://www.thehindu.com/news/national/?service=rss	local	english
76	hindustan_bhopal	http://feeds.hindustantimes.com/HT-Bhopal?format=xml	local	english
77	hindustan_chandigarh	http://feeds.hindustantimes.com/HT-Punjab?format=xml	local	english
78	hindustan_dehradun	http://feeds.hindustantimes.com/HT-Dehradun?format=xml	local	english
79	hindustan_delhi	http://feeds.hindustantimes.com/HT-Delhi?format=xml	local	english
80	hindustan_gurgaon	http://feeds.hindustantimes.com/HT-Gurgaon?format=xml	local	english
81	hindustan_india	http://feeds.hindustantimes.com/HT-India?format=xml	local	english
82	hindustan_indore	http://feeds.hindustantimes.com/HT-Indore?format=xml	local	english
83	hindustan_jaipur	http://feeds.hindustantimes.com/HT-Jaipur?format=xml	local	english
84	hindustan_kolkata	http://feeds.hindustantimes.com/HT-Kolkata?format=xml	local	english
85	hindustan_lucknow	http://feeds.hindustantimes.com/HT-Lucknow?format=xml	local	english
86	hindustan_mumbai	http://feeds.hindustantimes.com/HT-Mumbai-News?format=xml	local	english
87	hindustan_noida	http://feeds.hindustantimes.com/HT-Noida?format=xml	local	english
88	hindustan_patna	http://feeds.hindustantimes.com/HT-Patna?format=xml	local	english
89	hindustan_ranchi	http://feeds.hindustantimes.com/HT-Ranchi?format=xml	local	english
90	hindustan_world	http://feeds.hindustantimes.com/HT-World?format=xml	local	english
91	houstoncron_news	http://www.chron.com/rss/feed/News-270.php	local	english
92	hungary_budbusjourn	http://www.bbj.hu/assets/rss/rss.php	local	english
93	hurriyet	http://www.hurriyetdailynews.com/rss.aspx	international	english
94	india_deccanher_elec	http://www.deccanherald.com/rss/election-news.rss	local	english
95	india_deccanher_int	http://www.deccanherald.com/rss-internal/top-stories.rss	local	english
96	india_deccanher_news	http://www.deccanherald.com/rss/news.rss	local	english
97	india_mint_companies	http://www.livemint.com/rss/companies	local	english
98	india_mint_econpol	http://www.livemint.com/rss/economy_politics	local	english
99	india_mint_homepage	http://www.livemint.com/rss/homepage	local	english
100	india_mint_industry	http://www.livemint.com/rss/industry	local	english
101	india_statesman_bengal	http://www.thestatesman.net/feed.aspx?cat_id=10	local	english
102	india_statesman_india	http://www.thestatesman.net/feed.aspx?cat_id=1	local	english
103	india_statesman_odisha	http://www.thestatesman.net/feed.aspx?cat_id=429	local	english
104	india_statesman_world	http://www.thestatesman.net/feed.aspx?cat_id=2	local	english
105	india_telegraph_bengal	http://www.telegraphindia.com/feeds/rss.jsp?id=8	local	english
106	india_telegraph_bihar	http://www.telegraphindia.com/feeds/rss.jsp?id=22	local	english
107	india_telegraph_calcutta	http://www.telegraphindia.com/feeds/rss.jsp?id=5	local	english
108	india_telegraph_int	http://www.telegraphindia.com/feeds/rss.jsp?id=13	local	english
109	india_telegraph_jharkhand	http://www.telegraphindia.com/feeds/rss.jsp?id=23	local	english
110	india_telegraph_nation	http://www.telegraphindia.com/feeds/rss.jsp?id=4	local	english
111	india_telegraph_nbengal	http://www.telegraphindia.com/feeds/rss.jsp?id=14	local	english
112	india_telegraph_northeast	http://www.telegraphindia.com/feeds/rss.jsp?id=24	local	english
113	india_telegraph_odisha	http://www.telegraphindia.com/feeds/rss.jsp?id=25	local	english
114	india_zee_national	http://zeenews.india.com/rss/india-national-news.xml	local	english
115	india_zee_states	http://zeenews.india.com/rss/india-news.xml	local	english
116	india_zee_world	http://zeenews.india.com/rss/world-news.xml	international	english
117	india_zee_seasia	http://zeenews.india.com/rss/south-asia-news.xml	international	english
118	insight	http://www.insightcrime.org/news/feed	international	english
119	int_the_news_islamabad	http://feeds.feedburner.com/TheNewsInternational-Islamabad?format=xml	local	english
120	int_the_news_karachi	http://feeds.feedburner.com/TheNewsInternational-Karachi?format=xml	local	english
121	int_the_news_lahore	http://feeds.feedburner.com/TheNewsInternational-Lahore?format=xml	local	english
122	int_the_news_latest	http://feeds.feedburner.com/com/YEor?format=xml	local	english
123	int_the_news_national	http://feeds.feedburner.com/TheNewsInternational-National?format=xml	local	english
124	int_the_news_peshawar	http://feeds.feedburner.com/TheNewsInternational-Peshawar?format=xml	local	english
125	int_the_news_top	http://feeds.feedburner.com/com/cwEr?format=xml	local	english
126	int_the_news_world	http://feeds.feedburner.com/World-TheNewsInternational?format=xml	international	english
127	ips_africa	http://www.ipsnews.net/news/regional-categories/africa/	international	english
128	ips_aid	http://www.ipsnews.net/news/development-aid/feed/	international	english
129	ips_asiapac	http://www.ipsnews.net/news/regional-categories/asia-pacific/	international	english
130	ips_civsoc	http://www.ipsnews.net/news/civil-society/feed/	international	english

3 of 6

Phoenix Data Project: News Event Sources / As of: 29 Mar 2017

#	Name of News Source	Website address	News Type	Language
131	ips_econ	http://www.ipsnews.net/news/economy-trade/feed/	international	english
132	ips_env	http://www.ipsnews.net/news/environment/feed/	international	english
133	ips_europe	http://www.ipsnews.net/news/regional-categories/europe/	international	english
134	ips_gender	http://www.ipsnews.net/news/gender/feed/	international	english
135	ips_gg	http://www.ipsnews.net/news/global-governance/feed/	international	english
136	ips_headlines	http://www.ipsnews.net/news/headlines/feed/	international	english
137	ips_hr	http://www.ipsnews.net/news/human-rights/feed/	international	english
138	ips_latinam	http://www.ipsnews.net/news/regional-categories/latin-america-and-caribbean/	international	english
139	ips_me	http://www.ipsnews.net/news/regional-categories/middle-east/	international	english
140	ips_namerica	http://www.ipsnews.net/news/regional-categories/north-america/	international	english
141	ips_ss	http://www.ipsnews.net/news/south-south/	international	english
142	ips_world	http://www.ipsnews.net/news/regional-categories/world/	international	english
143	ireland_herald	http://www.herald.ie/rss	local	english
144	ireland_rte	http://www.rte.ie/news/rss/news-headlines.xml	international	english
145	irin	http://www.irinnews.org/irin.xml	international	english
146	japan_times	http://www.japantimes.co.jp/feed/topstories/	local	english
147	jordan_times	http://feeds.feedburner.com/TheJordanTimes-LatestNews?format=xml	international	english
148	jpost_defense	http://www.jpost.com/Rss/RssFeedsDefense.aspx	international	english
149	jpost_front	http://www.jpost.com/Rss/RssFeedsFrontPage.aspx	international	english
150	jpost_int	http://www.jpost.com/Rss/RssFeedsInternationalNews.aspx	international	english
151	jpost_iran	http://www.jpost.com/Rss/RssFeedsIT.aspx	international	english
152	jpost_me	http://www.jpost.com/Rss/RssFeedsMiddleEastNews.aspx	international	english
153	kenya_nation	http://www.nation.co.ke/-/1148/1148/-/view/asFeed/-/vtvnjq/-/index.xml	local	english
154	kenya_news24	http://feeds.news24.com/articles/kenya/National/rss	local	english
155	kenya_star	http://www.the-star.co.ke/rss.xml	local	english
156	kosovapress	http://www.kosovapress.com/en/rss/news/?xml=1	local	english
157	kyodo	http://english.kyodonews.jp/rss/news.xml	international	english
158	lithuania_tribune	http://www.lithuaniatribune.com/feed/	local	english
159	maan_news	http://maannews.net/ENG/Rss.aspx?CID=NEW	international	english
160	maan_regional	http://maannews.net/ENG/Rss.aspx?CID=RGN	international	english
161	maan_politics	http://maannews.net/ENG/Rss.aspx?CID=POL	international	english
162	mail_and_guardian	http://mg.co.za/rss/	local	english
163	malstar_nat	http://www.thestar.com.my/RSS/News/Nation/	local	english
164	malstar_regional	http://www.thestar.com.my/RSS/News/Regional/	international	english
165	malstar_world	http://www.thestar.com.my/RSS/News/World/	international	english
166	malta_independent	http://www.independent.com.mt/rss/news-51118080/	local	english
167	malta_today	http://www.maltatoday.com.mt/rss/	local	english
168	mb	http://www.mb.com.ph/feed/	local	english
169	mcclatchy_econ	http://www.mcclatchydc.com/economy/v-rss/index.rss	international	english
170	mcclatchy_iraq	http://www.mcclatchydc.com/iraq/v-rss/index.rss	international	english
171	mcclatchy_mideast	http://www.mcclatchydc.com/middle-east/v-rss/index.rss	international	english
172	mcclatchy_mexico	http://www.mcclatchydc.com/mexico/v-rss/index.rss	international	english
173	mcclatchy_guantanamo	http://www.mcclatchydc.com/guantanamo/v-rss/index.rss	international	english
174	mcclatchy_europe	http://www.mcclatchydc.com/europe/v-rss/index.rss	international	english
175	mcclatchy_asia	http://www.mcclatchydc.com/asia/v-rss/index.rss	international	english
176	mcclatchy_afpak	http://www.mcclatchydc.com/afghanistan-pakistan/v-rss/index.rss	international	english
177	mcclatchy_whitehouse	http://www.mcclatchydc.com/white-house/v-rss/index.rss	international	english
178	mcclatchy_congress	http://www.mcclatchydc.com/congress/v-rss/index.rss	international	english
179	mcclatchy_state	http://www.mcclatchydc.com/state/v-rss/index.rss	international	english
180	mcclatchy_election	http://www.mcclatchydc.com/election-news/v-rss/index.rss	international	english
181	mcclatchy_politics	http://www.mcclatchydc.com/political-news/v-rss/index.rss	international	english
182	mcclatchy_natsec	http://www.mcclatchydc.com/national-security/v-rss/index.rss	international	english
183	mcclatchy_courtscrime	http://www.mcclatchydc.com/courts-crime/v-rss/index.rss	local	english
184	mcclatchy_nation	http://www.mcclatchydc.com/nation-news/v-rss/index.rss	international	english
185	mcclatchy_syria	http://www.mcclatchydc.com/syria/v-rss/index.rss	international	english
186	mcclatchy_egypt	http://www.mcclatchydc.com/egypt/v-rss/index.rss	international	english
187	menafn_algeria	http://www.menafn.com/rss/menafn_Algeria.xml	international	english
188	menafn_bahrain	http://www.menafn.com/rss/menafn_Bahrain.xml	international	english
189	menafn_egypt	http://www.menafn.com/rss/menafn_Egypt.xml	international	english
190	menafn_iraq	http://www.menafn.com/rss/menafn_Iraq.xml	international	english
191	menafn_jordan	http://www.menafn.com/rss/menafn_Jordan.xml	international	english
192	menafn_kuwait	http://www.menafn.com/rss/menafn_Kuwait.xml	international	english
193	menafn_lebanon	http://www.menafn.com/rss/menafn_Lebanon.xml	international	english
194	menafn_morocco	http://www.menafn.com/rss/menafn_Morocco.xml	international	english
195	menafn_oman	http://www.menafn.com/rss/menafn_Oman.xml	international	english

4 of 6

Phoenix Data Project: News Event Sources / As of: 29 Mar 2017

#	Name of News Source	Website address	News Type	Language
196	menafn_palestine	http://www.menafn.com/rss/menafn_Palestine.xml	international	english
197	menafn_qatar	http://www.menafn.com/rss/menafn_Qatar.xml	international	english
198	menafn_saudi	http://www.menafn.com/rss/menafn_Saudi_Arabia.xml	international	english
199	menafn_syria	http://www.menafn.com/rss/menafn_Syria.xml	international	english
200	menafn_tunisia	http://www.menafn.com/rss/menafn_Tunisia.xml	international	english
201	menafn_turkey	http://www.menafn.com/rss/menafn_Turkey.xml	international	english
202	menafn_uae	http://www.menafn.com/rss/menafn_UAE.xml	international	english
203	menafn_yemen	http://www.menafn.com/rss/menafn_Yemen.xml	international	english
204	mercopress	http://en.mercopress.com/rss/	international	english
205	miami_americas	http://www.miamiherald.com/news/americas/index.xml	local	english
206	miami_cuba	http://www.miamiherald.com/news/americas/cuba/index.xml	local	english
207	miami_haiti	http://www.miamiherald.com/news/americas/haiti/index.xml	local	english
208	miami_nation	http://www.miamiherald.com/news/nation/index.xml	local	english
209	miami_politics	http://www.miamiherald.com/news/politics/index.xml	local	english
210	miami_world	http://www.miamiherald.com/news/world/index.xml	international	english
211	middleeasteye	http://www.middleeasteye.net/rss	international	english
212	miltimes_army	http://projects.militarytimes.com/rss-feed/?sitename=Army	international	english
213	miltimes_navy	http://projects.militarytimes.com/rss-feed/?sitename=Navy	international	english
214	minnstartrib_national	http://www.startribune.com/nation/index.rss2	local	english
215	minnstartrib_world	http://www.startribune.com/world/index.rss2	international	english
216	moldova_infotag	http://www.infotag.md/eng/	local	english
217	moscow_times	http://www.themoscowtimes.com/rss/news/	international	english
218	nation_news	http://feeds.feedburner.com/pakistan-news-newspaper-daily-english-online/24hours-news?format=xml	international	english
219	nigeria_abusidiqu	http://abusidiqu.com/feed/	local	english
220	nigeria_advocate	http://theadvocatengr.com/new/?feed=rss2	local	english
221	nigeria_blanknews	http://blanknewsonline.wordpress.com/feed/	local	english
222	nigeria_blueprint	http://www.blueprint.ng/feed/	local	english
223	nigeria_businessday	http://businessdayonline.com/feed/	local	english
224	nigeria_businessnews	http://businessnews.com.ng/feed/	local	english
225	nigeria_businessworld	http://businessworldng.com/new/?feed=rss2	local	english
226	nigeria_dailyindependent	http://dailyindependentnig.com/feed/	local	english
227	nigeria_dailypost	http://dailypost.ng/feed/	local	english
228	nigeria_desertherald	http://desertherald.com/feed/	local	english
229	nigeria_hallmark	http://www.hallmarknews.com/feed/	local	english
230	nigeria_herald	http://www.theheraldnews.info/feed	local	english
231	nigeria_leadership	http://leadership.ng/feed/	local	english
232	nigeria_nationalmirror	http://nationalmirroronline.net/new/feed/	local	english
233	nigeria_newsday	http://newsdayngonline.com/feed/	local	english
234	nigeria_newschronicle	http://thenews-chronicle.com/feed/	local	english
235	nigeria_newswatch	http://www.mydailynewswatchng.com/feed/	local	english
236	nigeria_osundefender	http://www.osundefender.org/?feed=rss2	local	english
237	nigeria_peoplesdaily	http://www.peoplesdaily-online.com/feed/	local	english
238	nigeria_pilot	http://nigerianpilot.com/feed/	local	english
239	nigeria_pmnews	http://feeds.feedburner.com/PmNewsNigeriaFeed?format=xml	local	english
240	nigeria_premiumtimes	http://www.premiumtimesng.com/feed	local	english
241	nigeria_promptnews	http://www.promptnewsonline.com/feed/	local	english
242	nigeria_quicknews	http://www.quicknews-africa.net/feed/	local	english
243	nigeria_saharareporters	http://saharareporters.com/feeds/latest/feed	local	english
244	nigeria_standard	http://www.thenigeriastandard.com/index.php?format=feed&type=rss	local	english
245	nigeria_sunnews	http://sunnewsonline.com/new/?feed=rss2	local	english
246	nigeria_thepunch	http://www.punchng.com/feed/	local	english
247	nigeria_tidenews	http://www.thetidenewsonline.com/feed/	local	english
248	nigeria_tribune_conf	http://www.tribune.com.ng/confab?format=feed	local	english
249	nigeria_tribune_headlines	http://www.tribune.com.ng/news/news-headlines?format=feed	local	english
250	nigeria_tribune_politics	http://www.tribune.com.ng/quicklinkss/politics?format=feed	local	english
251	nigeria_vangard	http://www.vanguardngr.com/feed/	local	english
252	nyt	http://rss.nytimes.com/services/xml/rss/nyt/World.xml	wire	english
253	nytafrica	http://rss.nytimes.com/services/xml/rss/nyt/Africa.xml	wire	english
254	nytamericas	http://rss.nytimes.com/services/xml/rss/nyt/Americas.xml	wire	english
255	nytasiapacific	http://rss.nytimes.com/services/xml/rss/nyt/AsiaPacific.xml	wire	english
256	nytatwar	http://atwar.blogs.nytimes.com/feed/	wire	english
257	nyteurope	http://rss.nytimes.com/services/xml/rss/nyt/Europe.xml	wire	english
258	nytindia	http://india.blogs.nytimes.com/feed/	wire	english
259	nytmiddleeast	http://rss.nytimes.com/services/xml/rss/nyt/MiddleEast.xml	wire	english
260	nxherald_national	http://rss.nzherald.co.nz/rss/xml/nzhrsscid_000000001.xml	local	english

5 of 6

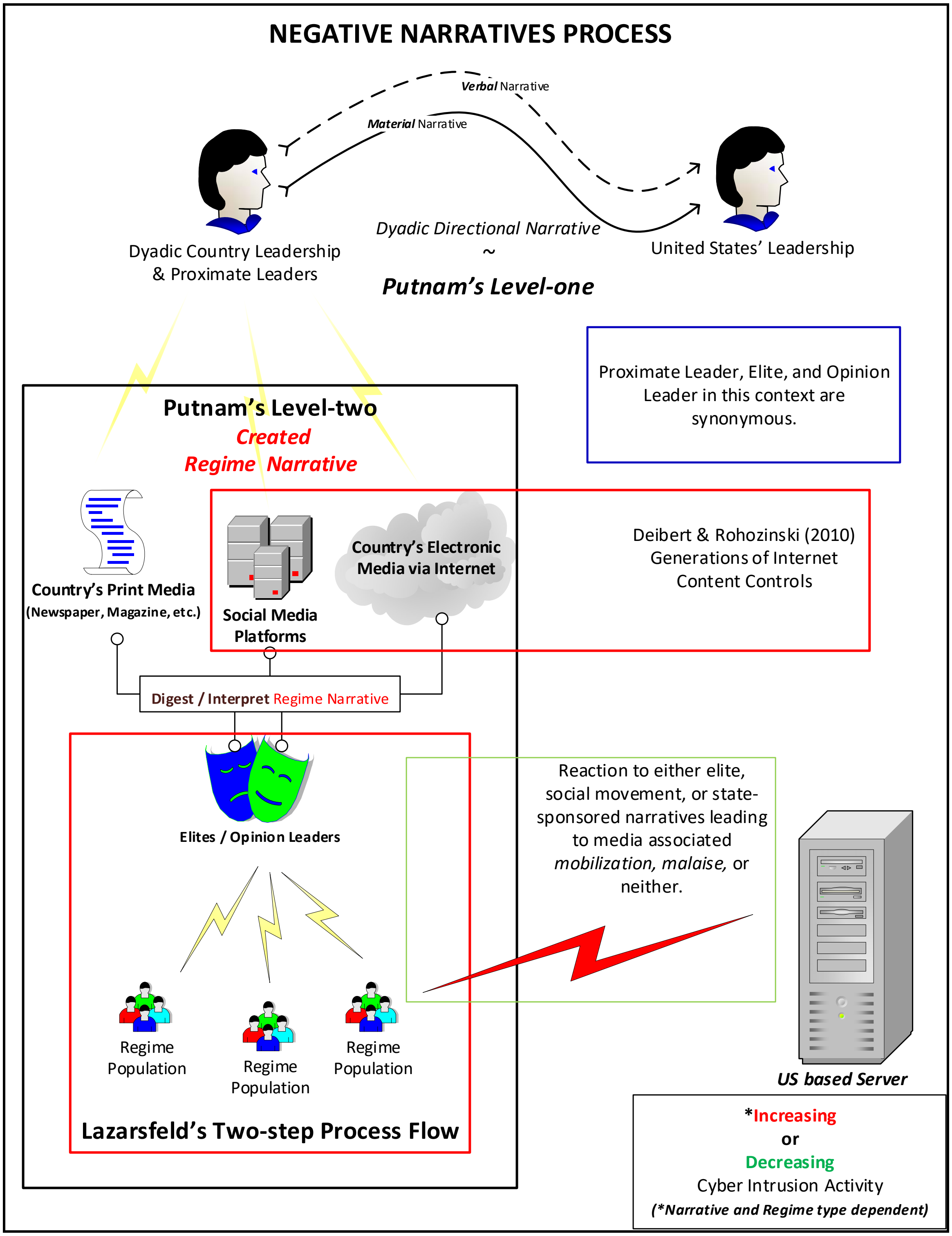
Phoenix Data Project: News Event Sources / As of: 29 Mar 2017

#	Name of News Source	Website address	News Type	Language
261	nzherald_world	http://rss.nzherald.co.nz/rss/xml/nzhrsscid_000000002.xml	international	english
262	ocregister_ap	http://hosted2.ap.org/atom/CAANR/0260ea4c3e85456b80715585ba3c7b5b	international	english
263	pahjwok_english	http://www.pajhwok.com/en/nodequeue/1/feed	international	english
264	pakistan_balohhal	http://thebalochhal.com/feed/	local	english
265	pakistan_busrecorder_pak	http://www.brecorder.com/rss/?feed_id=2&format=raw	local	english
266	pakistan_busrecorder_world	http://www.brecorder.com/rss/?feed_id=3&format=raw	international	english
267	pakistan_explorer_regional	http://dailyexplorer.net/category/regional-news/feed/	local	english
268	pakistan_explorer_national	http://dailyexplorer.net/category/national-news/feed/	local	english
269	pakistan_dailymessanger	http://dailymessenger.com.pk/feed/	local	english
270	pakistan_frontierpost	http://thefrontierpost.com/rss/	local	english
271	pakistan_fridaytimes	http://thefridaytimes.com/tft/feed/	local	english
272	pakistan_lahoredispatch	http://lahoredispatch.com/feed	local	english
273	pakistan_kooza	http://www.thekooza.com/feed	local	english
274	pakistan_thenews	http://feeds.feedburner.com/Newspakistanpk?format=xml	international	english
275	pakistan_pakasiatimes	http://www.pakasiatimes.com/feed/	international	english
276	pakistan_thepioneer	http://thepioneer.com.pk/feed/	international	english
277	pakistan_tribune	http://www.pakistantribune.com.pk/feed	local	english
278	pakistan_telegraph	http://www.pakistantelegraph.com/index.php/rss/8c3d7d78943a99c7	local	english
279	pakistan_worldtribune	http://worldtribunepakistan.com/feed/	international	english
280	panamanews	http://thepanamanews.com/wp/?feed=rss2	local	english
281	payvand	http://www.payvand.com/news/rssfeed.xml	local	english
282	phil_inquirer	http://www.inquirer.net/fullfeed	local	english
283	phil_manilatimes	http://www.manilatimes.net/feed/	local	english
284	phil_manilabulletin	http://www.mb.com.ph/feed/	local	english
285	phil_manilastandard	http://manilastandardtoday.com/feed/news/	local	english
286	phil_sunstar_breaking	http://www.sunstar.com.ph/feeds/breaking-news	local	english
287	phil_sunstar_bacolod	http://www.sunstar.com.ph/feeds/bacolod	local	english
288	phil_sunstar_cagayan	http://www.sunstar.com.ph/feeds/cagayan-de-oro	local	english
289	phil_sunstar_cebu	http://www.sunstar.com.ph/feeds/cebu	local	english
290	phil_sunstar_davao	http://www.sunstar.com.ph/feeds/davao	local	english
291	phil_sunstar_dumaguete	http://www.sunstar.com.ph/feeds/dumaguete	local	english
292	phil_sunstar_iloilo	http://www.sunstar.com.ph/feeds/iloilo	local	english
293	phil_sunstar_manila	http://www.sunstar.com.ph/feeds/manila	local	english
294	phil_sunstar_pangasinan	http://www.sunstar.com.ph/feeds/pangasinan	local	english
295	phil_sunstar_tacloban	http://www.sunstar.com.ph/feeds/tacloban	local	english
296	phil_sunstar_zamboanga	http://www.sunstar.com.ph/feeds/zamboanga	local	english
297	phil_sunstar_pampanga	http://www.sunstar.com.ph/feeds/pampanga	local	english
298	philstar_headlines	http://www.philstar.com/rss/headlines	local	english
299	philstar_nation	http://www.philstar.com/rss/nation	local	english
300	philstar_world	http://www.philstar.com/rss/world	local	english
301	philstar_region	http://www.philstar.com/rss/region	local	english
302	phil_bicolmail	http://www.bicolmail.com/2012/?feed=rss2	local	english
303	phil_manilachannel	http://www.manilachannel.com/feed/	local	english
304	reuters	http://feeds.reuters.com/Reuters/worldNews	wire	english
305	rfa	http://www.rfa.org/english/RSS	wire	english
306	rfe	http://www.rferl.org/api/epiqq	wire	english
307	rfi	http://www.english.rfi.fr/last_24h/rss	wire	english
308	romania_nineoclock	http://www.nineoclock.ro/feed/	local	english
309	russia_interpreter	http://www.interpretermag.com/feed/	local	english
310	russia_stpetersburgtimes	http://feeds.feedburner.com/sptimes?format=xml	local	english
311	sacbee_natworld	http://www.sacbee.com/830/index.rss	international	english
312	sacbee_state	http://www.sacbee.com/state/index.rss	local	english
313	seurtimes	http://www.setimes.com/cocoon/setimes/rss/en_GB/setimes.rss	international	english
314	sfgate_bayarea	http://www.sfgate.com/bayarea/feed/Bay-Area-News-429.php	local	english
315	sfgate_national	http://www.sfgate.com/rss/feed/National-News-RSS-Feed-435.php	international	english
316	sfgate_world	http://www.sfgate.com/rss/feed/World-News-From-SFGate-432.php	international	english
317	shanghai_national	http://rss.shanghaidaily.com/Portal/mainSite/Handler.ashx?i=3	international	english
318	shanghai_world	http://rss.shanghaidaily.com/Portal/mainSite/Handler.ashx?i=7	international	english
319	skorea_chosun	http://english.chosun.com/site/data/rss/rss.xml	local	english
320	skorea_hankung_econ	http://rss.hankyung.com/english/latest.xml	local	english
321	skorea_yonhap_nk	http://english.yonhapnews.co.kr/RSS/northkorea.xml	local	english
322	skorea_yonhap_sk	http://english.yonhapnews.co.kr/RSS/headline.xml	local	english
323	somalia_horseed	http://feeds.feedburner.com/horseed?format=xml	local	english
324	somalia_sabahi	http://sabahionline.com/en_GB/rss	local	english
325	southaf_busdaily_nat	http://www.bdlive.co.za/national/?service=rss	local	english

6 of 6

Phoenix Data Project: News Event Sources / As of: 29 Mar 2017				
#	**Name of News Source**	**Website address**	**News Type**	**Language**
326	southaf_busdaily_world	http://www.bdlive.co.za/world/?service=rss	international	english
327	southaf_capetownt	http://www.iol.co.za/cmlink/1.1046095	local	english
328	southaf_citypress	http://www.citypress.co.za/feature-type/top-stories/feed/	local	english
329	southaf_iol_pretoria	http://www.iol.co.za/cmlink/1.1118954	local	english
330	southaf_iol_thestar	http://www.iol.co.za/cmlink/1.1073915	local	english
331	southaf_iol	http://iol.co.za/cmlink/1.640	local	english
332	southaf_mailg	http://mg.co.za/rss/	local	english
333	spiegel	http://www.spiegel.de/international/index.rss	international	english
334	straits_times_asia	http://straitstimes.com.feedsportal.com/c/32792/f/640960/index.rss	international	english
335	straits_times_singapore	http://straitstimes.com.feedsportal.com/c/32792/f/640958/index.rss	international	english
336	straits_times_world	http://straitstimes.com.feedsportal.com/c/32792/f/640961/index.rss	international	english
337	taipeitimes_taiwan	http://www.taipeitimes.com/xml/taiwan.rss	international	english
338	taipeitimes_world	http://www.taipeitimes.com/xml/world.rss	international	english
339	thailand_bankokpost	http://www.bangkokpost.com/rss/data/news.xml	international	english
340	thailand_nation_national	http://www.nationmultimedia.com/home/rss/national.rss	international	english
341	thailand_national_politics	http://www.nationmultimedia.com/home/rss/politics.rss	local	english
342	thailand_phuket	http://www.phuketgazette.net/rss/get_rss_news_by_type/5/15	local	english
343	thenational_uae	http://www.thenational.ae/section/rss	local	english
344	thenews_pk_islamabad	http://feeds.feedburner.com/TheNewsInternational-Islamabad	local	english
345	thenews_pk_karachi	http://feeds.feedburner.com/TheNewsInternational-Karachi	local	english
346	thenews_pk_lahore	http://feeds.feedburner.com/TheNewsInternational-Lahore	local	english
347	thenews_pk_national	http://feeds.feedburner.com/TheNewsInternational-National	local	english
348	thenews_pk_peshawar	http://feeds.feedburner.com/TheNewsInternational-Peshawar	local	english
349	times_of_india_india	http://timesofindia.feedsportal.com/c/33039/f/533965/index.rss	local	english
350	times_of_india_world	http://timesofindia.feedsportal.com/c/33039/f/533917/index.rss	international	english
351	tolo	http://www.tolonews.com/en/component/ninjarsssyndicator/?feed_id=1&format=raw	local	english
352	toronto_star_top	http://www.thestar.com/feeds.topstories.rss	international	english
353	toronto_star_world	http://www.thestar.com/feeds.articles.news.world.rss	international	english
354	toronto_star_canada	http://www.thestar.com/feeds.articles.news.canada.rss	international	english
355	uganda_monitor	http://www.monitor.co.ug/-/691150/691150/-/view/asFeed/-/11emxavz/-/index.xml	local	english
356	uganda_newvision_national	http://www.newvision.co.ug/feed.aspx?cat_id=1	local	english
357	uganda_newvision_world	http://www.newvision.co.ug/feed.aspx?cat_id=2	local	english
358	uk_telegraph_world	http://www.telegraph.co.uk/news/worldnews/rss	international	english
359	uk_telegraph_national	http://www.telegraph.co.uk/news/uknews/rss	international	english
360	uk_telegraph_politics	http://www.telegraph.co.uk/news/politics/rss	international	english
361	un_africa	http://www.un.org/apps/news/rss/rss_africa.asp	international	english
362	upi	http://rss.upi.com/news/emerging_threats.rss	international	english
363	voa_africa	http://www.voanews.com/api/z-$otevtiq	international	english
364	voa_all	http://www.voanews.com/api/epiqq	international	english
365	voa_am	http://www.voanews.com/api/zoripegtim	international	english
366	voa_asia	http://www.voanews.com/api/zo$o_egviy	international	english
367	voa_euro	http://www.voanews.com/api/zj$oveytit	international	english
368	voa_me	http://www.voanews.com/api/zr$opeuvim	international	english
369	voa_news	http://www.voanews.com/api/zji-veyj-v	international	english
370	wn_africa	http://rss.wn.com/English/keyword/africa	international	english
371	wn_americas	http://rss.wn.com/English/keyword/america	international	english
372	wn_asia	http://rss.wn.com/English/keyword/asia	international	english
373	wn_europe	http://rss.wn.com/English/keyword/europe	international	english
374	wn_mideast	http://rss.wn.com/English/keyword/mideast	international	english
375	wn_politics	http://rss.wn.com/English/keyword/politics	international	english
376	wn_world	http://rss.wn.com/English/keyword/world	international	english
377	wpr_africa	http://www.worldpress.org/feeds/africa.xml	international	english
378	wpr_americas	http://www.worldpress.org/feeds/americas.xml	international	english
379	wpr_asia	http://www.worldpress.org/feeds/asia.xml	international	english
380	wpr_europe	http://www.worldpress.org/feeds/europe.xml	international	english
381	wpr_mideast	http://www.worldpress.org/feeds/Mideast.xml	international	english
382	xinhua	http://www.xinhuanet.com/english/rss/worldrss.xml	wire	english
383	yahoo_india	http://in.news.yahoo.com/rss/asia	local	english
384	yemen_times	http://www.yementimes.com/?tpl=1341	local	english
385	zaman	http://www.todayszaman.com/104.rss	international	english
386	zawya	http://www.zawya.com/top-stories/rss/home/	local	english
	Intl#	184		
	Local#	187		
	Wire#	15		
	Total	386		

APPENDIX C. LOGIC MAP: NEGATIVE *MATERIAL / VERBAL* NARRATIVES



Proximate Leader, Elite, and Opinion Leader in this context are synonymous.

Reaction to either elite, social movement, or state-sponsored narratives leading to media associated *mobilization, malaise,* or neither.

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX D. MACRO-MODEL COMPARISON RESULTS

CYBER INTRUSION ATTEMPTS (Macro-Model: All-Media Narratives) 29 Oct 2020

	Dependent Variable										
	Total Intrusions_Lead (Today)										
	Normal	**Poisson**	Zero-Poisson	Zero-Poisson2	Hurdle-Poisson	Hurdle-Poisson2	NegBinomial (NegBin)	Zero-NegBin	Zero-NegBin2	Hurdle-NegBin	Hurdle-NegBin2
	(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)	(9)	(10)	(11)
Neg Mat Narratives	**85.840*****	**0.006*****	**0.016*****	**0.016*****	**0.016*****	**0.016*****	**0.623*****	**0.189*****	**0.193*****	**0.188*****	**0.188*****
	(12.347)	**(0.002)**	**(0.002)**	**(0.002)**	**(0.002)**	**(0.002)**	**(0.040)**	**(0.036)**	**(0.036)**	**(0.038)**	**(0.038)**
Neg Ver Narratives	59.524***	–0.168***	–0.161***	–0.161***	–0.161***	–0.161***	0.348***	0.162***	0.164***	0.166***	0.166***
	(8.737)	(0.001)	(0.001)	(0.001)	(0.001)	(0.001)	(0.028)	(0.026)	(0.026)	(0.028)	(0.028)
Avg NN Tone	**7.948*****	**0.001****	**0.001****	**0.001****	**0.001****	**0.001****	**0.111*****	**0.063*****	**0.062*****	**0.066*****	**0.066*****
	(2.008)	**(0.0004)**	**(0.0004)**	**(0.0004)**	**(0.0004)**	**(0.0004)**	**(0.007)**	**(0.006)**	**(0.006)**	**(0.007)**	**(0.007)**
NN Tone StdDev	–6.646**	–0.031***	–0.032***	–0.032***	–0.032***	–0.032***	–0.008	–0.009	–0.008	–0.006	–0.006
	(3.183)	(0.001)	(0.001)	(0.001)	(0.001)	(0.001)	(0.011)	(0.010)	(0.010)	(0.011)	(0.011)
Polity	**–5.340*****	**–0.009*****	**–0.012*****	**–0.012*****	**–0.012*****	**–0.012*****	**0.007*****	**–0.006*****	**–0.006*****	**–0.006****	**–0.006****
	(0.559)	**(0.0002)**	**(0.0002)**	**(0.0002)**	**(0.0002)**	**(0.0002)**	**(0.002)**	**(0.002)**	**(0.002)**	**(0.002)**	**(0.002)**
Polity squared	0.559***	0.001***	0.0004***	0.0004***	0.0004***	0.0004***	0.0003	0.003***	0.003***	0.003***	0.003***
	(0.098)	(0.00004)	(0.00004)	(0.00004)	(0.00004)	(0.00004)	(0.0004)	(0.0004)	(0.0004)	(0.0004)	(0.0004)
Internet PenRate	**–1.334*****	**–0.004*****	**–0.004*****	**–0.004*****	**–0.004*****	**–0.004*****	**0.011*****	**0.005*****	**0.005*****	**0.006*****	**0.006*****
	(0.190)	**(0.0001)**	**(0.0001)**	**(0.0001)**	**(0.0001)**	**(0.0001)**	**(0.001)**	**(0.001)**	**(0.001)**	**(0.001)**	**(0.001)**
Internet Not Free	20.635***	0.199***	0.201***	0.201***	0.201***	0.201***	–0.052*	0.063**	0.063**	0.095***	0.095***
	(6.741)	(0.003)	(0.003)	(0.003)	(0.003)	(0.003)	(0.028)	(0.029)	(0.029)	(0.031)	(0.031)
Media Not Free	**0.198**	**–0.186*****	**–0.250*****	**–0.250*****	**–0.251*****	**–0.251*****	**–0.004**	**0.017**	**0.016**	**0.014**	**0.014**
	(7.622)	**(0.003)**	**(0.003)**	**(0.003)**	**(0.003)**	**(0.003)**	**(0.028)**	**(0.025)**	**(0.025)**	**(0.027)**	**(0.027)**
Media Self-Censor	8.156	0.078***	0.104***	0.104***	0.104***	0.104***	0.010	0.045*	0.046*	0.055*	0.055*
	(7.590)	(0.003)	(0.003)	(0.003)	(0.003)	(0.003)	(0.028)	(0.026)	(0.026)	(0.028)	(0.028)
Log: Population	**–11.752*****	**0.131*****	**0.090*****	**0.090*****	**0.090*****	**0.090*****	**0.420*****	**0.215*****	**0.215*****	**0.219*****	**0.219*****
	(2.080)	**(0.001)**	**(0.001)**	**(0.001)**	**(0.001)**	**(0.001)**	**(0.008)**	**(0.008)**	**(0.008)**	**(0.009)**	**(0.009)**
Log: GDP	–23.486***	0.257***	0.156***	0.156***	0.156***	0.156***	0.380***	0.170***	0.170***	0.159***	0.159***
	(4.442)	(0.003)	(0.003)	(0.003)	(0.003)	(0.003)	(0.019)	(0.020)	(0.020)	(0.021)	(0.021)

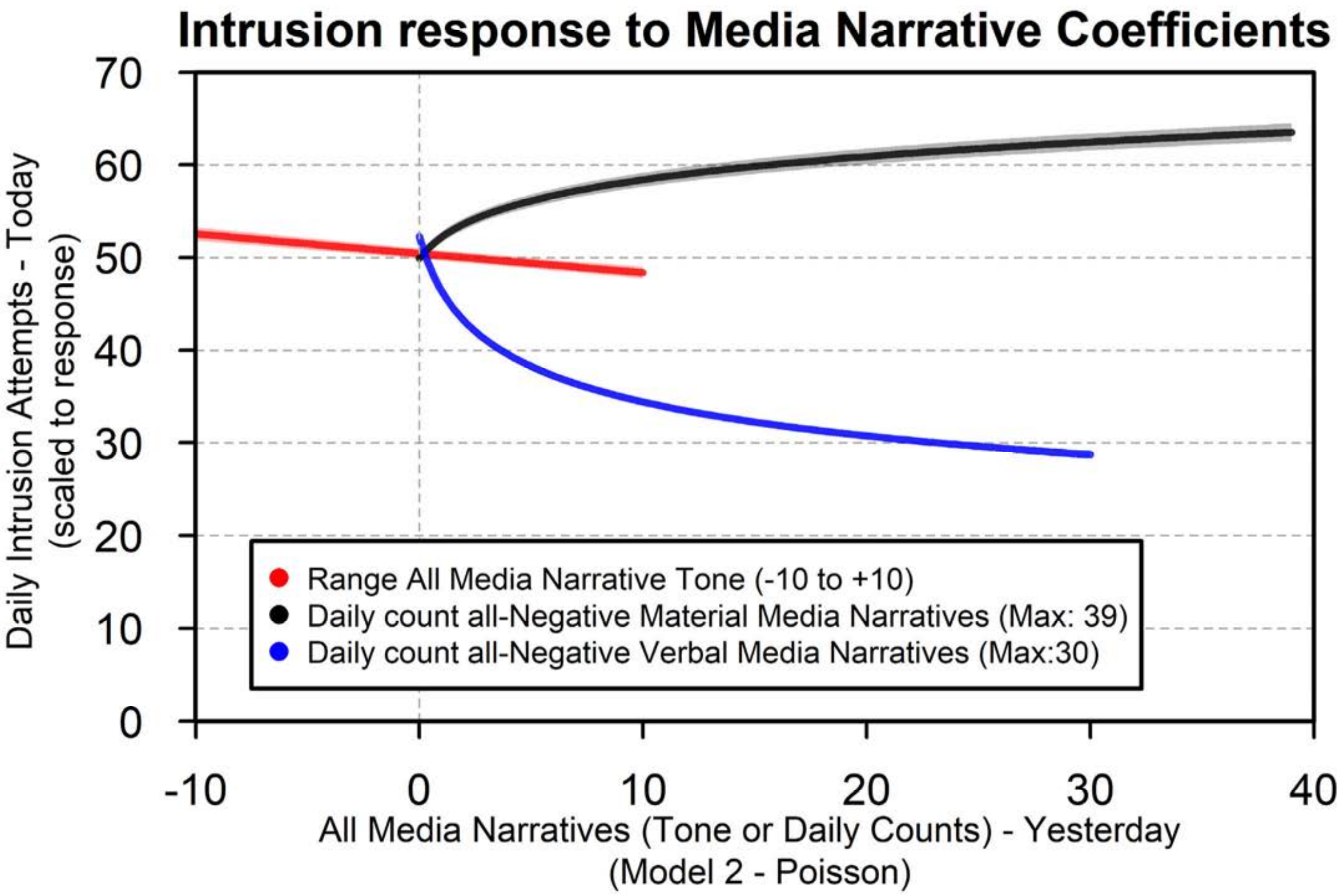
Log: Tot Narratives	**5.197**	**0.151*****	**0.163*****	**0.163*****	**0.163*****	**0.163*****	**0.048****	**0.107*****	**0.104*****	**0.104*****	**0.104*****
	(5.747)	**(0.001)**	**(0.001)**	**(0.001)**	**(0.001)**	**(0.001)**	**(0.020)**	**(0.017)**	**(0.017)**	**(0.019)**	**(0.019)**
Log: Tot Intrusions	120.781***	0.790***	0.764***	0.764***	0.764***	0.764***	0.781***	0.759***	0.759***	0.771***	0.771***
	(1.924)	(0.0005)	(0.0005)	(0.0005)	(0.0005)	(0.0005)	(0.007)	(0.005)	(0.005)	(0.006)	(0.006)
Tuesday	**–0.765**	**–0.0004**	**0.002**	**0.002**	**0.002**	**0.002**	**–0.028**	**0.119*****	**0.118*****	**0.120*****	**0.120*****
	(8.402)	**(0.003)**	**(0.003)**	**(0.003)**	**(0.003)**	**(0.003)**	**(0.032)**	**(0.031)**	**(0.030)**	**(0.033)**	**(0.033)**
Wednesday	15.280*	0.198***	0.192***	0.192***	0.192***	0.192***	0.052	–0.024	–0.015	–0.016	–0.016
	(8.360)	(0.003)	(0.003)	(0.003)	(0.003)	(0.003)	(0.032)	(0.030)	(0.030)	(0.033)	(0.033)
Thursday	**3.325**	**0.044*****	**0.044*****	**0.044*****	**0.044*****	**0.044*****	**–0.052**	**–0.020**	**–0.026**	**–0.028**	**–0.028**
	(8.433)	**(0.003)**	**(0.003)**	**(0.003)**	**(0.003)**	**(0.003)**	**(0.032)**	**(0.030)**	**(0.029)**	**(0.032)**	**(0.032)**
Friday	13.491	0.172***	0.182***	0.182***	0.182***	0.182***	0.241***	0.324***	0.317***	0.351***	0.351***
	(8.358)	(0.003)	(0.003)	(0.003)	(0.003)	(0.003)	(0.031)	(0.030)	(0.029)	(0.032)	(0.032)
Saturday	**11.341**	**0.176*****	**0.178*****	**0.178*****	**0.178*****	**0.178*****	**0.153*****	**0.201*****	**0.197*****	**0.205*****	**0.205*****
	(8.423)	**(0.003)**	**(0.003)**	**(0.003)**	**(0.003)**	**(0.003)**	**(0.032)**	**(0.030)**	**(0.029)**	**(0.032)**	**(0.032)**
Sunday	–21.571**	–0.268***	–0.267***	–0.267***	–0.267***	–0.267***	–0.165***	–0.218***	–0.220***	–0.215***	–0.215***
	(8.553)	(0.003)	(0.003)	(0.003)	(0.003)	(0.003)	(0.033)	(0.031)	(0.031)	(0.034)	(0.034)
Feb 2015	**10.297**	**0.203*****	**0.230*****	**0.230*****	**0.230*****	**0.230*****	**0.083***	**0.554*****	**0.553*****	**0.548*****	**0.548*****
	(10.428)	**(0.008)**	**(0.008)**	**(0.008)**	**(0.008)**	**(0.008)**	**(0.047)**	**(0.063)**	**(0.063)**	**(0.067)**	**(0.067)**
Mar 2015	13.065	–0.088***	–0.025***	–0.025***	–0.025***	–0.025***	–0.370***	–0.017	–0.017	–0.019	–0.019
	(10.101)	(0.008)	(0.008)	(0.008)	(0.008)	(0.008)	(0.047)	(0.062)	(0.062)	(0.065)	(0.065)
April 2015	**2.189**	**–0.058*****	**–0.035*****	**–0.035*****	**–0.036*****	**–0.036*****	**–0.009**	**0.220*****	**0.220*****	**0.218*****	**0.218*****
	(10.190)	**(0.008)**	**(0.008)**	**(0.008)**	**(0.008)**	**(0.008)**	**(0.046)**	**(0.059)**	**(0.059)**	**(0.062)**	**(0.062)**
May 2015	35.796**	1.953***	1.995***	1.995***	1.995***	1.995***	2.146***	2.821***	2.812***	2.819***	2.819***
	(15.746)	(0.007)	(0.007)	(0.007)	(0.007)	(0.007)	(0.057)	(0.085)	(0.085)	(0.090)	(0.090)
Sep 2016	**30.780****	**0.568*****	**0.490*****	**0.490*****	**0.490*****	**0.490*****	**0.594*****	**–0.183*****	**–0.182*****	**–0.243*****	**–0.243*****
	(13.104)	**(0.006)**	**(0.006)**	**(0.006)**	**(0.006)**	**(0.006)**	**(0.053)**	**(0.056)**	**(0.056)**	**(0.060)**	**(0.060)**
Oct 2016	–34.995***	0.414***	0.335***	0.335***	0.335***	0.335***	0.875***	–0.008	–0.009	–0.068	–0.068
	(10.246)	(0.006)	(0.006)	(0.006)	(0.006)	(0.006)	(0.042)	(0.047)	(0.047)	(0.050)	(0.050)
Nov 2016	**–98.488*****	**0.610*****	**0.474*****	**0.474*****	**0.474*****	**0.474*****	**1.395*****	**0.503*****	**0.501*****	**0.472*****	**0.472*****
	(10.440)	**(0.006)**	**(0.006)**	**(0.006)**	**(0.006)**	**(0.006)**	**(0.042)**	**(0.047)**	**(0.047)**	**(0.049)**	**(0.049)**
Dec 2016	–86.385***	0.639***	0.515***	0.515***	0.515***	0.515***	1.401***	0.344***	0.343***	0.311***	0.311***
	(10.754)	(0.006)	(0.006)	(0.006)	(0.006)	(0.006)	(0.043)	(0.047)	(0.047)	(0.049)	(0.049)

Jan 2017	**–141.828*****	**0.404*****	**0.236*****	**0.236*****	**0.236*****	**0.236*****	**1.101*****	**0.068**	**0.067**	**0.014**	**0.014**
	(10.497)	**(0.006)**	**(0.006)**	**(0.006)**	**(0.006)**	**(0.006)**	**(0.042)**	**(0.047)**	**(0.047)**	**(0.050)**	**(0.050)**
Feb 2017	–167.618***	0.486***	0.318***	0.318***	0.318***	0.318***	1.302***	0.179***	0.178***	0.123**	0.123**
	(11.489)	(0.006)	(0.006)	(0.006)	(0.006)	(0.006)	(0.045)	(0.048)	(0.048)	(0.051)	(0.051)
Mar 2017	**–164.415*****	**0.436*****	**0.270*****	**0.270*****	**0.270*****	**0.270*****	**1.268*****	**0.138*****	**0.136*****	**0.064**	**0.064**
	(12.795)	**(0.006)**	**(0.006)**	**(0.006)**	**(0.006)**	**(0.006)**	**(0.049)**	**(0.050)**	**(0.050)**	**(0.054)**	**(0.054)**
NN Gold_Mean *x* Polity	–0.139	–0.001***	–0.001***	–0.001***	–0.001***	–0.001***	–0.013***	–0.011***	–0.011***	–0.011***	–0.011***
	(0.204)	(0.00005)	(0.00005)	(0.00005)	(0.00005)	(0.00005)	(0.001)	(0.001)	(0.001)	(0.001)	(0.001)
Constant	**386.601*****	**–4.065*****	**–1.976*****	**–1.976*****	**–1.976*****	**–1.976*****	**–11.966*****	**–5.213*****	**–5.212*****	**–5.271*****	**–5.271*****
	(51.498)	**(0.029)**	**(0.031)**	**(0.031)**	**(0.031)**	**(0.031)**	**(0.216)**	**(0.222)**	**(0.222)**	**(0.238)**	**(0.238)**
Observations	34,881	34,881	34,881	34,881	34,881	34,881	34,881	34,881	34,881	34,881	34,881
Observations (test sample)	9,664	9,664	9,664	9,664	9,664	9,664	9,664	9,664	9,664	9,664	9,664
MAE	123.350	31.439	31.340	31.340	31.350	31.349	111.913	44.049	44.048	45.523	45.520
MAE (test sample)	130.924	**38.634**	38.837	38.838	38.842	38.842	111.246	48.766	48.720	49.796	49.794
RMSE	418.867	351.229	342.724	342.726	342.729	342.730	2,072.289	543.335	543.759	585.268	585.268
RMSE (test sample)	1,005.313	**928.845**	931.251	931.251	931.249	931.249	1,293.566	946.218	945.726	947.278	947.278
AIC	520,247.768	1,775,769.093	1,682,839.334	1,682,829.772	1,682,814.926	1,682,805.882	162,105.122	153,432.191	153,429.251	153,034.533	153,025.488
Log Likelihood	–260,089.884	–887,851.546	–841,353.667	–841,358.886	–841,341.463	–841,346.941	–81,018.561	–76,649.095	–76,657.625	–76,450.266	–76,455.744

Note: In Models 4, 6, 9, and 11 the statistically **insignificant** coefficients for the zero-inflated or hurdle portions of the models were removed to improve model fit (Zeileis, Kleiber, and Jackman, 2015).

*p < 0.1; **p < 0.05; ***p<0.01

.


Intrusion response to Media Narrative Coefficients
Daily Intrusion Attempts - Today
(scaled to response)
70
60
50
40
30
20
10
0
-10
0
10
20
30
40
All Media Narratives (Tone or Daily Counts) - Yesterday
(Model 2 - Poisson)
● Range All Media Narrative Tone (-10 to +10)
● Daily count all-Negative Material Media Narratives (Max: 39)
● Daily count all-Negative Verbal Media Narratives (Max:30)

APPENDIX E. RESEARCH MODEL COMPARISON RESULTS

CYBER INTRUSION ATTEMPTS – Today **13 Nov 2020**

TotalIntrusions – Today (Regime and Country Comparison)

Poisson Model

Independent Variables / Model	All-Negative Narrative	All-Autocracies	China	Iran	All-Anocracies	Russia	Turkey	All-Democracies	United Kingdom	India
NegMaterialNarratives	**0.03*****	**0.14*****	**0.42*****	**–0.12*****	**0.10*****	**–0.11*****	**0.03**	**0.03*****	**–0.27*****	**0.22*****
	(0.002)	**(0.002)**	**(0.003)**	**(0.004)**	**(0.005)**	**(0.01)**	**(0.03)**	**(0.004)**	**(0.01)**	**(0.01)**
NegVerbalNarratives	–0.24***	–0.23***	0.09***	–0.22***	0.0000	–0.12***	–0.41***	0.08***	–0.19***	–0.18***
	(0.002)	(0.002)	(0.003)	(0.004)	(0.005)	(0.01)	(0.02)	(0.004)	(0.01)	(0.01)
Avg NN Tone (GoldMean)	**–0.003*****	**–0.21*****	**0.12*****	**0.02*****	**–0.001**	**0.001**	**0.01**	**0.23*****	**–0.63*****	**–0.01****
	(0.001)	**(0.02)**	**(0.001)**	**(0.001)**	**(0.001)**	**(0.003)**	**(0.02)**	**(0.01)**	**(0.06)**	**(0.003)**
NN Tone StdDev	–0.01***	0.04***	0.15***	–0.07***	–0.02***	–0.03***	0.02**	–0.03***	0.06***	–0.20***
	(0.001)	(0.001)	(0.001)	(0.002)	(0.002)	(0.004)	(0.01)	(0.001)	(0.004)	(0.003)
Polity	**–0.01*****	**–2.75*****			**–0.01*****		**–0.08*****	**0.77*****	**–0.02**	
	(0.0001)	**(0.05)**			**(0.001)**		**(0.01)**	**(0.02)**	**(0.02)**	
Polity squared	–0.001***	–0.21***			–0.01***			–0.04***		
	(0.0000)	(0.003)			(0.001)			(0.001)		
Internet Not Free	**0.12*****				**–0.29*****			**0.08*****		
	(0.003)				**(0.01)**			**(0.005)**		
Media Not Free	–0.21***							–0.12***		
	(0.003)							(0.003)		
Media Self-Censorship	**0.08*****				**3.50*****			**0.04*****		
	(0.003)				**(0.45)**			**(0.003)**		
Friday	0.22***	0.17***	0.15***	0.58***	0.56***	0.42***	0.48***	0.29***	0.53***	–0.91***
	(0.002)	(0.004)	(0.01)	(0.01)	(0.01)	(0.01)	(0.01)	(0.003)	(0.01)	(0.01)
Saturday	**0.12*****	**0.19*****	**0.18*****	**0.66*****	**0.28*****	**0.32*****	**0.32*****	**0.07*****	**0.07*****	**–0.25*****
	(0.002)	**(0.004)**	**(0.01)**	**(0.01)**	**(0.01)**	**(0.01)**	**(0.01)**	**(0.003)**	**(0.01)**	**(0.01)**
Sunday	–0.32***	–0.31***	–0.17***	–0.27***	–0.29***	–0.25***	0.02	–0.27***	–0.31***	–0.15***
	(0.003)	(0.005)	(0.01)	(0.01)	(0.01)	(0.01)	(0.02)	(0.004)	(0.01)	(0.01)
NN Gold_Mean *x* Polity	**0.002*****	**–0.03*****			**0.01*****		**0.01****	**–0.03*****	**0.07*****	
	(0.0001)	**(0.003)**			**(0.0004)**		**(0.004)**	**(0.001)**	**(0.01)**	
Constant	–4.49***	–13.75***	3,209.80***	–13,296.73***	–11.69***	–47,474.37***	1.86***	–5.99***	–0.67	–11,174.95***
	(0.03)	(0.20)	(77.65)	(104.99)	(0.47)	(976.82)	(0.20)	(0.10)	(0.65)	(337.85)
Observations	40,608	5,184	288	288	10,071	288	288	24,126	288	288
MAE	36.9	137.1	1,245.2	841.9	15.7	146.5	96.7	22.2	140.2	399.0
RMSE	581.0	1,309.9	4,466.3	1,905.6	118.9	250.5	323.0	202.8	432.0	1,176.5
AIC	2,512,547.6	1,174,295.0	414,419.0	364,709.0	192,375.2	33,555.2	37,022.5	767,059.7	35,507.4	108,732.1
Log Likelihood	–1,256,240.8	–587,117.5	–207,185.5	–182,330.5	–96,155.6	–16,753.6	–18,486.3	–383,496.8	–17,728.7	–54,342.1

Notes: *p<0.1; **p<0.05; ***p<0.01

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX F. ADDITIONAL CHARTS USED IN ANALYSIS

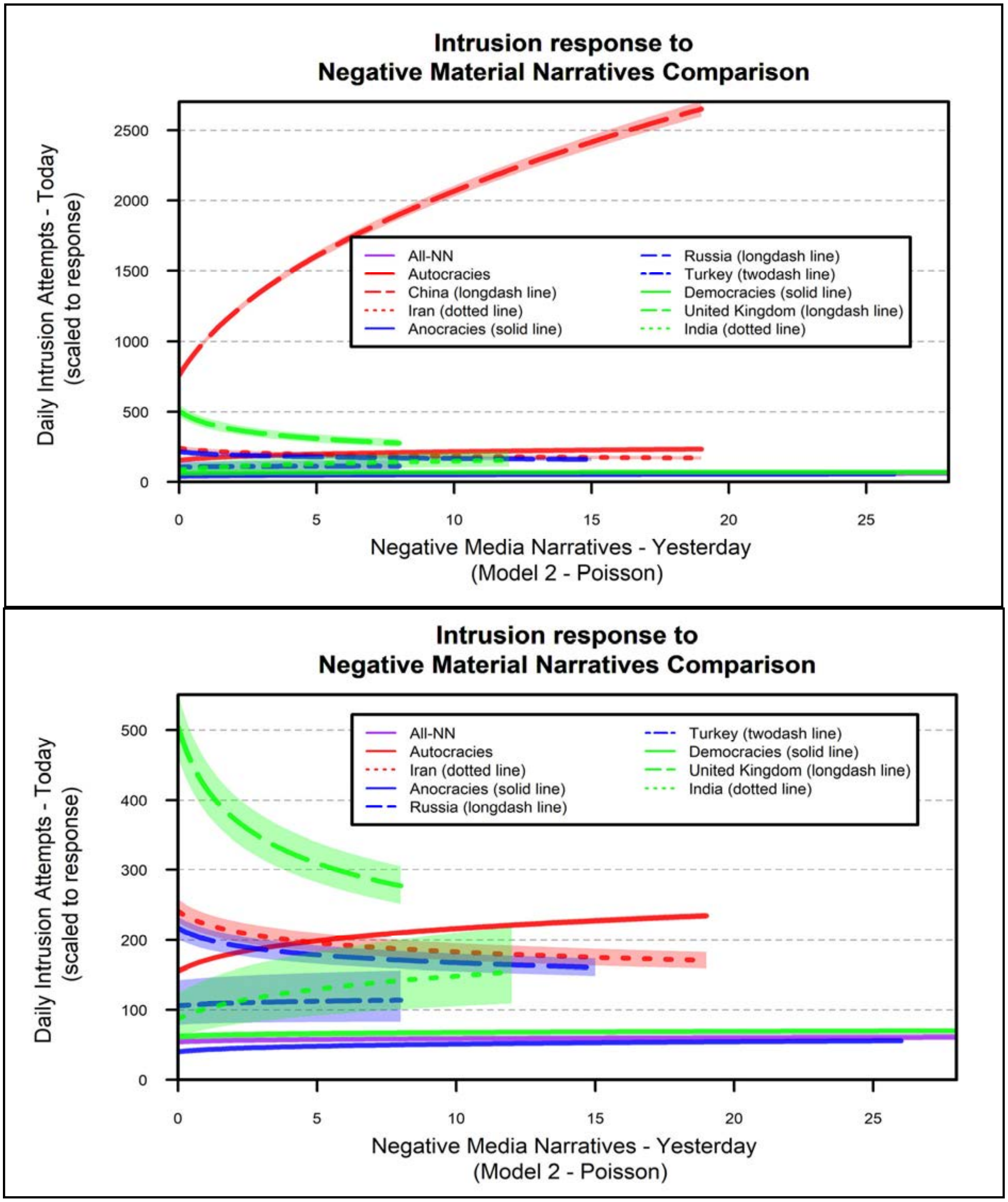


Figure 33. Coefficient Intrusion Prediction (Plot 1 & 2 [w/out China])

2 of 4

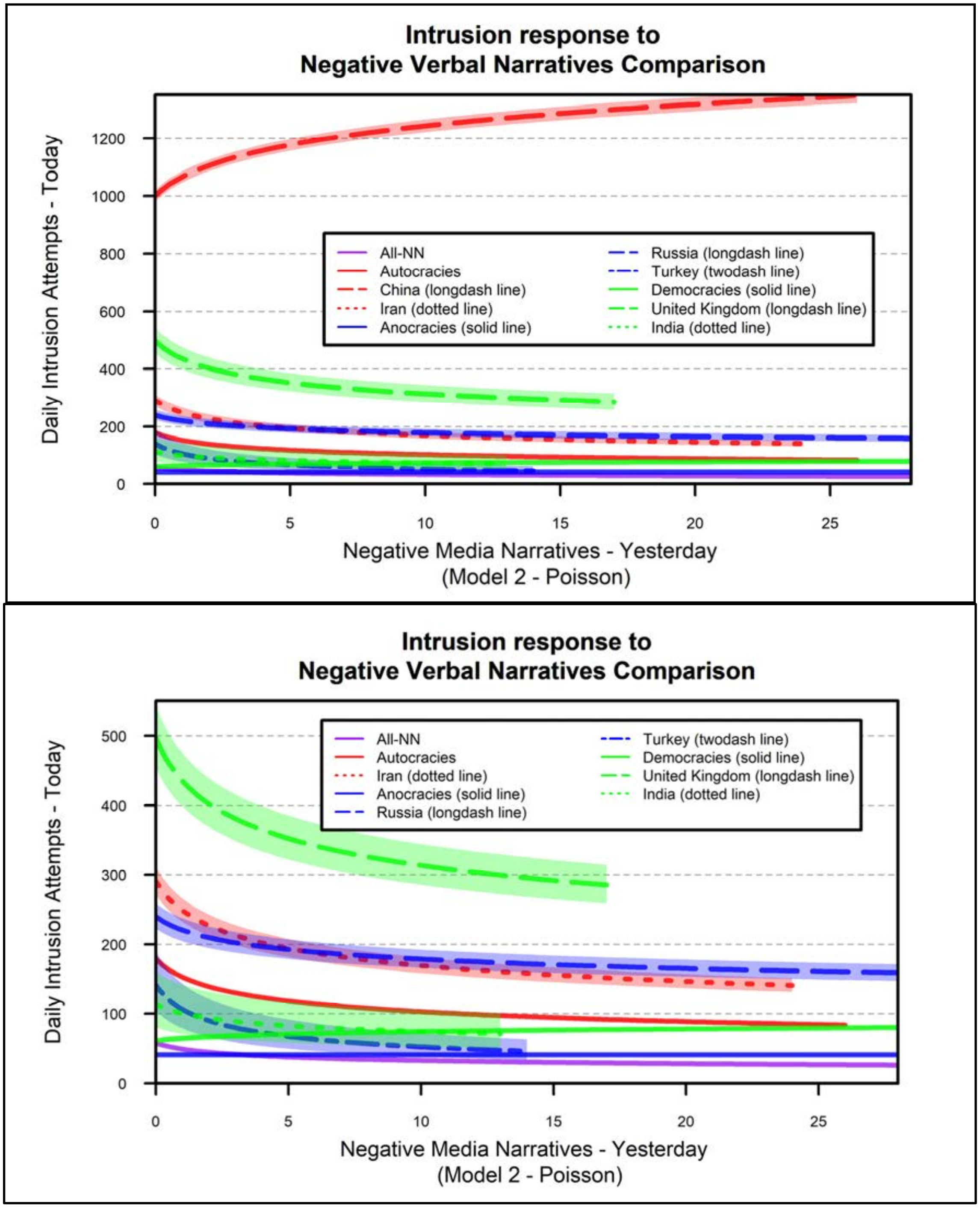


Figure 34. Coefficient Intrusion Prediction (Plot 3 & 4 [w/out China])

3 of 4

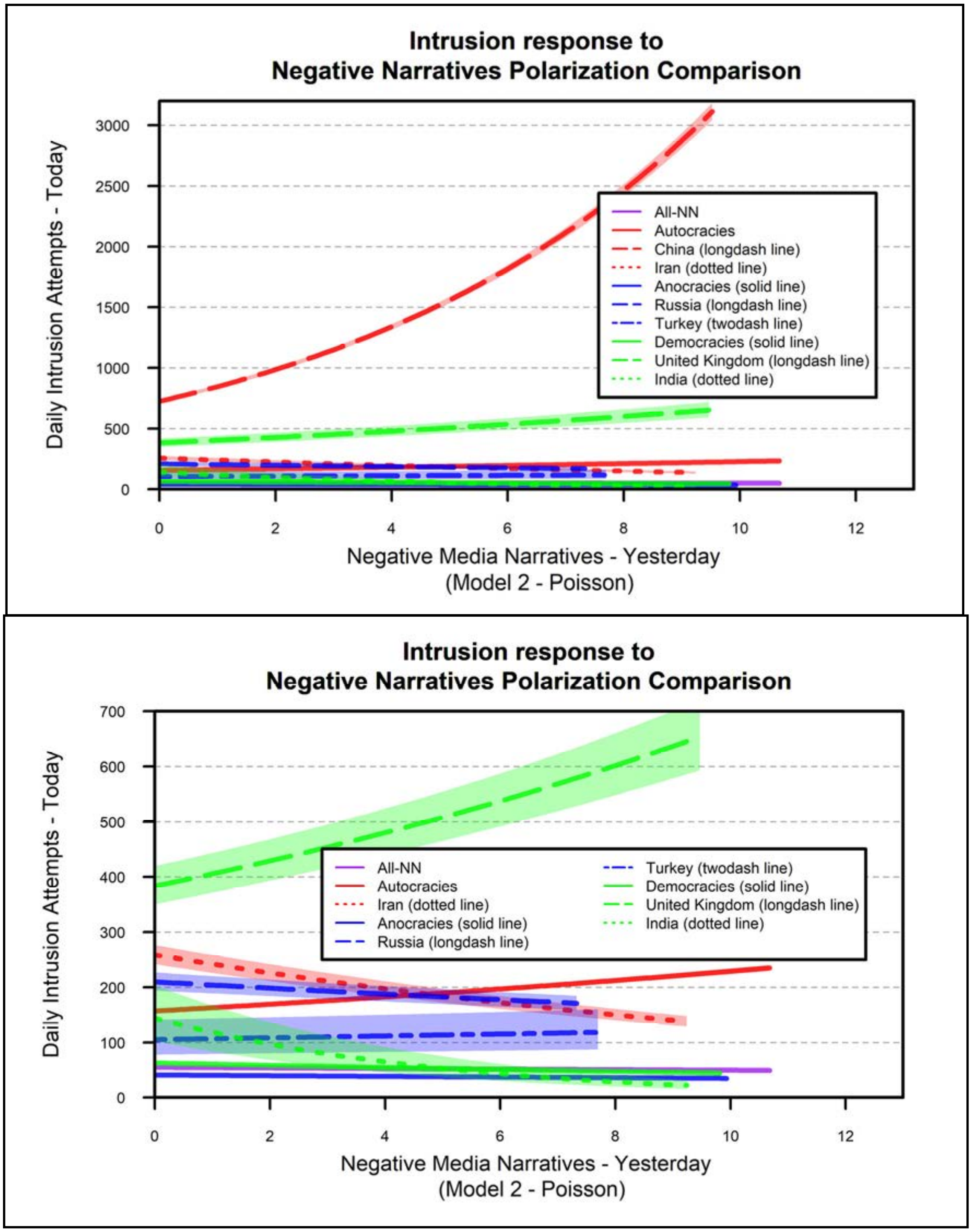


Figure 35. Coefficient Intrusion Prediction (Plot 5 & 6 [w/out China])

4 of 4

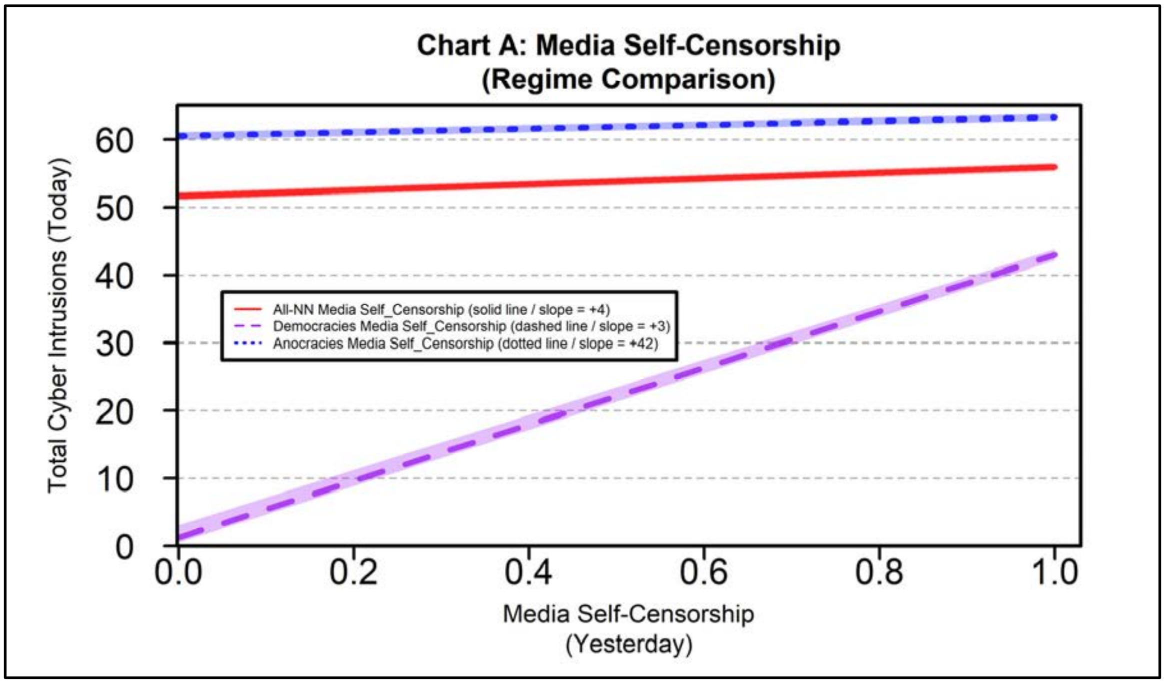


Figure 36. Self-Censorship Model Comparison

APPENDIX G. COUNTRIES INCLUDED IN THE ANALYSIS BY REGIME TYPE

Autocracies (19)

#	Country	Polity Score	PenRate	#	Country	Polity Score	PenRate
1	Azerbaijan	–7	0.790	11	Laos	–7	0.255
2	Bahrain	–10	0.980	12	Oman	–8	0.801
3	Belarus	–7	0.744	13	Qatar	–10	0.974
4	**China**	**–7**	0.543	14	Saudi Arabia	–10	0.942
5	Cuba	–7	0.571	15	Swaziland	–9	0.303
6	Eritrea	–7	0.013	16	Syria	–9	0.343
7	**Iran (Persia)**	**–7**	0.640	17	United Arab Emirates	–8	0.948
8	Kazakhstan	–6	0.764	18	Uzbekistan	–9	0.487
9	PRC, Korea	–10	0.010	19	Vietnam	–7	0.581
10	Kuwait	–7	0.980				

Anocracies (43)

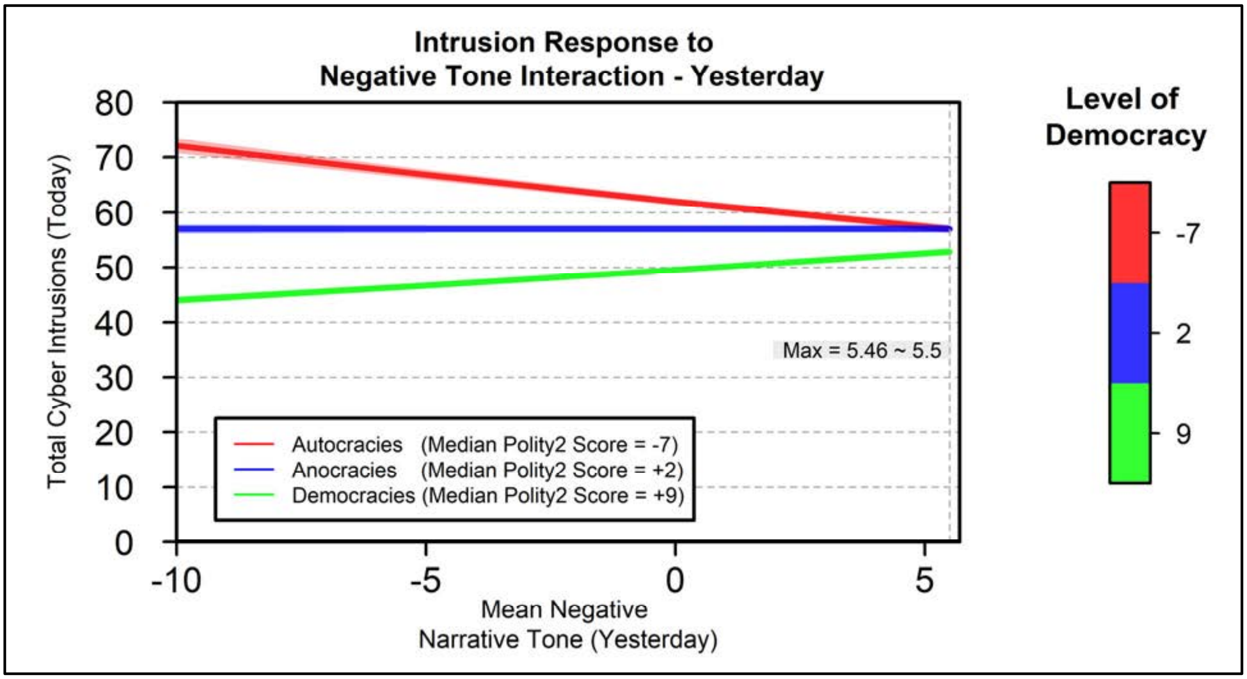
#	Country	Polity Score	Penrate	#	Country	Polity Score	Penrate
1	Afghanistan	–1	0.114	23	Mauritania	–2	0.208
2	Algeria	2	0.477	24	Morocco	–4	0.618
3	Angola	–2	0.143	25	Myanmar (Burma)	–3	0.217
4	Armenia	5	0.647	26	Niger	5	0.102
5	Bangladesh	1	0.180	27	Nigeria	4	0.360
6	Bhutan	5	0.418	28	Papua New Guinea	5	0.112
7	Burundi	–1	0.052	**29**	**Russia (Soviet Union)**	**4**	**0.760**
8	Cambodia (Kampuchea)	2	0.329	30	Rwanda	–3	0.218
9	Cameroon	–5	0.232	31	Singapore	–4	0.845
10	Chad	–1	0.065	32	Somalia	5	0.020
11	Congo, Rep of	–4	0.087	33	Sri Lanka (Ceylon)	4	0.121
12	DRC, Congo, (Zaire)	5	0.086	34	Sudan	–4	0.309
13	Cote D'Ivoire	4	0.438	35	Surinam	5	0.489
14	Djibouti	3	0.557	36	Tajikistan	–3	0.220
15	Ecuador	5	0.541	37	Tanzania/Tanganyika	3	0.200
16	Egypt	–4	0.450	38	Thailand	–3	0.529
17	Ethiopia	–3	0.186	**39**	**Turkey(Ottoman Empire)**	**3**	**0.647**
18	Gambia	4	0.198	40	Uganda	–1	0.237
19	Haiti	5	0.123	41	Ukraine	4	0.589
20	Jordan	–3	0.668	42	Venezuela	4	0.643
21	Malaysia	5	0.801	43	Zimbabwe (Rhodesia)	4	0.271
22	Mali	5	0.127				

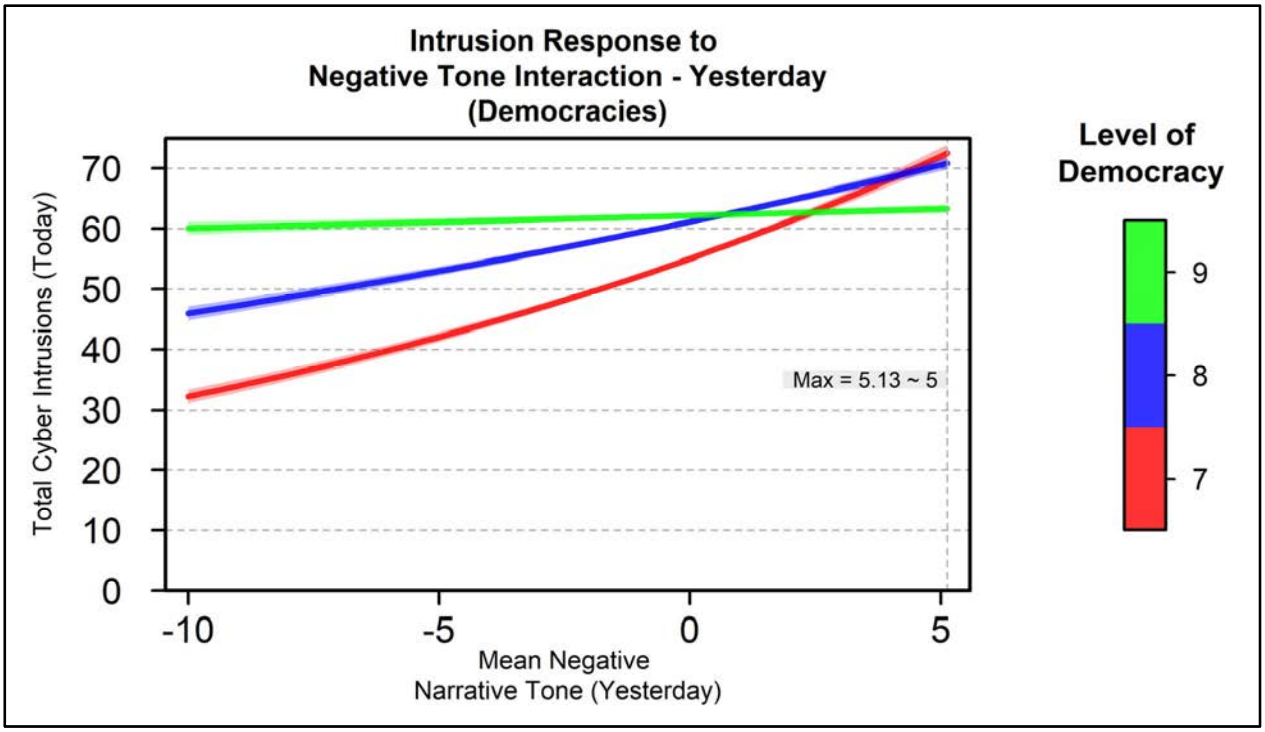
2 of 2

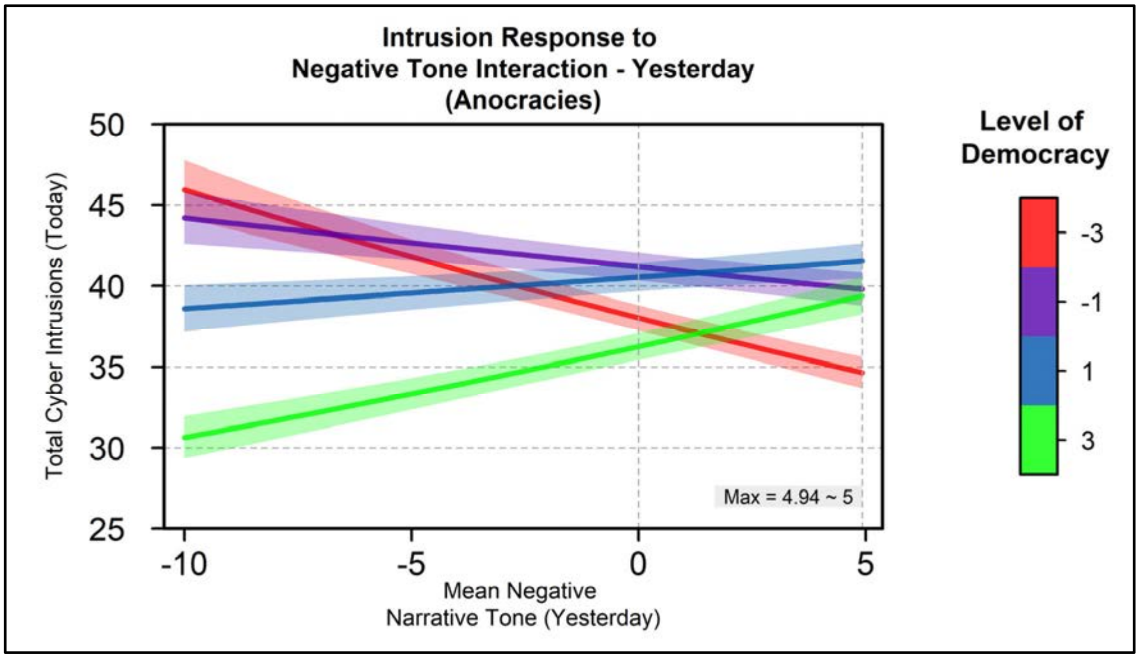
Democracies (88)

#	Country	Polity Score	Pen rate	#	Country	Polity Score	Pen rate	#	Country	Polity Score	Pen rate
1	Albania	9	0.72	*31*	Guatemala	8	0.41	*60*	Nicaragua	9	0.28
2	Argentina	9	0.74	*32*	Guyana	7	0.37	*61*	Niger	6	0.02
3	Australia	10	0.87	*33*	Honduras	7	0.32	*62*	Nigeria	7	0.26
4	Austria	10	0.88	*34*	Hungary	10	0.79	*63*	Norway	10	0.97
5	Belgium	8	0.88	***35***	**India**	**9**	**0.32**	*64*	Pakistan	7	0.17
6	Benin	7	0.14	*36*	Indonesia	9	0.32	*65*	Panama	9	0.60
7	Bolivia	7	0.44	*37*	Iraq	6	0.58	*66*	Paraguay	9	0.61
8	Botswana	8	0.41	*38*	Ireland	10	0.84	*67*	Peru	9	0.50
9	Brazil	8	0.67	*39*	Israel	6	0.82	*68*	Philippines	8	0.60
10	Bulgaria	9	0.63	*40*	Italy (Sardinia)	10	0.63	*69*	Poland	10	0.76
11	Burkina Faso	6	0.16	*41*	Jamaica	9	0.55	*70*	Portugal	10	0.74
12	Burundi	6	0.05	*42*	Japan	10	0.93	*71*	Rumania	9	0.64
13	Canada	10	0.93	*43*	Kenya	9	0.18	*72*	Senegal	7	0.30
14	Central African Republic	6	0.04	*44*	Korea, Republic of	8	0.95	*73*	Serbia	8	0.70
15	Chile	10	0.84	*45*	Kyrgyz Republic	7	0.38	*74*	Sierra Leone	7	0.13
16	Colombia	7	0.62	*46*	Latvia	8	0.80	*75*	Slovakia	10	0.82
17	Costa Rica	10	0.72	*47*	Lebanon	6	0.78	*76*	Slovenia	10	0.79
18	Croatia	9	0.73	*48*	Liberia	6	0.33	*77*	Solomon Islands	8	0.12
19	Cyprus	10	0.81	*49*	Lithuania	10	0.78	*78*	South Africa	9	0.56
20	Czech Republic	9	0.79	*50*	Macedonia (Yugoslavia)	9	0.75	*79*	Spain	10	0.85
21	Denmark	10	0.97	*51*	Mauritius	10	0.55	*80*	Sri Lanka (Ceylon)	6	0.34
22	Dominican Republic	8	0.68	*52*	Mexico	8	0.64	*81*	Sweden	10	0.93
23	El Salvador	8	0.34	*53*	Moldova	9	0.76	*82*	Switzerland	10	0.90
24	Estonia	9	0.88	*54*	Mongolia	10	0.24	*83*	Taiwan	10	0.88
25	Finland	10	0.88	*55*	Montenegro	9	0.71	*84*	Trinidad and Tobago	9	0.77
26	France	10	0.81	*56*	Namibia	6	0.37	*85*	Tunisia	7	0.56
27	Georgia	7	0.60	*57*	Nepal	6	0.21	***86***	**United Kingdom**	**8**	**0.95**
28	Germany	10	0.88	*58*	Netherlands	10	0.93	*87*	Uruguay	10	0.70
29	Ghana	8	0.38	*59*	New Zealand	10	0.91	*88*	Zambia	7	0.28
30	Greece	10	0.70								

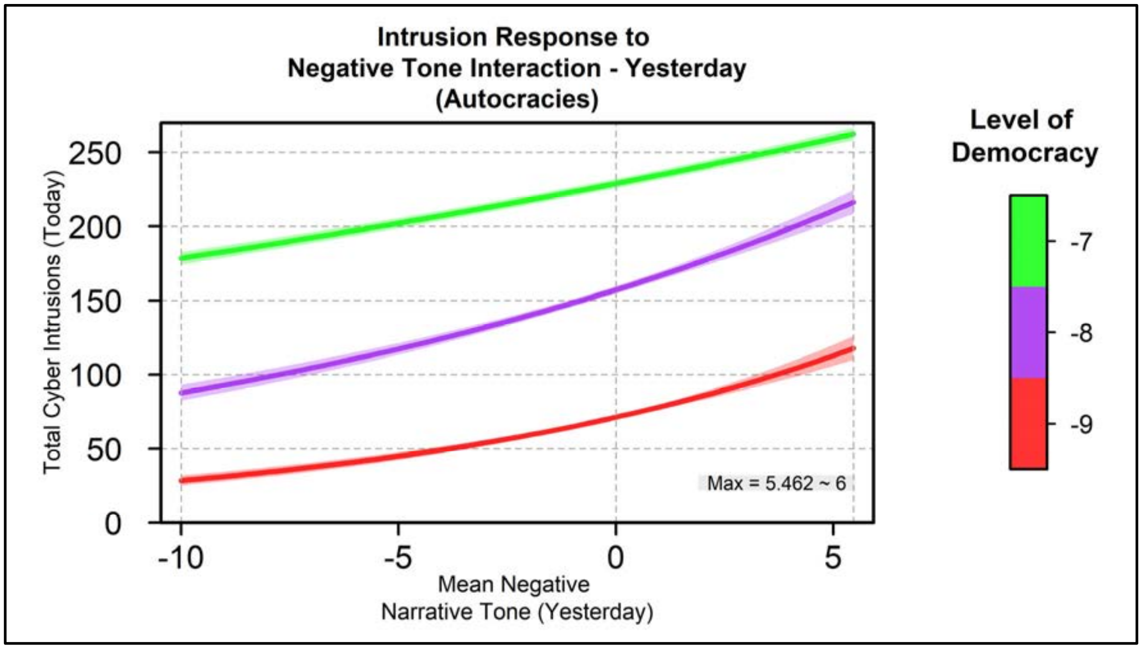
APPENDIX H. FIGURES COMPARING REGIME TYPE NEGATIVE NARRATIVE TONE TO LEVEL OF DEMOCRACY



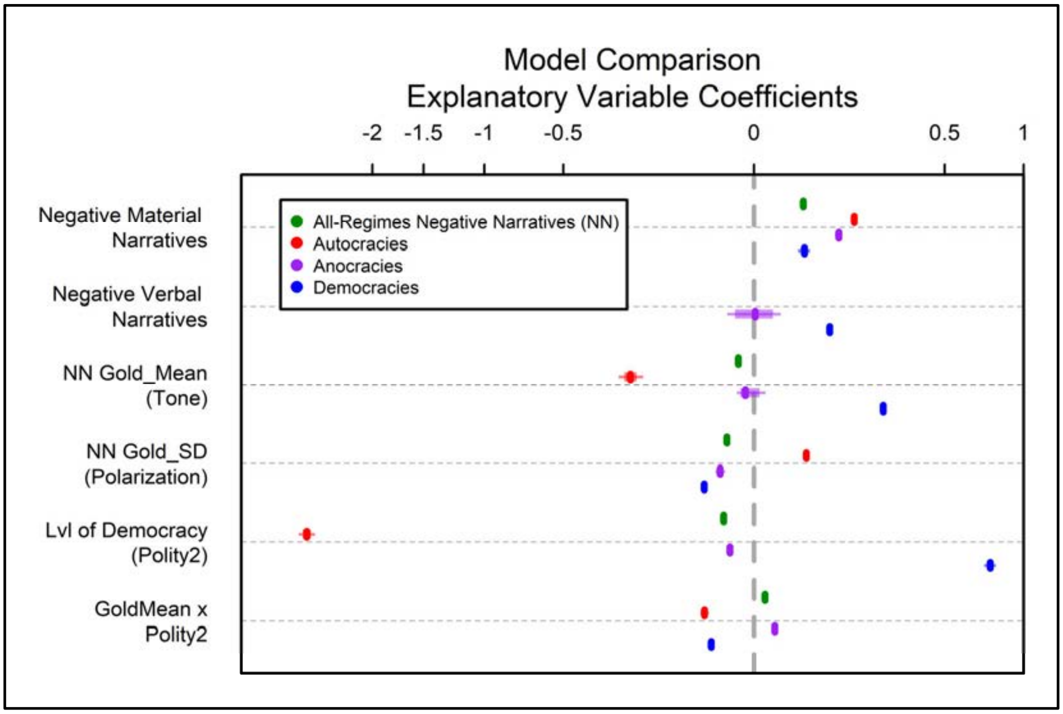


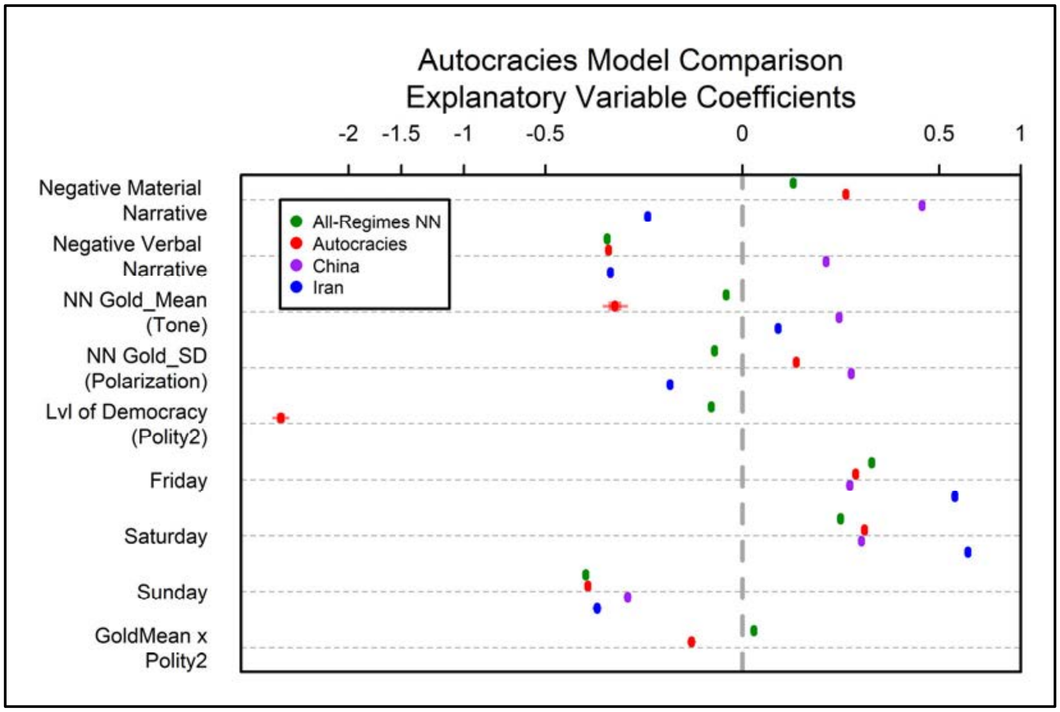

Intrusion Response to
Negative Tone Interaction - Yesterday
(Anocracies)
Total Cyber Intrusions (Today)
50
45
40
35
30
25
-10
-5
0
5
Mean Negative
Narrative Tone (Yesterday)
Max = 4.94 ~ 5
Level of
Democracy
-3
-1
1
3

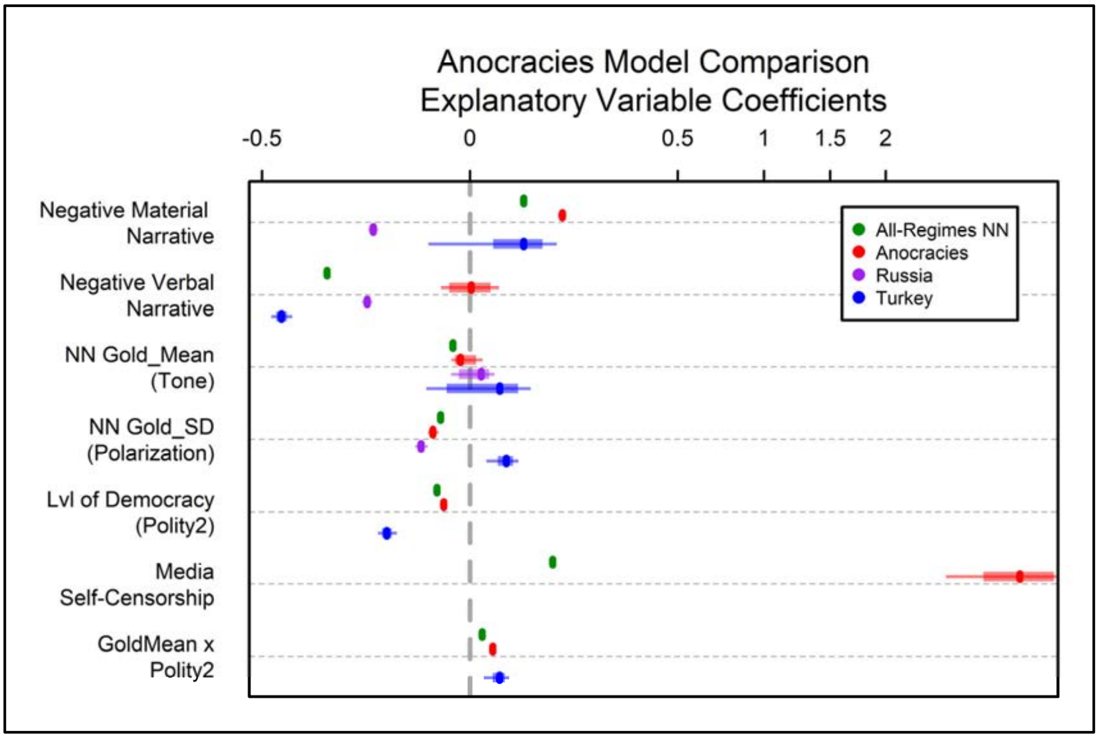
2 of 2

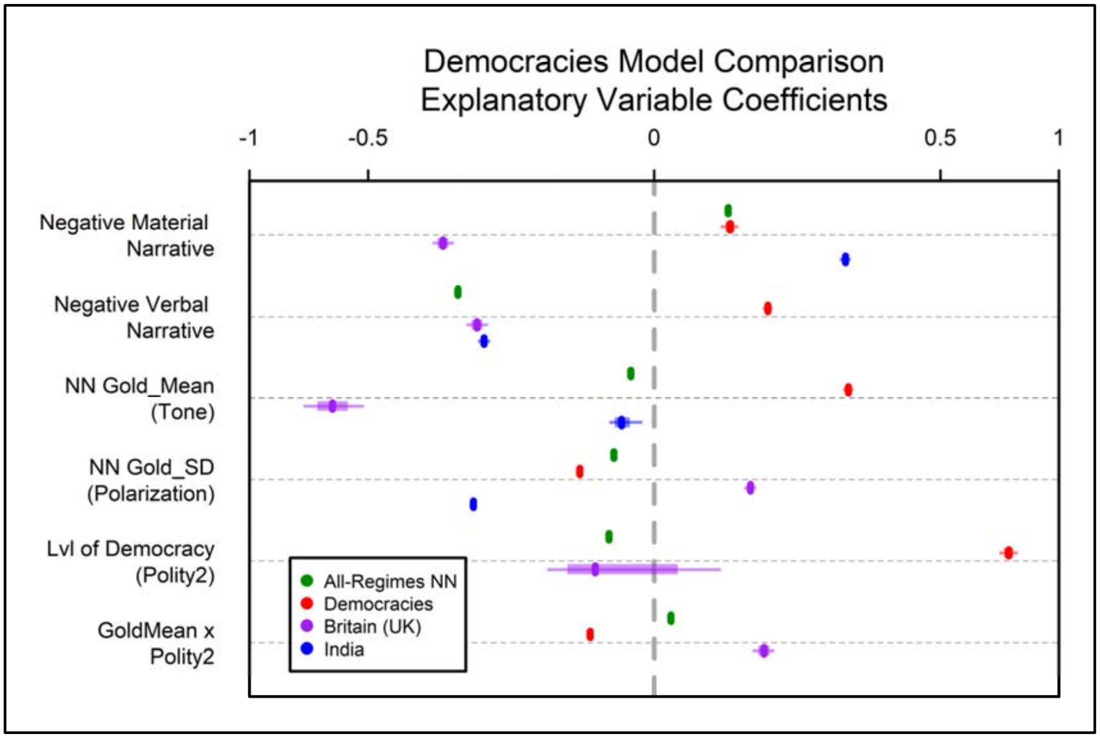

Intrusion Response to
Negative Tone Interaction - Yesterday
(Autocracies)
Total Cyber Intrusions (Today)
250
200
150
100
50
0
-10
-5
0
5
Mean Negative
Narrative Tone (Yesterday)
Max = 5.462 ~ 6
Level of
Democracy
-7
-8
-9

APPENDIX I. MODEL EXPLANATORY COEFFICIENT COMPARISON CHART



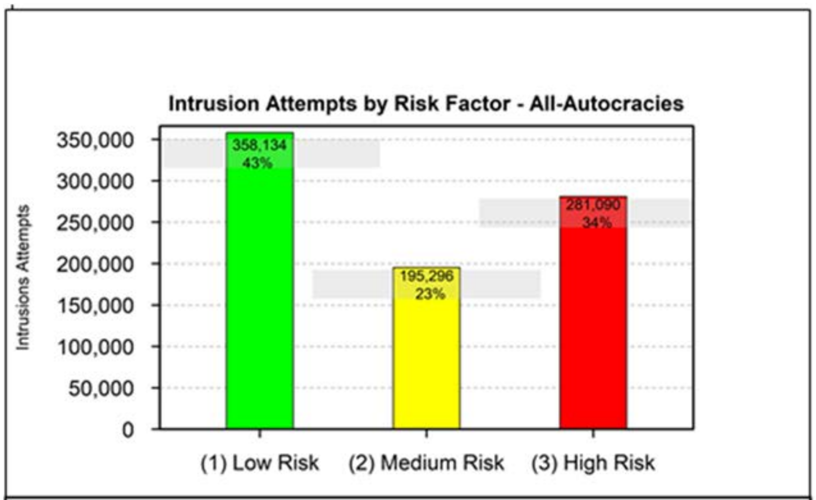


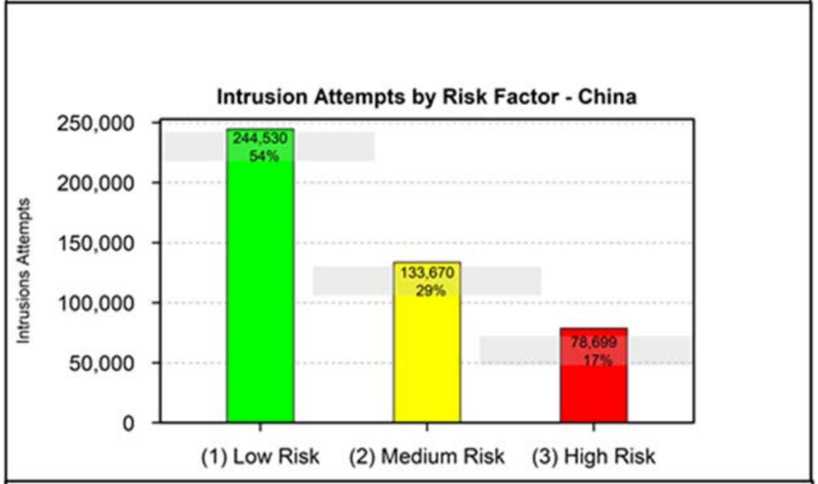

Anocracies Model Comparison
Explanatory Variable Coefficients
-0.5
0
0.5
1
1.5
2
Negative Material Narrative
Negative Verbal Narrative
NN Gold_Mean (Tone)
NN Gold_SD (Polarization)
Lvl of Democracy (Polity2)
Media Self-Censorship
GoldMean x Polity2
All-Regimes NN
Anocracies
Russia
Turkey

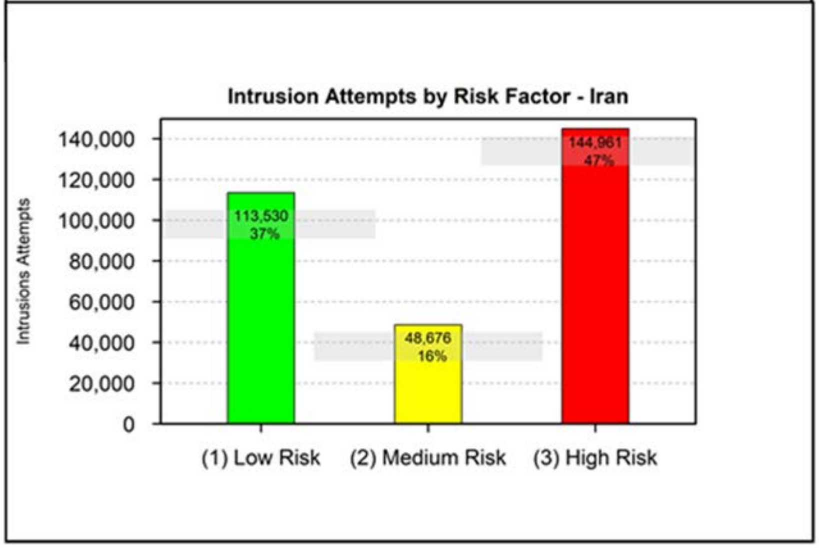

Democracies Model Comparison
Explanatory Variable Coefficients
-1
-0.5
0
0.5
1
Negative Material Narrative
Negative Verbal Narrative
NN Gold_Mean (Tone)
NN Gold_SD (Polarization)
Lvl of Democracy (Polity2)
GoldMean x Polity2
All-Regimes NN
Democracies
Britain (UK)
India

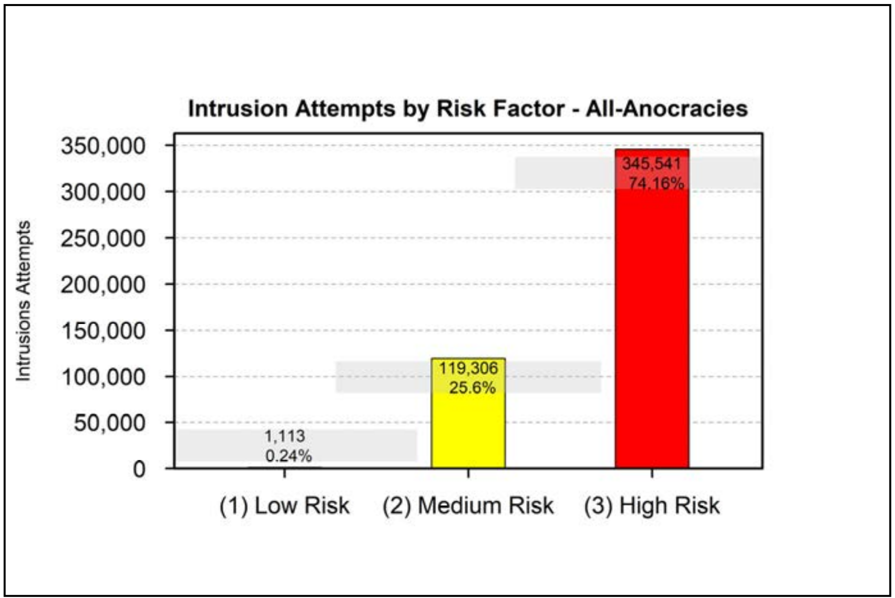
Page 2 of 2

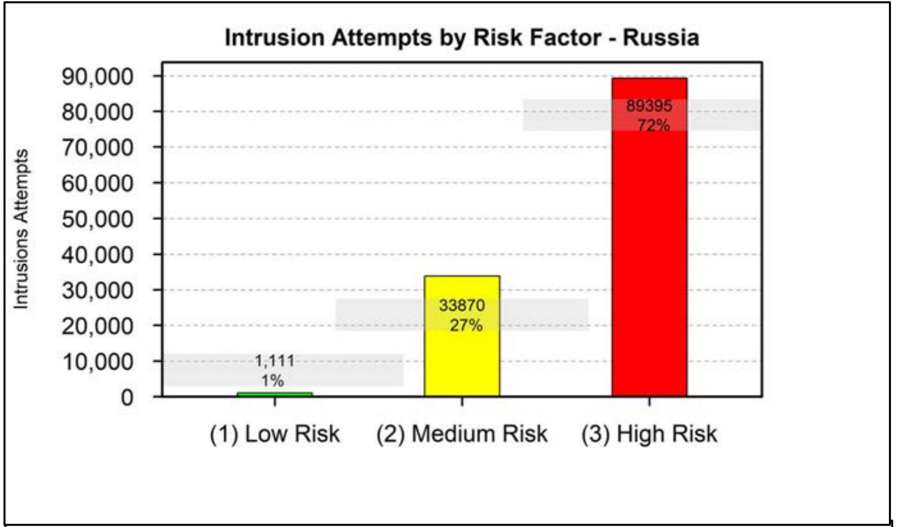
APPENDIX J. INTRUSION RISK FACTOR COUNTS BY REGIME AND COUNTRY

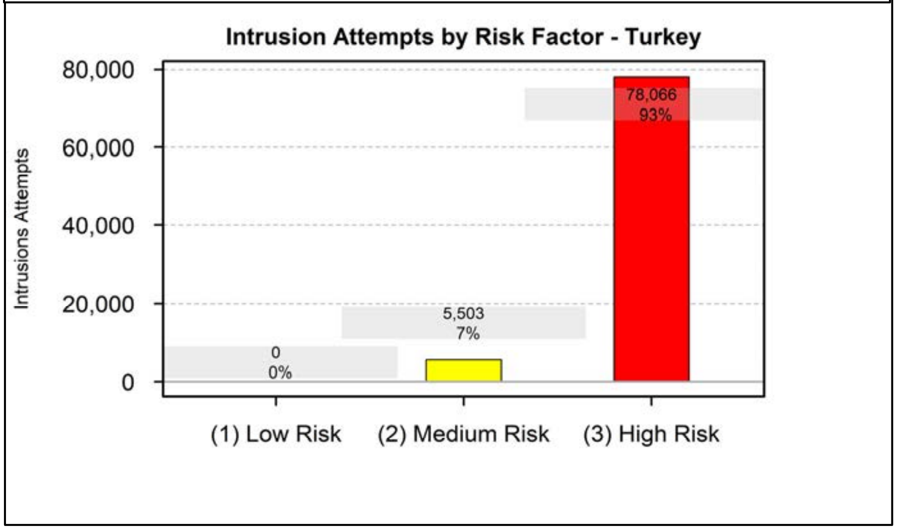


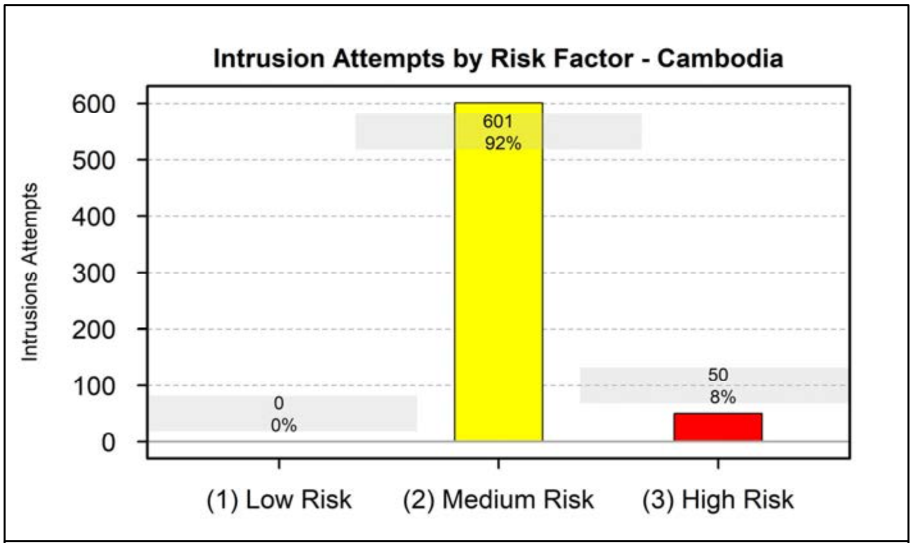


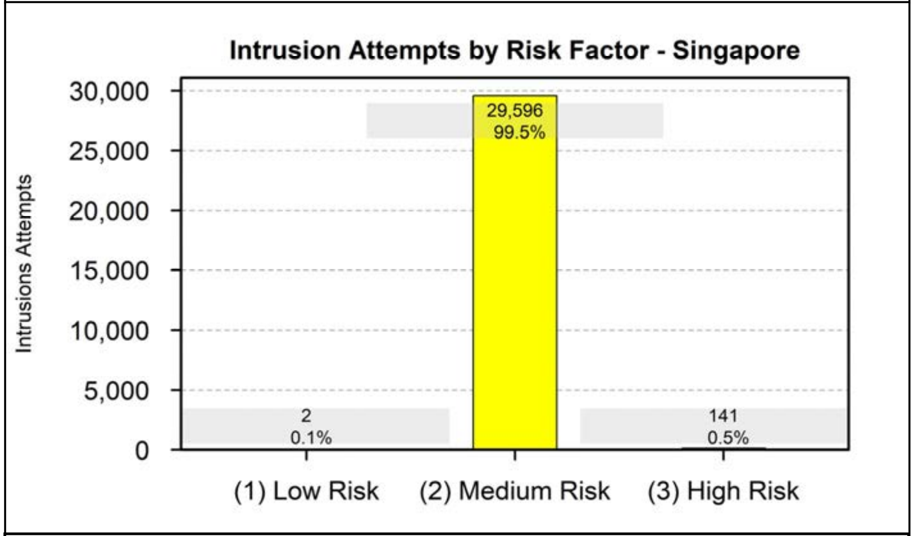


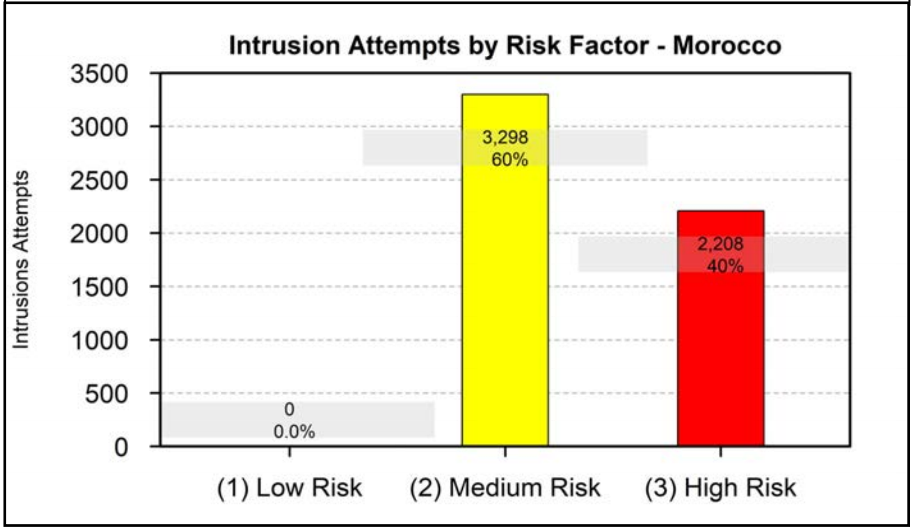

Intrusion Attempts by Risk Factor - All-Anocracies
Intrusions Attempts
350,000
300,000
250,000
200,000
150,000
100,000
50,000
0
1,113
0.24%
119,306
25.6%
345,541
74.16%
(1) Low Risk
(2) Medium Risk
(3) High Risk


Intrusion Attempts by Risk Factor - Russia
Intrusions Attempts
90,000
80,000
70,000
60,000
50,000
40,000
30,000
20,000
10,000
0
1,111
1%
33870
27%
89395
72%
(1) Low Risk
(2) Medium Risk
(3) High Risk

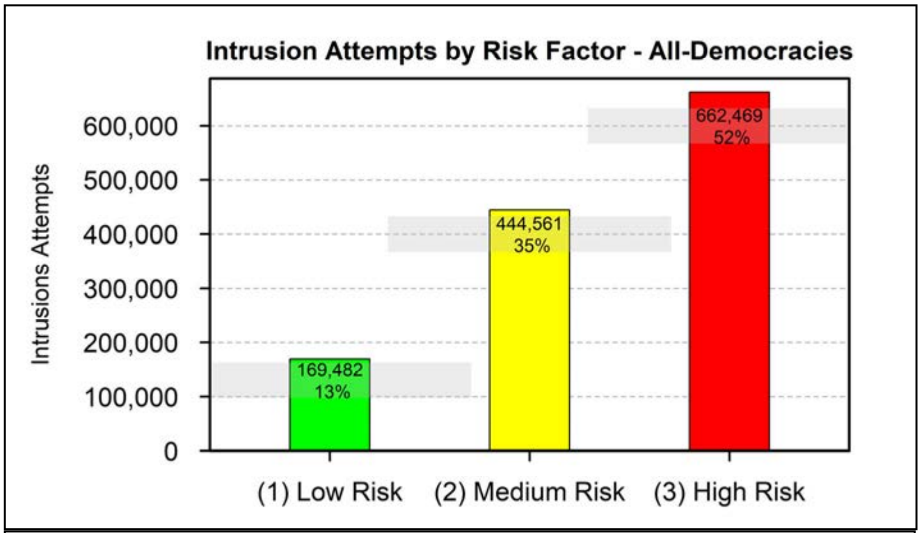

Intrusion Attempts by Risk Factor - Turkey
Intrusions Attempts
80,000
60,000
40,000
20,000
0
0
0%
5,503
7%
78,066
93%
(1) Low Risk
(2) Medium Risk
(3) High Risk

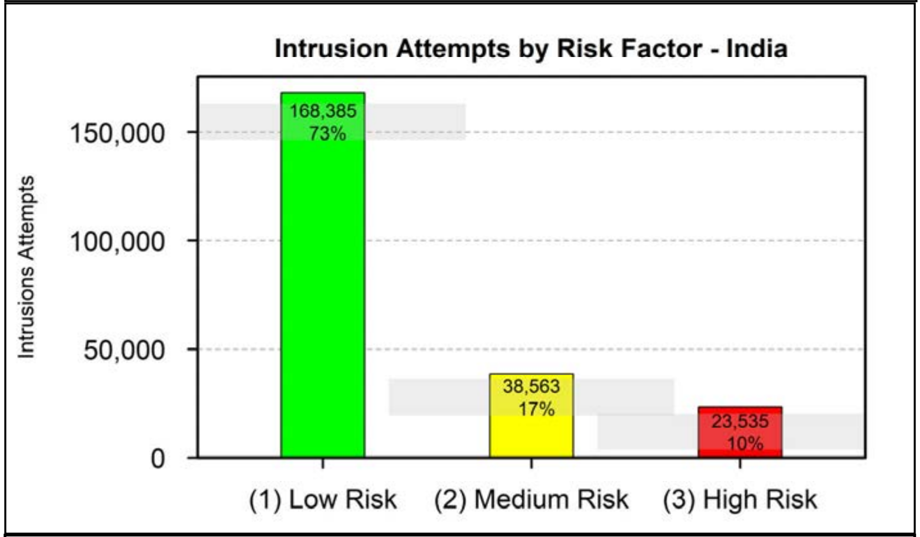

Intrusion Attempts by Risk Factor - Cambodia
Intrusions Attempts
600
500
400
300
200
100
0
601
92%
0
0%
50
8%
(1) Low Risk
(2) Medium Risk
(3) High Risk

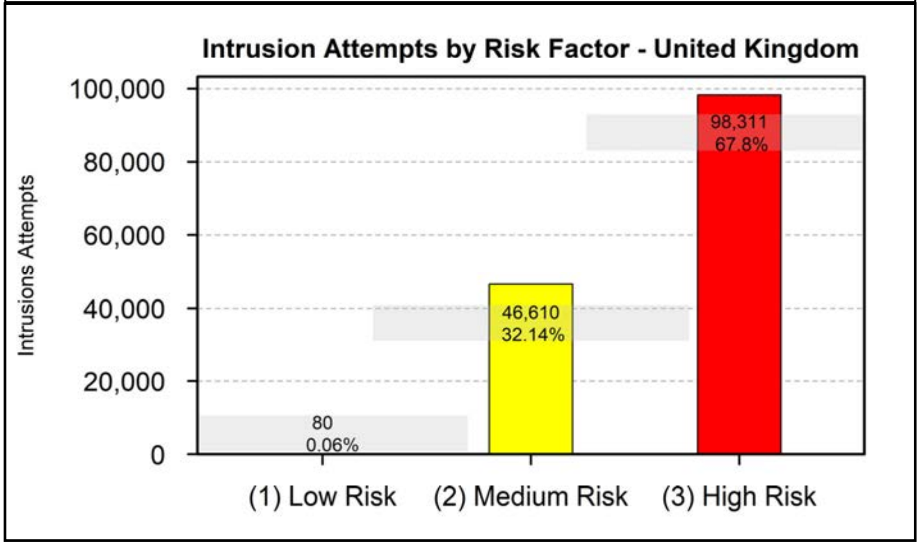

Intrusion Attempts by Risk Factor - Singapore
Intrusions Attempts
30,000
25,000
20,000
15,000
10,000
5,000
0
29,596
99.5%
2
0.1%
141
0.5%
(1) Low Risk
(2) Medium Risk
(3) High Risk


Intrusion Attempts by Risk Factor - Morocco
Intrusions Attempts
3500
3000
2500
2000
1500
1000
500
0
3,298
60%
2,208
40%
0
0.0%
(1) Low Risk
(2) Medium Risk
(3) High Risk

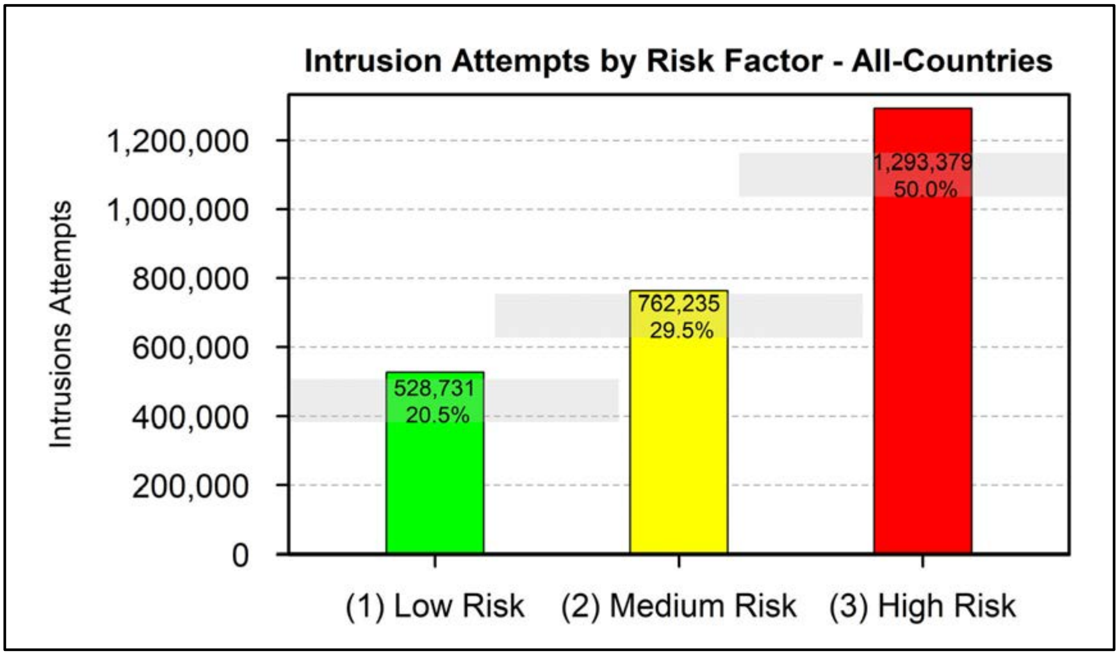
Page 4 of 5


Intrusion Attempts by Risk Factor - All-Democracies


Intrusion Attempts by Risk Factor - India


Intrusion Attempts by Risk Factor - United Kingdom

Page 5 of 5


Intrusion Attempts by Risk Factor - All-Countries
Intrusions Attempts
1,200,000
1,000,000
800,000
600,000
400,000
200,000
0
528,731
20.5%
762,235
29.5%
1,293,379
50.0%
(1) Low Risk
(2) Medium Risk
(3) High Risk

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF REFERENCES

Aelst, P. V. (2017). Media malaise and the decline of legitimacy: Any room for good news? In C. Van Ham, J. Thomassen, A. Kees, & A. Ruby B. (Eds.), *Explaining Trends and Cross-National Differences in Established Democracies* (pp. 95–114). Oxford: Oxford University Press.

Aftab, O., Cheung, P., Kim, A., Thakkar, S., & Yeddanapudi, N. (2002). *Information theory: Information theory and the digital age*. Boston: 6.933 Project History, Massachusetts Institute of Technology.

Akgül, M., & Kirlidoğ, M. (2015). Internet censorship in Turkey. *Internet Policy Review*, 4(2), 1–21.

Al Jazeera. (2016, July 15). Timeline: A history of Turkish coups. Retrieved from Al Jazeera: https://www.aljazeera.com/news/europe/2012/04/20124472814687973.html

Al Jazeera. (2018, January 2). Five things you need to know about protests in Iran. Doha, Qatar. Retrieved from https://www.aljazeera.com/news/2017/12/protests-iran-171231083620343.html

Alfoneh, A. (2010). The revolutionary guards' looting of Iran's economy. Washington, DC: American Enterprise Institute for Public Policy Research. Retrieved March 30, 2020, from https://www.jstor.org/stable/resrep03091

Altiparmak, K., & Gürol, S. (2017). Turkey's derogation of human rights under the state of emergency: Examining its legitimacy and proportionality. *Austrian Review of International and European Law, 22*(1), 101–136.

Anderson, C. (2013). Dimming the internet: Detecting throttling as a mechanism of censorship in Iran. *arXiv preprint arXiv:1306.4361*, 1–31.

Anderson, C., & Sadjadpour, K. (2018). *Iran's cyber threat: Espionage, sabotage, and revenge*. Washington, DC: Carnegie Endowment for International Peace.

Anderson, L. (1993). Gross Domestic Product. In D. R. Henderson, *The Fortune Encyclopedia of Economics* (pp. 203–207). New York: Warner Books, Inc.

Andriotis, A., & Minaya, E. (2017, September 8). Equifax reports data breach possibly affecting 143 Million U.S. consumers. *Wall Street Journal*.

Andriotis, A., Rapoport, M., & McMillian, R. (2017, September 18). We've been breached: Inside the Equifax hack. *The Wall Street Journal*.

Aneez, Z., Neyazi, T. A., Kalogeropoulos, A., & Nielsen, R. K. (2018). *India digital news report.* Oxford, England: Reuters Institute for the Study of Journalism.

Ansari, A. M. (2017). *Iran under Ahmadinejad: The politics of confrontation.* New York: Routledge.

Arango-Kure, M., Garz, M., & Rott, A. (2014). Bad news sells: The demand for news magazines and the tone of their covers. *Journal of Media Economics*, *27*(4), 199–214.

Arquilla, J., & Ronfeldt, D. (1993). Cyberwar is Coming! *Comparative Strategy*, 12(2), 141–165.

Arsan, E. (2013). Killing me softly with his words: Censorship and self-censorship from the perspective of Turkish journalists. *Turkish Studies*, 14(3), 447–462.

Aryan, S., Aryan, H., & Halderman, J. A. (2013). Internet censorship in Iran: A first look. *3rd USENIX Workshop on Free and Open Communications on the Internet* (p. 8). Washington, DC: National Science Foundation.

Asmolov, G. (2016). Dynamics of innovation and the balance of power in Russia. In M. M. Hussain (Ed.), *State Power 2.0: Authoritarian Entrenchment and Political Engagement Worldwide* (2d ed., pp. 139–152). Burlington, Vermont: Routledge.

Axelrod, R., & Iliev, R. (2014). Timing of cyber conflict. *Proceedings of the National Academy of Sciences*, *111(4)*, (pp. 1298–1303). Ann Arbor: National Academy of Sciences.

Baarda, R. (2017). Digital democracy in authoritarian Russia: Opportunity for participation, or site of Kremlin control? In R. Luppicini, & R. Baarda (Eds.), *Digital Media Integration for Participatory Democracy*. Hershey, PA: IGI Global.

Baharan, B. (2009). *Iran / death penalty: A state terror policy.* Paris: International Federation for Human Rights.

Ball, D. (2011). China’s cyber warfare capabilities. *Security Challenges*, 7(2), 81–103.

Ball-RoKeach, S. J., & DeFleur, M. L. (1976). Mass-media effects. *Communications Research*, 3(1), 3–21.

Balsiger, J. (2007). Social movement theory. In M. Bevir, *Encyclopedia of Governance* (pp. 889–892). Thousand Oaks: Sage Publishing, Inc.

Barabasi, A.L. (2003). *Linked.* New York: First Plume Printing.

———. (2016). *Network Science.* Cambridge: Cambridge University Press.

Barbatsis, G. (2004). Narrative. In K. L. Smith (Ed.), *Handbook of Visual Communication: Theory, Methods, and Media* (pp. 329–349). London and New York: Routledge.

Bardakçi, M. (2013). Coup plots and the transformation of civil-military relations in Turkey under AKP Rule. *Turkish Studies*, 14(3), 411–428.

Barme, E. R., & Ye, S. (1997, June 01). The great firewall of China. Retrieved from Wired: https://www.wired.com/1997/06/china-3/

Bass, T. (2000). Intrusion detection systems and multisensor data fusion. *Communication of the Association for Computing Machinery (ACM)*, 43(4), 99–105.

Baum, M. A., & Zhukov, Y. (2015). Filtering revolution. *Journal of Peace Research*, 52(3), 384–400.

Baum, M. A., & Zhukov, Y. M. (2019). Media ownership and news coverage of international conflict. *Political Communication*, 36(1), 36–63.

Bayat, A. (2005). Islamism and social movement theory. *Third World Quarterly*, 26(6), 891–908.

BBC. (2009, February 06). Warning over "surveillance state." Retrieved from British Broadcasting Corporation (BBC) News: http://news.bbc.co.uk/2/hi/uk_news/politics/7872425.stm.

———. (2017, May 23). Cyber-attack: Europol says it was unprecedented in scale. *British Broadcasting Corporation (BBC)*.

Beale, J., Foster, J. C., Posluns, J., & Caswell, B. (2003). *Snort 2.0 Intrusion Detection.* Rockland, Massachusetts: Syngress Publishing, Inc.

Beaumont, P. (2007, September 15). *The Guardian.* Retrieved from Was Israeli raid a dry Run for attack on Iran?, https://www.theguardian.com/world/2007/sep/16/iran.israel.

Beaver, K. (2018, March 26). Distributed denial of service (DDOS). Retrieved from SearchNetworking: http://searchsecurity.techtarget.com/definition/distributed-denial-of-service-attack.

Benford, R. D., & Snow, D. A. (2000). Framing processes and social movements : An Overview and Assessment. *Annual Review Sociology*, 26(2000), 611–639.

Bennett, W. L. (1990). Toward a theory of press-state relations in the United States. *Journal of Communication*, 40(2), 103–127.

Bentham, J. (2012). Chapter II: The Panopticon. In P. Priestley, & M. Vanstone (Eds.), *Offenders or Citizens? Readings in Rehabilitation* (pp. 166–18). New York: Taylor & Francis.

Best, H., & Higley, J. (Eds.). (2018). *The Palgrave Handbook of Political Elites.* London: Palgrave MacMillian.

Bi, S. G. (2015). A contrast of the degree of activity among the three major powers, USA, China, and Russia: Insights from media reports. . *2015 International Conference on Behavioral, Economic and Socio-Cultural Computing, BESC 2,* (pp. 38–42). Nanjing.

Biçakci, S., Doruk, E., & Mitat, Ç. (2015). The Cyber Security Scene in Turkey. In *A Primer on Cyber Security in Turkey and the Case of Nuclear Power* (pp. 22–51). Istanbul, Turkey: Centre for Economics and Foreign Policy Studies (EDAM).

Bilgiç, A. (2018). Reclaiming the National Will: Resilience of Turkish Authoritarian Neoliberalism after Gezi. *South European Society and Politics*, 23(2), 259–280.

Bjola, C., & Manor, I. (2018). Revisiting Putnam's two-level game theory in the digital age: domestic digital diplomacy and the Iran nuclear deal. *Cambridge Review of International Affairs*, 31(1), 3–32.

Black, P. E., Scrafone, K., & Souppaya, M. (2008). Cyber Security Metrics and Measures. In J. G. Voeller, *Wiley Handbook of Science and Technology for Homeland Security* (pp. 1–9). Wiley and Sons, Inc.

Blout, E. L. (2017). Soft war: Myth, nationalism, and media in Iran. *Communications Review*, 20(3), 212–224.

Botsman, R. (2017, October 21). Big data meets Big Brother as China moves to rate its citizens. *Wired*. Retrieved September 15, 2020, from https://www.wired.co.uk/article/chinese-government-social-credit-score-privacy-invasion

Brambor, T., Clark, W. R., & Golder, M. (2006). Understanding interaction models: improving empirical analyses. *Political Analysis*, 14(1), 63–82.

Brandt, P. T., Colaresi, M., & Freeman, J. R. (2008). The dynamics of reciprocity, accountability, and credibility. *Journal of Conflict Resolution*, 52(3), 343–374.

Buckley, W. F. (2004). *The Fall of the Berlin Wall.* Hoboken, NJ: John Wiley & Sons, Inc.

Bull, H. (2012). *The Anarchical Society* (4th ed.). New York: Columbia University Press.

Caerus, A. (2015). Phoenix event data set codebook (0.0.1b). Retrieved from Phoenix Data Project: https://s3.amazonaws.com/oeda/docs/phoenix_codebook.pdf

Calamur, K. (2017, June 1). Putin says ‘patriotic hackers’ may have targeted U.S. election. Retrieved from The Atlantic: URL: https://www.theatlantic.com/news/archive/2017/06/putin-russia-us-election/528825/

Capra, F. (1996). *Web of Life: A Scientific Understanding of Living Systems.* New York: Random House.

Carrieri, M., Deibert, R. J., & Khan, S. O. (2016). Information Infrastructure and Anti-Regime Protests in Iran and Tunisia. In M. M. Hussain, & P. N. Howard (Eds.), *State Power 2.0: Authoritarian Entrenchment and Political Engagement Worldwide* (2d ed., pp. 1–208). Burlington, Vermont: Routledge.

Carroll, W. K., & Hackett, R. A. (2006). Democratic media activism through the lens of social movement theory. *Media, Culture, & Society*, 28(1), 83–104.

Carter, A. (2015). *Department of Defense Cyber Strategy.* Washington, DC: Department of Defense.

Case, D. O., & Given, L. M. (2016). *Looking for information: A survey of research on information seeking* (Fourth ed.). (J.–E. Mai, Ed.) Bingley, UK: Emerald Publishing.

Castillo, C., El-Haddad, M., Pfeffer, J., & Stempeck, M. (2014). Characterizing the Life Cycle of Online News Stories using Social Media Reactions. *Proceedings of the Association of Computing Machinery (ACM) Conference on Computer Supported Cooperative Work (CSCW)* (pp. 211–223). Baltimore: Association of Computing Machinery.

Cavusoglu, H., Mishra, B., & Raghunathan, S. (2005). The Value of Intrusion Detection Systems. *Information Systems Research*, 16(1), 28–46.

Chairman of the Joint Chiefs of Staff. (2016). *Joint Publication 1–02, Department of Defense Dictionary of Military and Associated Terms* (15 February 2016 ed.). Arlington: United States Department of Defense. Retrieved August 13, 2018, from https://fas.org/irp/doddir/dod/jp1_02.pdf

Chakchouk, M., Kehl, D., Ben-Avie, J., & Coyer, K. (2013). From revolution to reform: Recommendations for spectrum policy in transitional Tunisia. *Journal of Information Policy*, 3(2013), 575–600.

Chesterman, S. (2011). *One Nation under Surveillance : A New Social Contract to Defend Freedom Without Sacrificing Liberty.* New Haven and London: Oxford University Press.

Choo, K.–K. R. (2011). The cyber threat landscape: Challenges and future research directions. *Computers and Security*, 30(8), 719–731.

Choucri, N. (2012). *Cyberpolitics in International Relations.* Cambridge: MIT Press.

CIA. (2019, December 2). The World fact book. Retrieved from Central Intelligence Agency (CIA): https://www.cia.gov/library/publications/the-world-factbook/

Cichonski, P., Millar, T., Grance, T., & Scarfone, K. (2012). *Computer Security Incident Handling Guide: Recommendations of the National Institute of Standards and Technology, 800–61. Revision 2.* Washington: National Institute for Standards and Technology.

Clapper, J. R. (2013). *Worldwide Threat Assessment to the Senate Select Committee on Intelligence.* Washington, DC: Director of National Intelligence.

Clarke, R. A. (1988). Information technology and dataveillance. *Communications of the ACM*, 31(5), 498–512.

Clarke, R. A., & Knake, R. K. (2010). *Cyberwar.* New York: HarperCollins .

———. (2019). *The Fifth Domain: Defending our Country, Our Companies, and Ourselves in the Age of Cyber Threats.* New York: Penguin Press.

Clinton, W. J. (1996). Executive Order 13010 – Critical Infrastructure Protection. Washington, DC, USA: Office of the Federal Register.

Colaresi, M. (2004). When doves cry: International rivalry, unreciprocated cooperation, and leadership turnover. *American Journal of Political Science*, 48(3), 555–570.

Colomer, J. M., Banerjea, D., & Mello, F. B. (2016). To democracy Through anocracy. *Democracy & Society*, 13(1), 19–25.

Comer, D. (2015). *Computer Networks and Internets.* Pearson.

Comer, D. E., & Stevens, D. L. (1993). *Vol III: Client-Server Programming and Applications. Internetworking with TCP/IP.* West Layfayette, IN: Prentice Hall.

Committee on National Security Systems. (2015, April 06). National Institute for Standards and Technology. Retrieved from Committee on National Security Systems(CNSS): https://www.cnss.gov/CNSS/openDoc.cfm?cMhq7WLTeeIZ1qjJ+rHk5w==

Conceição-Heldt, E. d., & Mello, P. A. (2017). Two-Level Games in Foreign Policy Analysis. In *Oxford Research Encyclopedia of Politics* (pp. 1–33). New York and Oxford: Oxford University Press.

Cong, X. (2013). Road to revival: A new move in the making of legitimacy for the ruling party in China. *Journal of Contemporary China*, 22(83), 905–922.

Connolly, O. (1979). *The French Revolution and the Napoleonic Era.* New York: Holt, Rinehart, and Winson.

Cook, S. (2019, November 13). State-Led Content Manipulation Drove the Backlash Against the NBA in China. *Freedom House, Freedom at Issue blog*. Retrieved from https://freedom- house.org/blog/state-led-content-manipulation-drove-backlash-against-nba-china.

Cotta, M. (2018). Elite dynamics and dilemmas. In H. Best, & J. Higley (Eds.), *The Palgrave Handbook of Political Elites* (pp. 1–661). London: Springer. Retrieved from https://link.springer.com/content/pdf/10.1057/978–1–137–51904–7.pdf

Crabtree, C., Darmofal, D., & Kern, H. L. (2015). A spatial analysis of the impact of West German television on protest mobilization during the East German revolution. *Journal of Peace Research*, 52(3), 269–284.

Creemers, R. (2018). *China's Social Credit System: An evolving practice of control.* Leiden, Netherlands: University of Leiden.

Creswell, J. W. (2014). *Research Design: Qualitative, Quantitative, and Mixed Methods Approaches, 4th Edition.* Thousand Oaks: Sage Publishing.

Cronin, A. K. (2002). Behind the curve: Globalization and international terrorism. *International Security*, 27(3), 30–58.

Custer, S., Prakash, M., Solis, J. A., Knight, R., & Lin, J. J. (2019). *Influencing the narrative : How the Chinese government mobilizes students and media to burnish its image.* Washington, DC: U.S. Department of State.

Czosseck, C., Ottis, R., & Taliharm, A.–M. (2013). Estonia after the 2007 Cyber Attacks: Legal, strategic, and organizational changes in cyber security. In M. Warren, *Case Studies in Information Warfare and Security* (pp. 72–91). London: Saffon House.

De Tocqueville, A. (1856). *The Old Regime and the Revolution.* (J. Bonner, Trans.) New York: Harper and Brothers, Publishers.

———. (1955). *The Old Regime and the French Revolution.* (S. Gilbert, Trans.) Garden City: Double Day and Company, Inc.

———. (2002). *Democracy in America* (Vol. 1 & 2). (H. Reeves, Trans.) University Park: Penn State University.

Dedeoglu, B. (2016). Turkey and the West after the Failed Coup: Possible Scenarios. *Insight Turkey*, 18(3), 31–42.

DeFleur, M. L., & Dennis, E. E. (1981). *Understanding mass communication.* Boston: Houghton Mifflin.

Deibert, R. (2015). Cyberspace under siege. *Journal of Democracy*, 26(3), 64–78.

Deibert, R. J. (2013). *Black Code: Surveillance, privacy, and the dark side of the internet.* Toronto: Random House.

Deibert, R., & Rohozinski, R. (2010). *Access controlled: The shaping of power, rights, and rule in cyberspace.* Cambridge, Massuchusetts & London, England: MIT Press.

Denning, D. E. (2001). Activism, hacktivism, and cyberterrorism: The internet as a tool for influencing foreign policy. *Networks and Netwars: The Future of Terror, Crime, and Militancy*, (pp. 239–288). Washington, DC.

———. (2011). Cyber Conflicts as an Emergent Social Phenomenon. In T. J. Holt, & B. H. Schell, *Corporate Hacking and Technology-Driven Crime: Social Dynamics and Implications* (pp. 170–186). Hershey, PA: Information Science Reference.

Denning, P. J., & Denning, D. E. (2010). The profession of IT discussing cyber attack. *Communications of the Association of Computing Machinery (ACM)*, 53(9), 29–31.

Dervin, B., & Naumer, C. M. (2009). Sense-Making. In S. Littlejohn, & K. Foss (Eds.), *Encyclopedia of Communication Theory.* Thousand Oaks: SAGE Publishing Inc.

Diamond, L. (1994). Rethinking civil society: Toward democratic consolidation. *Journal of Democracy*, 5(3), 4–17.

———. (2010). Liberation technology. *Journal of Democracy*, 21(3), 69–83.

———. (2015). Liberation technology. In *In Search of Democracy* (pp. 132–146). New York: Routledge.

———. (2018). *Chinese influence & American interests: Promoting constructive vigilance.* Palo Alto: Hoover Institute.

Diehl, P. F., & Goertz, G. (2001). *War and peace in international rivalry.* Ann Arbor: University of Michigan Press.

Dixon, P. (2017). A failure to do no harm – India's Aadhaar biometric ID program and its inability to protect privacy in relation to measures in Europe and the U.S. *Health Technology*, 7(4), 539–567.

Duffy, N. (2015). Internet freedom in Vladimir Putin's Russia : The noose tightens. *American Enterprise Institute*, 1–12.

Duindam, J. (2018). Pre-modern power elites: Princes, courts, intermediaries. In H. Best, & J. Higley (Eds.), *The Palgrave Handbook of Political Elites* (pp. 161–180). London: Palgrave MacMillian.

Eldem, T. (2020). The governance of Turkey's cyberspace: Between cyber security and information security. *International Journal of Public Administration*, 43(5), 452–465.

Ensafi, R., Winter, P., Mueen, A., & Crandall, J. R. (2015). Analyzing the great firewall of China over space and time. *Proceedings on Privacy Enhancing Technologies*, 61–76.

Esen, B., & Gumuscu, S. (2016). Rising competitive authoritarianism in Turkey. *Third World Quarterly*, 37(9), 1581–1606.

Farlin, J. (2014). *Instruments of national power: How America earned independence.* Carlisle: U.S. Army War College.

Farwell, J. P., & Rohozinski, R. (2011). Stuxnet and the future of cyber war. *Survival*, 53(1), 23–40.

Federal Communications Commission. (2020, March 31). Protecting and promoting the open internet. Retrieved from Federal Comminications Commission: https://www.govinfo.gov/content/pkg/FR-2015-04-13/pdf/2015-07841.pdf.

Findley, M. G., Piazza, J. A., & Young, J. K. (2012). Games rivals play: Terrorism in international rivalries. *Journal of Politics*, 74(1), 235–248.

FireEye, M. (2016). *M–Trends* . Milpitas, CA: Mandiant, Fire Eye Inc.

———. (2017). *M–Trends.* Milpitas: Mandiant, Fire Eye Inc.

Fitri, N. (2011). Democracy discourses through the internet communication: understanding the hacktivism for the global changing. . *Online Journal of Communication And Media Technologies*, 1(2), 1–20.

Floridi, L. (2008). Foundations of Information Ethics. In K. E. Himma, & H. T. Tavani (Eds.), *The Handbook of Information and Computer Ethics* (pp. 3–23). Hoboken, New Jersey, USA: John Wiley & Sons.

Foucault, M. (1977). *Discipline and Punish.* New York: Vintage Books.

Foucault, M., & Ewald, F. (2003). *Society must be defended: Lectures at the Collège de France, 1975–1976.* New York: MacMillian.

Freedom House. (2017). *Freedom of the world: United Kingdom.* Washington, DC: Freedom House.

———. (2017). *Press Freedom's dark horizon.* New York: Freedom House.

———. (2019). *Freedom on the net 2019: India.* Washington, D.C.: Freedom House.

———. (2020). Freedom of the world 2020: Iran. New York: ———. Retrieved March 27, 2020, from https://freedomhouse.org/country/iran/freedom-world/2020

———. (2020). *Freedom of the world 2020: Russia.* Washington, DC: Freedom House.

———. (2020). *Freedom of the world 2020: Turkey.* Washington, DC: Freedom House.

———. (2020). *Freedom of the world 2020: United Kingdom.* Washington, DC: Freedom House.

Gabdulhakov, R. (2020). (Con)trolling the web: Social media user arrests, state-supported vigilantism and citizen counter-forces in Russia. *Global Crime*, Gabdulhakov, 21(3–4), 1–23.

Galič, M., Timan, T., & Koops, B.–j. (2017). Bentham, Deleuze and beyond: An overview of surveillance theories from the panopticon to participation. *Philosophy and Technology*, 30(1), 9–37.

Gamson, W. A., & Meyer, D. S. (1999). Framing political opportunity. In D. McAdams, J. D. McCarthy, & M. N. Zald (Eds.), *Comparative Perspectives on Social Movements: Political Opportunities, Mobilizing Structures, and Cultural Framing* (pp. 274–290). Cambridge: Cambridge University Press.

Gandhi, R., Sharma, A., Mahoney, W., Sousan, W., Zhu, Q., & Laplante, P. (2011). Dimensions of Cyber Attacks. *IEEE Technology and Society Magazine*, 30(1), 28–38.

Gartzke, E. (2013). The myth of cyberwar: Bringing war in cyberspace backdown to Earth. *International Security*, 38(2), 41–73.

Gartzke, E., & Lindsay, J. R. (2015). Weaving tangled webs: Offense, defense, and deception in Cyberspace. *Security Studies*, 24(2), 316–386.

Gebhart, G., Anonymous, A., & Kohno, T. (2017). Internet censorship in Thailand: User practices and potential threats. *Proceedings – 2nd IEEE European Symposium on Security and Privacy, 2017* (pp. 417–432). Paris: IEEE, 2017.

Gehlbach, S., & Sonin, K. (2013). Government Control of the Media. *Journal of Public Economics*, 118, 163–171.

Gladwell, M. (2010, October 4). Small change. *New Yorker*, pp. 1–15.

Godfrey-Smith, P. (2003). *An Introduction to the Philosophy of Science: Theory and Reality*. Chicago: University of Chicago Press.

Goldsmith, J., & Wu, T. (2006). *Who Controls the Internet? Illusions of a Borderless World*. New York: Oxford University Press.

Goldstein, J. (1992). A Conflict-Cooperation Scale for WEIS Events Data. *Journal of Conflict Resolution*, 36(2), 369–385.

Goldstein, J. S., & Pevehouse, J. C. (1997). Reciprocity, Bullying, and International Cooperation: Time-Series Analysis of the Bosnia Conflict. *The American Political Science Review*, 91(3),515–529.

Golkar, S. (2011). Liberation or suppression technologies? The internet, the green movement and the regime in Iran. *Australian Journal of Emerging Technologies and Society*, 9(1), 50–70.

Goodman, M. (2015). *Future Crimes: Everything is Connected, Everyone is Vulnerable, and What we can do about it.* New York: Random House.

Grdesic, M. (2014). Television and protest in East Germany's revolution, 1989–1990: A Mixed Methods Analysis. *Communist and Post-Communist Studies*, 47(1), 93–103.

Gregory, P. (2017, June 21). How much is Saudi Aramco worth? It depends on the country's institutions. Retrieved from Forbes: https://www.forbes.com/sites/uhenergy/2017/06/21/how-much-is-saudi-aramco-worth-it-depends-on-the-countrys-institutions/#4285f75d7b83

Greitens, S. C. (2013). Authoritarianism Online: What can we learn from internet data in nondemocracies? *PS – Political Science and Politics, 46*(2), 262–270.

Grix, J. (2000). *The Role of the Masses in the Collapse of the GDR.* New York: Springer.

Gunitsky, S. (2015). Corrupting the cyber-commons: Social media as a tool of autocratic stability. *Perspectives on Politics*, 13(1), 42–54.

Gurdeniz, C. (2020). Turkey in the century of the sea and Asia. *Belt and Road Initiative Quarterly, 1*(2), pp. 81–88.

Habermas, J. (1987). *The Theory of Communicative Action: Volume 2: Lifeworld and System: A Critique of Functionalist Reason* (3d ed.). (T. McCarthy, Trans.) Boston: Beacon Press.

———. (2006). Political communication in media society: Does democracy still enjoy an epistemic dimension? The impact of normative theory on empirical research. *Communication Theory*, 16(4),411–426.

Hamilton, S. N., Miller, W. L., Ott, A., & Saydjari, O. S. (2002). Challenges in Applying Game Theory to the Domain of Information Warfare. *Proceedings of the 4th Information Survivability Workshop (ISW–2001/2002).*

Hammond, J. (2018). Maps of mayhem: Strategic location and deadly violence in Civil War. *Journal of Peace*, 55(1), 32–46.

Harris, S. (2008). China's Cyber-Militia. *National Journal*.

———. (2017, December 19). U.S. blames North Korea for 'WannaCry' cyberattack. Retrieved from Wall Street Journal: https://www.wsj.com/articles/u-s-blames-north-korea-for-wannacry-cyberattack-1513701911?mod=searchresults&page=1&pos=10

Hayes, D., & Guardino, M. (2013). *Influence from abroad: Foreign voices, the Media, and U.S. Public Opinion.* Cambridge: Cambridge University Press.

Henry, C. M. (2018). Political Elites in the Middle East and North Africa. In H. Best, & J. Higley (Eds.), *The Palgrave Handbook of Political Elites* (pp. 1–698). London: Palgrave MacMillian.

Heradstveit, D. (1979). *The Arab-Israeli conflict : psychological obstacles to peace.* Universitetsforlaget; New York: Columbia University Press.

Herman, D., Jahn, M., & Ryan, M.–L. (Eds.). (2005). *Routledge Encyclopedia of Narrative Theory.* New York: Routledge (Taylor and Francis Group).

Higley, J. (2018). Political Elites in the West. In H. Best, & J. Higley, *The Palgrave Handbook of Political Elites* (pp. 315 – 328). London: Palgrave McMillian.

Higley, J., & Burton, M. (2006). *Elite Foundations of Liberal Democracy.* New York: Rowman & Littlefield Publishers, Inc.

Himma, K. E. (2008). Ethical Issues Involving Computer Security: Hacking, Hacktivism, and Counterhacking. In K. E. Himma, & H. T. Tavani (Eds.), *The Handbook of Information and Computer Ethics* (pp. 191–217). Hoboken: John Wiley & Sons.

Hinnebusch, R. (2015). Conclusion: Agency, Context and Emergent Post-Uprising Regimes. *Democratization*, 358–374.

Hoffman, L. (2011). Risky Business. *Communications of the Association of Computer Machinery (ACM)*, 11(20), 20–22.

Hoffman-Lange, U. (2018). Theory-Based Typologies of Political Elites. In H. Best, & J. Higley (Eds.), *The Palgrave Handbook of Political Elites* (pp. 53–68). London: Palgrave-MacMillian.

Holmes, O. (2016, January 26). Unicef warns of severe child malnourshment in North Korea. Retrieved from The Guardian: https://www.theguardian.com/global-development/2016/jan/26/unicef-appeal-2016–severe-child-malnourishment-north-korea.

Hornyak, T. (2015, February 04). 2014 Cyberattack to Cost Sony $35M in IT Repairs. Retrieved from ComputerWorld.com: https://www.computerworld.com/article/2879480/2014–cyberattack-to-cost-sony-35m-in-it-repairs.html

Howell, L. D. (1983). A Comparative Study of the WEIS and COPDAB data sets. *International Studies Quarterly*, 27(2, 149–159.

Hurrell, A. (2012). The Anarchical Society 25 Years On. In H. Bull, *The Anarchical Society* (4th ed., pp. vii-xxiii). New York: Columbia University Press.

Hussain, A., & Hussain, N. (2017). Post-coup Turkey and its relevance to Middle East dynamics. *Journal of Social Sciences & Humanities*, 25(1), 67–82.

Hussain, M. M. (2016). *State Power 2.0: Authoritarian Entrenchment and Political Engagement Worldwide* (2d ed.). New York: Routledge.

IBM, M. C. (2018, February 02). *10 Key Marketing Trends for 2017.* Retrieved from IBM Offering Information: https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=WRL12345USEN

ICANN. (2018, May 11). *The IANA Functions: An Introduction to the Internet Assigned Numbers Authority (IANA) Functions.* Retrieved May 11, 2018, from Internet Corporation for Assigned Names and Numbers (ICANN): https://www.icann.org/en/system/files/files/iana-functions-18dec15–en.pdf

Inkster, N. (2016). Information warfare and the U.S. presidential election. *Survival*, 58(5), 29–50.

Internet Users by Country. (2017, November 06). Retrieved from internetlivestats: http://www.internetlivestats.com/internet-users-by-country/

Iran Development Organization. (2010). Soft war reasons against Islamic Republic of Iran. Retrieved from http://www.ido.ir/en/en-a.aspx?a=1388101204

Jaitner, M., & Mattsson, P. A. (2015). Russian information warfare of 2014. *International Conference on Cyber Conflict, CYCON* (pp. 39–52). Tallinn, Estonia: NATO Cooperative Cyber Defence Center of Excellence.

Jarausch, K. H. (1994). *The Rush to German Unity.* Oxford: Oxford University Press.

Jervis, R. (1976). *Perception and misperception in international politics.* Princeton, NJ: Princeton University Press.

Johnson IV, J. J., Tolk, A., & Sousa-Poza, A. (2013). A theory of emergence and entropy in systems of systems. *Procedia Computer Science*, 20(2013), 283–289.

Joint Chiefs of Staff. (2014). *JP 3–13, Information Operations.* Arlington, VA, USA: Department of Defense.

Jones, J. (2016, Feb 10). How many physical servers (connected to the Internet) are there in the world? Retrieved from Quora: https://www.quora.com/How-many-physical-servers-connected-to-the-Internet-are-there-in-the-world

Jones, S. G., & Newlee, D. (2020). *Iran's Protests and the Threat to Domestic Stability.* Washington, DC: Center for Strategic and International Studies.

Jordan, S. (2017). Evaluating Zero-rating and associated throttling practices under the open internet order. *Journal of Information Policy*, 7(2017),450–507.

Jordan, T., & Taylor, P. (2004). *Hacktivism and Cyberwars: Rebels with a Cause?* New York: Psychology Times.

Kantchev, G., & Strobel, W. P. (2021, 01 04). Hackers bolster Kremlin ambitions. *Wall Street Journal*.

Katz, E. (2001). Lazarsfeld's map of media effects. *International Journal of Public Opinion*, 13(3),270–279.

Kearns, M. (2005). Coding for Reading. In D. Herman, M. Jahn, & M.–L. Ryan (Eds.), *Routledge Encyclopedia of Narrative Theory* (pp. 66–67). London and New York: Routledge.

Keating, C. B. (2009). Emergence in System of Systems. In M. Jamshidi, *System of Systems Engineering: Innovations for the 21st Century* (pp. 169–190). Hoboken: John Wiley & Sons, Inc.

Keck, M., & Sikkink, K. (1998). *Activists beyond borders: Transnational Activist Networks in International Politics.* Itaca, NY: Cornell University Publishing.

Kello, L. (2013). The meaning of cyber revolution: Perils to theory and statecraft. *International Security*, 38(2), 7–40.

Kerlinger, F. N., & Lee, H. B. (2000). *Foundaions of Behavioral Research.* Northridge: Wadsworth Thomson Learning.

Kern, H. L. (2011). Foreign Media and Protest Diffusion in Authoritarian Regimes: The Case of the 1989 East German Revolution. *Comparative Politics*, 44(9), 1179–1205.

Khan, A. (2010, December 09). What is the Tor project and how Tor works [Complete Guide]. Retrieved from Additive Tips: https://www.addictivetips.com/internet-tips/what-is-tor-project-and-how-tor-works-complete-guide/

King, G., Pan, J., & Roberts, M. E. (2013). How Censorship in China allows Government Criticism but Silences Collective Expression. *American Political Science Review,* 107(2), 326–343.

King, M. L. (1963, April 16). *Letter from Birmingham jail.* (M. L. King, Performer) Birmingham, Alabama, United States.

Kissinger, H. (1994). *Diplomacy.* New York: Touchstone Publishing.

Klapper, J. T. (1960). *The Effects of Mass Communication.* Oxford, England: Free Press of Glencoe.

Klein, J. P., Goertz, G., & Diehl, P. F. (2006). The new rivalry dataset: Procedures and patterns. *Journal of Peace Research*, 43(4), 331–348.

Koh, H. H. (2012). Cyber Attacks. *USCYBERCOM Inter-Agency Legal Conference* (pp. 1–7). Fort Meade: USCYBERCOM.

Kriesi, H. (1999). The organization of new social movements in a political context. In D. McAdam, J. D. McCarthy, & M. N. Zald, *Comparative Perspectives on Social Movements* (pp. 152–184). Cambridge: Cambridge University Press.

Krinsky, J., & Crossley, N. (2014). Social movements and social networks: Introduction. *Social Movement Studies*, 13(1), 1–21.

Kroft, S. (2015, April 12). The attack on Sony. Retrieved from CBS News: http://www.cbsnews.com/news/north-korean-cyberattack-on-sony-60–minutes/

Kugler, R. L. (2009). Deterrence of cyber attacks. *Cyberpower and National Security*, 320, 309–340.

Kuhn, T. S. (1962). *The Structure of Scientific Revolutions.* Chicago, Illinios: Chicago University Press.

Kuran, T. (1991). Now out of never: The element of surprise in the East European revolution of 1989. *World Politics*, 7–48.

Ladd, J. M. (2013). The era of media distrust and its consequences for perceptions of political reality. In T. N. Ridout, *New Directions in Media and Politics* (pp. 42–62). New York: Routledge.

Lasswell, H. D. (1935). *World Politics and Personal Insecurity*. New York: Free Press.

Layers of Earth's Atmosphere. (2018, February 02). Retrieved from UCAR Center for Science Education: https://scied.ucar.edu/atmosphere-layers

Lazarsfeld, P. F., Berelson, B., & Gaudet, H. (1944). *The People's Choice.*

Lazer, D. M., Baum, M. A., Benlder, Y., Berinsky, A. J., Greenhlll, M., Menczer, F., . . . Zittrain, J. L. (2018, March 9). The Science of Fake News. *Science, 359*(6380), pp. 1094–1096.

Lee, E. (2017, January 17). Sony Pictures would make an interesting buy for a tech giant. Retrieved from Recode: https://www.recode.net/2017/1/17/14273598/sony-pictures-buy-amazon-alphabet-facebook-ap

Levada Center. (2019). *Russia Public Opinion 2018.* Moscow: Levada Center. Retrieved from https://www.levada.ru/en/

Levin, N. (2016, July 18). Ankara widens crackdown on suspects. *Wall Street Journal*.

Levine, D. M., Berenson, M. L., & Stephan, D. (1998). *Statistics for Managers using Microsoft Excel.* Upper Saddle River, New Jersey: Prentice-Hall, Inc.

Libicki, M. C. (2007). *Conquest in Cyberspace : National Security and Information Warfare.* Cambridge: Cambridge University Press.

Lindsay, J. (2013). Stuxnet and the limits of cyber warfare. *Security Studies*, 22(3), 365–404.

———. (2014). The Impact of China on Cybersecurity: Fiction or Friction. *International Security*, 39(3), 7–47.

———. (2015). Tipping the Scales: The Attribution Problem and the Feasibility of Deterrence against Cyberattack. *Journal of Cybersecurity*, 1, 53–67.

Lindsay, J. R., & Cheung, T. M. (2015). From Exploitation to Innovation: Acquisition, Absorption, and Application. In J. R. Lindsay, T. M. Cheung, & D. S. Reveron, *China and Cybersecurity: Espionage, Strategy, and Politics in the Digital Domain* (p. 379). Oxford, New York: Oxford University Press.

Lipow, J. (2016). *Survival: The Economic Foundations of American National Security.* Lanham, Maryland, USA: Lexington Books.

Loadenthal, M. (2018). The Panopticon. In B. A. Arrigo, *The SAGE Encyclopedia of Surveillance, Security, and Privacy.* Thousand Oaks: SAGE Publications, Inc.

Ludecke, D. (2019, March 15). SJSTATS: Collection of Convenient Functions for Common Statistical Computations. Retrieved from CRAN: https://github.com/strengejacke/sjstats

Lukasik, S. J. (2011). Protecting users of the cyber commons. *Communications of the Automated Computer Machinery (ACM)*, 54(9), 54–61.

Lynn III, W. J. (2010). Defending a new domain: The Pentagon's cyberstrategy defending a new domain. *Foreign Affairs*, 89(5), 97–108.

MacKinnon, R. (2011). China's "networked authoritarianism." *Journal Of Democracy*, 22(2), 32–46.

———. (2012). *Consent of the Networked: The Worldwide Struggle For Internet Freedom.* New York: Basic Books.

Mandiant Consulting, A. F. (2016). *M–Trends 2016.* Milpitas, CA: FireEye, Incorporated.

Maness, R. C., & Valeriano, B. (2016). The impact of cyber conflict on international interactions. *Armed Forces and Society*, 42(2), 301–323.

Manion, M., & Goodrum, A. (2000). Terrorism or civil disobedience: Toward a hacktivist ethic. *Computers and Society*, 30(2), 14–19.

Manokha, I. (2018). Surveillance, Panopticism, and Self-Discipline in the Digital Age. *Surveillance and Society, 16*(2), 219–237.

Maoz, Z. (1990). *National Choices and International Processes.* New York: Cambridge University Press.

Maoz, Z., & Mor, B. D. (2002). *Bound by Struggle; The Stategic Evolution of Enduring International Rivalries.* Ann Arbor: The University of Michigan Press.

Maoz, Z., & San-Akca, B. (2012). Rivalry and state support of non-state armed groups (NAGs), 1946–2001. *International Studies Quarterly*, 56(4), 720–734.

Marcellino, W., Marcinek, K., Pezard, S., & Matthews, M. (2020). *Detecting Malign or Subversive Information Efforts over Social Media.* Santa Monica, CA: Rand Corporation.

Maréchal, N. (2017). Networked authoritarianism and the geopolitics of information: understanding Russian internet policy. *Media and Communication, 5*(1), 29–41.

Marsh, S. (2012). 'Global security: US-UK relations': Lessons for the special relationship? *Journal of Transatlantic Studies*, 10(2), 182–199.

Marshall, M. G., & Cole, B. R. (2014). *Global Report 2014: Conflict, Governance, and State Fragility.* Vienna, VA: Center for Systematic Peace.

Marshall, M. G., & Elzinga-Marshall, G. (2017). *Global Report 2017: Conflict, Governance, and State.* Vienna: Center for Systematic Peace.

Mattis, J. (2018). *2018 National Defense Strategy Summary.* Arlington, VA: Office of the Secretary of Defense.

McAdam, D., McCarthy, J. D., & Zald, M. N. (1999). *Comparative perspectives on social movements: Political opportunities, mobilizing structures, and cultural framings.* Cambridge: Cambridge University Press.

McAdam, D., Tarrow, S. G., & Tilly, C. (2001). *Dynamics of Contention.* Cambridge: Cambridge University Press.

McAdams, D. (1999). The Framing Function of Movement Tactics: Strategic Dramaturgy in the American Civil Rights Movement. In D. McAdams, J. D. McCarthy, & M. N. Zald, *Comparative Perspectives On Socia Movements: Political Opportunities, Mobilizing Structures, and Cultural Framings* (pp. 338–357). Cambridge: Cambridge University Press.

McAdams, D., McCarthy, J. D., & Zald, M. N. (1999). *Comparative Perspectives on Social Movements: Political Opportunities, Mobilizing Structures, and Cultural Framings.* Cambridge: Cambridge University Press.

McAdams, D., Tarrow, S. G., & Tilly, C. (2001). *Dynamics of Contention.* Cambridge: Cambridge University Press.

McCarthy, J. D., & Zald, M. N. (1977). Resource mobilization and social movements: A partial theory. *American Journal of Sociology*, 82(2), 1212–1241.

McComb, M. E., & Shaw, D. L. (1972). The agenda-setting function of mass media. *American Journal for Public Opinion Research*, 36(2), 176–187.

McCurry, J. (2017, August 22). Too many soldiers to feed: North Koreans fear more sanctions as drought threatens famine. Retrieved from The Guardian: https://www.theguardian.com/world/2017/aug/23/north-koreans-fear-more-sanctions-as-drought-pushes-millions-towards-malnutrition.

McDonald, P. J. (2015). Great powers, hierarchy, and endogenous regimes: Rethinking the domestic causes of peace. *International Organization*, 69(3),557–558.

McElreath, R. (2016). *Statistical Rethinking: A Bayesian Course with Examples in R and Stan.* New York: CRC Press: Taylor & Francis Group.

McGraw, G. (2013). Cyber war is inevitable (Unless we build security in). *Journal of Strategic Studies*, 36(1), 109–119.

McHugh, K., & Ramirez, K. (2018). The Patriot Act. In B. A. Arrigo, *The SAGE Encyclopedia of Surveillance, Security, and Privacy*. Thousand Oaks: SAGE Publications, Inc.

Mechkova, V., & Lindberg, S. I. (2016). *Country Brief: India. V–Dem Working Papers (Vol. 49)*. Gothenburg: V–Dem Institute. doi:10.1596/978–0–8213–7870–0

Melucci, A. (1980). The new social movements: A theoretical approach. *Social Science Information*, 19(2), 199–226.

Metzl, L. (1974). Reflections on Soviet secret police and intelligence services. *ORBIS – A Journal of World Affairs, 18*(3), 917–930.

Miller, C. (2019, October 5). China and Taiwan Clash over Wikipedia Edits. *British Broadcasting Company (BBC) News*. Retrieved from www.bbc.com/news/technology-49921173

Miller, R. A., & Albert, K. (2015). If It Leads, It Bleeds (and If It Bleeds, It Leads): Media Coverage and Fatalities in Militarized Interstate Disputes. *Political Communication*, *32*(1), 61–82. https://doi.org/10.1080/10584609.2014.880976

Millett, A. R., & Maslowski, P. (1984). *For the Common Defense*. New York: The Free Press.

Mims, C. (2017, July 23). In cyberwarfare , Everyone is a combatant. Retrieved from Wall Street Journal: https://www.wsj.com/articles/how-cyberwarfare-makes-cold-wars-hotter-1500811201

Ministry of Electronics and Information Technology, Government of India. (2020, August 05). *National Cyber Security Strategy – 2013*. Retrieved from Vikaspedia: https://vikaspedia.in/e-governance/national-e-governance-plan/national-cyber-security-policy

Mitroff, I. I., & Pondy, L. R. (1974, September/October). On the Organization of Inquiry: A comparison of some Radically Different Approaches to Policy Analysis.

Mohan, S. (2015). Locating the “Internet Hindu”: Political speech and performance in Indian cyberspace. *Television and New Media, 16*(4), 339–345.

Monroe, B. L., & Schrodt, P. A. (2008). Introduction to the special issue: The statistical analysis of political text. *Political Analysis*, 351–355.

Monroe, B. L., Pan, J., Roberts, M., Sen, M., & et al., e. (2015). No! formal theory, causal inference, and big data are not contradictory trends in Political Science. *Political Science & Politics*, 48(1), 71–74.

Moore, G. E. (1965, April 19). Cramming More Components onto Integrated Circuits. *Electronics, 38*.

Morgan, H. M. (2013). Regulating CCTV?: We can’t solve problems by using the same kind of thinking we used when we created them. *Critical Criminology*, 21(1), 15–30.

Morgan, S. (2016, October 26). Cybersecurity industry outlook: 2017 to 2021. Retrieved from CSO: https://www.csoonline.com/article/3132722/security/cybersecurity-industry-outlook-2017–to-2021.html#tk.rss_all

Morgenthau, H. J. (1947). *Politics among Nations: The Struggle for Power and Peace.* New York: McGraw Hill.

Morozov, E. (2011). *The Net Delusion.* New York: PublicAffairs, Pereus Books Group.

Murphy, B. C. (2014). *The Risky Shift toward Online Activism : Do Hacktivists Pose an Increased Threat to the Homeland?* Monterey: Naval Postgraduate School.

Murray, S. (2014). Broadening the debate about war: The inclusion of foreign critics in media coverage and its potential impact on U.S. public opinion. *Foreign Policy Analysis*, 10(4), 329–350.

Natarajan, K. (2014). Digital public diplomacy and a strategic narrative for India. *Strategic Analysis, 38*(1), 91–106.

Nathan, A. J. (2017). The authoritarian resurgence: China’s challenge. *Journal of Democracy*, *26*(1), 156–170.

National WWII Museum. (2018, February 1). *Research Starters: Worldwide Deaths in World War II*. Retrieved from The National WWII Museum: https://www.nationalww2museum.org/students-teachers/student-resources/research-starters/research-starters-worldwide-deaths-world-war

Nerone, J. (2015). Chapter N. In W. Donsbach (Ed.), *The Concise Encyclopedia of Communication* (First ed., pp. 208–210). New York: John Wiley & Sons, Inc.

Neuman, W. R., & Guggenheim, L. (2011). The evolution of media effects theory: A six-stage model of cumulative research. *Communication Theory*, 21(1), 169–196.

Newton, K. (1999). Mass media effects: Mobilization or media malaise? *British Journal of Political Science*, 29(4), 577–599.

Nicholson, A. (2019, August 30). Suspicion creeps into the Five Eyes. Retrieved from The Interpreter: https://www.lowyinstitute.org/the-interpreter/suspicion-creeps-five-eyes

Nocetti, J. (2015). Contest and conquest: Russia and global internet governance. *International Affairs, 91*(1), 111–130.

Norman, G. (2012, December 2012). It is well that war is so terrible. Retrieved from The Weekly Standard: http://www.weeklystandard.com/it-is-well-that-war-is-so-terrible/article/665187

Northam, J. (2012, January 113). Russian activists turn to social media. *National Public Radio*. Retrieved from https://www.npr.org/2012/01/13/145175753/russian-activists-turn-to-social-media

Nye, J. (2014). *The Regime Complex for Managing Global Cyber Activities.* Waterloo: Chatham House. Retrieved May 11, 2018, from http://www.cigionline.org/publications/regime-complex-managing- global-cyber-activities

Nye, J. S. (2007). *Understanding International Conflict: An Introduction to Theory and History* (6th ed.). New York: Pearson and Longman.

———. (2011). *The Future of Power.* New York: Public Affairs.

———. (2017). Deterrence and Dissuasion in Cyberspace. *International Security*, 41(3), 44–71.

Obama, B. (2015). *Fact Sheet: White House summit on cybersecurity and consumer protection.* Washington, DC: The White House.

———. (2015, January 20). *Test-Full text of Obama's State of the Union address.* Retrieved from Reuters: http://www.reuters.com/article/2015/01/21/usa-obama-text-idUSL1N0V006E20150121

Ognyanova, K. (2018). In Putin's Russia, Information has You: Media Control and Internet Censorship in the Russian Federation. In *Censorship, Surveillance, and Privacy: Concepts, Methodologies, Tools, and Applications* (pp. 1769–1786). Hershey, PA: IGI Global. doi:10.4018/978–1–5225–7113–1

OilPrice.com. (2017, July 12). *Cybersecurity: The most profitable sector of 2017.* Retrieved from Cision PR Newswire: https://www.prnewswire.com/news-releases/cybersecurity-the-most-profitable-sector-of-2017–634046713.html#

Oldenburg, P. (2018). Political elites in South Asia. In H. Best, & J. Higley, *The Palgrave Handbook of Political Elites* (pp. 203–240). London: Palgrave MacMillan.

Oliver, T., & Williams, M. J. (2016). Special relationships in flux: Brexit and the future of the US–EU and US–UK relationships. *International Affairs*, 92(3), 547–567.

Ookla. (2020, March 19). Speedtest global index. Retrieved from Ookla Speedtest: https://www.speedtest.net/global-index#mobile

Opp, K. D., & Gern, C. (1993). Dissident groups, personal networks and spontaneous cooperation: The East German revolution of 1989. *American Sociological Review,* 30(1), 659–680.

Orwell, G. (1949). *Nineteen Eighty-Four.* London: Martin Secker & Warburg Limited.

Owens, W. A., Dam, K. W., & Lin, H. S. (2009). *Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities.* Washington, DC: National Academy Press.

Oxford Dictionary. (2015, March 25). *Oxford Dictionaries: Language Matters*. Retrieved from Oxford Dictionary: http://www.oxforddictionaries.com/us/definition/american_english/ethnography

Paletta, D. (2015, September 24). Federal cyber breach was worse than first believed. *Wall Street Journal*, p. A6.

———. (2015, September 8). NSA chief Says cyberattack at Pentagon was sophisticated, persistent. *Wall Street Journal*.

———. (2015, September 10). *NSA Chief Says Iranian Cyberattacks Against U.S. Have Slowed.* Retrieved from Wall Street Journal: http://www.wsj.com/articles/nsa-chief-says-iranian-cyberattacks-against-u-s-have-slowed-1441905372

Paletta, D., & Yadron, D. (2015, July 09). OPM ratchets up estimate of hack’s scope. *Wall Street Journal*.

Panetta, L. (2012, 10 11). Cybersecurity remarks to the business executives for national security. New York City, New York, USA. Retrieved May 22, 2018, from http://archive.defense.gov/transcripts/transcript.aspx?transcriptid=5136

Paul, C., & Matthews, M. (2017). *The Russian “Firehose of Falsehood” Propaganda Model: Why It Might Work and Options to Counter It.* Santa Monica, CA: Rand Corporation.

PC Mag Digital Group. (2020, March 13). *Personal Computer (PC) Magazine*. Retrieved from PC Mag: https://www.pcmag.com/encyclopedia/term/bandwidth-throttling

Pinkaew, L. (2016). Mass surveillance and the militarization of cyberspace in post-coup Thailand. *Austrian Journal of South-East Asian Studies,* 9(2), 195–214.

Polity IV. (2018). *Political Regime Characteristics and Transitions, 1800–2018.* Retrieved from http://www.systemicpeace.org/polity/polity4.htm

Pollack, K. (2004). *The Persian Puzzle: Deciphering the Twenty-five-Year Conflict Between the United States and Iran.* New York: Random House.

Porta, D. d. (2003). Review of: Dynamics of contention, by Doug McAdam, Sidney Tarrow, and Charles Tilly. *Social Movement Studies*, 2(1), 103.

Porter, M. E. (1991). *Competitive advantage of nations: creating and sustaining superior performance (Vol. 2).* New York: First Free Press.

Postelnicu, M. (2008, 02 08). *Two-step Flow Model of Communication*. Retrieved from Encyclopedia Britannica: https://www.britannica.com/topic/two-step-flow-model-of-communication

Potter, W. J. (2012). *What is a Media Effect?* Thousand Oaks: Sage Publications.

Price, M. (2012). Iran and the soft war. *International Journal of Communication*, 6, 2397–2415.

Prost, A. (2014, October 08). *War losses.* Retrieved from International Encyclopedia of the First World War: https://encyclopedia.1914–1918–online.net/article/ war_losses.

Putnam, R. D. (1976). *The Comparative Study of Political Elites.* Upper Saddle River: Prentice-Hall.

———. (1988). Diplomacy and domestic politics : The Logic of Two-Level Games. *International Organization*, 42(3), 427–460.

Qin, X., & Lee, W. (2004). Attack plan recognition and prediction using causal networks. *Proceedings – 20th Annual Computer Security Applications Conference, ACSAC* (pp. 370–379). Institute for Electrical and Electronics Engineers (IEEE).

Quinn, J. (2017). A peek Over the great firewall: A dreakdown of China's new cybersecurity law . *SMU Science & Technology Law Review*, 407–436.

Rahbarqazi, M., & Baghban, S. M. (2019). Social media, political discussion, and political protest: A case study of the 2018 political protests in Iran. *Kome – International Journal of Pure Communications Inquiry*, 7(2), 89–103.

Rahimi, B. (2011). The agonistic social media: Cyberspace in the formation of dissent and consolidation of state power in postelection Iran. *Communication Review*, 14(3), 158–178.

———. (2015). Internet censorship in Rouhani's Iran: The "Wooden Sword." *Asian Politics & Policy*, 7(2), 336–341. ———. (2016). Vahid online: Post-2009 Iran and the politics of citizen media convergence. *Social Sciences*, 5(4), 1–12.

Ramli, D., Bergen, M., & Hunter, G. S. (2018, November 26). A company that's helping build China's panopticon won't stop There. *Bloomberg BusinessWeek*, pp. 23–24.

Rao, U., & Nair, V. (2019). Aadhaar: Governing with Biometrics. *Journal of South Asia Studies*, 42(3), 496–481.

Regalado, A. (2013). *The data made me do it.* Boston: MIT Technology Review.

Rehman, R. U. (2003). *Intrusion detection with SNORT.* Upper Saddle River, NJ: Prentice Hall.

Reifler, J., Clarke, H. D., Scotto, T. J., Sanders, D., Stewart, M. C., & Whiteley, P. (2014). Prudence, principle and minimal heuristics: British public opinion toward the use of military force in Afghanistan and Libya. *British Journal of Politics and International Relations*, 16(1), 28–55.

Richet, J.L. (2013). Covert censorship: Viewpoint a fatal mistake? *Communications of the ACM*, 56(8), 37–38.

Richwine, L. (2014, December 09). Cyber attack could cost Sony studio as much as $100 million. Retrieved from Reuters: http://www.reuters.com/article/2014/12/09/sony-cybersecurity-costs-idUSL1N0TT1YO20141209

Rid, T. (2012). Cyber War Will not take Place. *Journal of Stategic Studies*, 35(1), 5–32.

Rivero, T. (2017, May 15). The WannaCry cyberattack: Four things to know. Retrieved from Wall Street Journal: http://www.wsj.com/video/the-wannacry-cyberattack-four-things-to-know/0D7D7B7B–E4E6–4259–8027–ED6D9B6649A5.html

Rød, E. G., & Weidmann, N. B. (2015). Empowering Activists or Autocrats? The Internet in Authoritarian Regimes. *Journal of Peace Research*, 52(3), 338–351.

Rodrik, D. (2014). *The plot against the Generals.* Cambridge, Massachusetts: Harvard University. Retrieved from https://drodrik.scholar.harvard.edu/files/dani-rodrik/files/plot-against-the-general

Romanyuk, G. (2011). *Agenda Setting in Offline and Online Media : Index of Media Freedom.* Cambridge: Harvard University.

Ruijgrok, K. (2017). From the web to the streets: internet and protests under authoritarian regimes. *Democratization*, 24(3), 498–520.

Ryan, M. (2005). Lifeworld. In G. Ritzer, *Encyclopedia of Social Theory* (p. 1056). Thousand Oaks: Sage Publications, Inc.

Sadjadpour, K. (2020, January 10). The sinister genius of Qassem Soleimani. *Wall Street Journal*. Retrieved March 24, 2020, from https://www.wsj.com/articles/the-sinister-genius-of-qassem-soleimani-11578681560?mod=searchresults&page=1&pos=9

Saka, E. (2018). Social media in Turkey as a space for political battles: AKTrolls and other politically motivated trolling. *Middle East Critique, 27*(2), 161–177.

Samuel, A. (2002). Digital disobedience: Hacktivism in political context. *The Internet as Agent of Change: Bridging Barriers to Cultural, Political and Activist Discourse.* (pp. 1–44). San Francisco: American Political Science Association.

———. (2004a). *Hacktivism and the future of political participation.* Cambridge: Harvard University.

Samuel, A. W. (2004b). Hacktivism and the future of democratic discourse. In P. M. Shane, *Democracy Online: Prospects for Political Renewal through the Internet* (pp. 1–300). New York and London: Routledge.

Sanger, D. E. (2012, June 01). *Obama Order Sped Up Wave of Cyberattacks Against Iran.* Retrieved from The New York Times: http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html/.

Scheufele, D. A. (1999). Framing as a theory of media effects. *Journal of Communication*, 49(1), 103–122.

Scheufele, D. A., & Tewksbury, D. (2007). Framing, agenda setting, and priming: The evolution of three media effects models. *Journal of Communication*, 57(1), 9–20.

Schmitt, M. N. (2013). *Tallinn Manual on the International Law Applicable to Cyber Warfare.* Cambridge: Cambridge University Press.

Schrenk, M. (2012). *Webbots, Spiders, and Screen Scrapers.* San Francisco: No Starch Press.

Schrodt, P. A. (2012). *Conflict and mediation observations, event and actor codebook.* University Park, Pennsylvania: Pennsylvania State University.

———. (2012). Precedents, Progress, and Prospects in Political Event Data. *International Interactions*, 38(4), 546–569.

———. (2017). *A Practical Guide to Current Developments in Event Data.* Charlottesville: International Methodology Colloquium.

Schrodt, P. A., & Gerner, D. J. (1997). Empirical Indicators of Crisis Phase in the Middle East 1979–1995. *The Journal of Conflict Resolution*, 41(4), 529–552.

Shackelford, S. J. (2012). From Nuclear War to Net War: Analogizing Cyber Attacks in International Law From Nuclear War to Net War . *Berkeley Journal of International Law*, 27(1), 193–250.

Shahin, S., & Zheng, P. (2020). Big Data and the Illusion of Choice: Comparing the Evolution of India's Aadhaar and China's Social Credit System as Technosocial Discourses. *Social Science Computer Review*, 38(1), 25–41.

Shambayati, H. (2004). A Tale of Two Mayors: Courts and Politics in Iran and Turkey. *International Journal of Middle East Studies*, 36(2), 253–275.

Shannon, C. (1948). A Mathematical Theory of Communication. *The Bell System Technical Journal*, 27(1), 623–656.

Shannon, C. E., & Weaver, W. (1964). *The Mathematical Theory of Communication.* Ubana, IL, USA: The University of Illinois Press.

Sharma, A. (2011, October 28). RIM facility helps India in surveillance efforts. *Wall Street Journal*.

Sharp, T. (2017). Theorizing cyber coercion: The 2014 North Korean operation against Sony. *Journal of Strategic Studies*, 40(7), 898–926.

Shellman, S. M., Clare Hatfield, M., & Mills, M. J. (2010). Disaggregating actors in intranational conflict. *Journal of Peace Research*, 47(1), 83–90.

Sherry, J. L. (2004). Media Effects Theory and the Nature / Nurture Debate : A Historical Overview and Directions for Future Research. *Media Psychology*, *6*(March 2015), 83–109. https://doi.org/10.1207/s1532785xmep0601.

Shi, S. (Director). (2020, March 10). *China deploys drones, citizens, and big data to tackle Coronavirus* [Motion Picture]. Retrieved from Wall Street Journal: https://www.wsj.com/articles/fever-detecting-goggles-and-disinfectant-drones-countries-turn-to-tech-to-fight-coronavirus-11583832616?mod=searchresults&page=1&pos=2

Shin, S., Lin, R., & Guofei, G. (2011). Cross-Analysis of botnet victims: New insights and implications. In G. Goos, J. Hartmanis, J. van Leeuwen, D. Hutchison, & et.al. (Ed.), *4th International Symposium, RAID 2011 Menlo Park, CA, USA, September 20–21, 2011 Proceedings (LNCS 6961)* (pp. 242–261). Menlo Park, CA: Springer Publishing.

Shirky, C. (2011). The Political Power of Social Media: Technology, the Public Sphere, and Political Change. *Foreign Affairs*, 90(1), 28–42.

Shoemaker, P. J., & Reese, S. D. (1996). *Mediating the message* (pp. 781–795). White Plains, NY: Longman.

Singer, P. W., & Friedman, A. (2013). *Cybersecurity and Cyberwar: Whate Everyone Needs to Know*. New York: Oxford University Press.

Sinpeng, A. (2013). State repression in Cyberspace : The case of Thailand. *Asian Politics & Policy*, 5(3), 421–440.

Sklerov, M. J. (2009). *Solving the Dilemma of State Responses to Cyberattacks: A Justification for the use of active defenses against States who neglect their Duty to Prevent.* Charlottesville, VA: U.S. Army, Judge Advocate General's School.

Snegovaya, M. (2015). *Putin's Information Warfare in Ukraine: Soviet Origins of Russia's Hybrid Warfare.* Washington, DC: Institute for the Study of War.

Snidal, D. (1985). The game theory of international politics. *World Politics*, 38(1), 25–57.

Solomon, F. (2020, February 25). Internet Shutdowns Become a Favorite Tool of Governments: 'It's Like We Suddenly Went Blind'. *Wall Street Journal*. Retrieved from https://www.wsj.com/articles/internet-shutdowns-become-a-favorite-tool-of-governments-its-like-we-suddenly-went-blind-11582648765

Sreberny, A., & Khiabany, G. (2010). *Blogistan: The internet and politics in Iran.* New York: Palgrave Macmillan.

Stavridis, J. G. (2015, January 01). *Incoming: What is a cyber attack.* Retrieved from Armed Forces Communications and Electronics Association (AFCEA): http://www.afcea.org/content/?q=incoming-what-cyber-attack.

Sterman, J. D. (2010). *Business Dynamics; Systems Thinking and Modeling for a Complex World.* New Delhi: McGraw-Hill Education.

Stier, S. (2015). Democracy, Autocracy and the news: The impact of regime type on media freedom. *Democratization*, 22(7), 1273–1295.

———. (2017). Internet diffusion and regime type: Temporal patterns in technology adoption. *Telecommunications Policy*, 41(1), 25–34.

Stockmann, D., & Gallagher, M. E. (2011). Remote Control: How the Media Sustain Authoritarian Rule in China. *Comparative Political Studies*, 44(4), 436–467.

Stoddart, K. (2016). Live free or die hard: U.S.–UK Cybersecurity Policies. *Political Science Quarterly*, 131(4), 803–842.

Strong, J. (2017). Two-Level Games beyond the United States: International Indexing in Britain during the Wars in Afghanistan, Iraq and Libya. *Global Society*, 31(2), 293–313.

Strovsky, D. L. (2015). The Media as a Tool for Creating Political Subordination in President Putin's Russia. *Styles of Communication, 7*(1/2015), 10–17.

Tabansky, L. (2016). Cyber Power in the changing Middle East. *Turkish Policy Quarterly,* 15(1), 107–114.

Tarrow, S. (1996). States and Opportunities: The Political Structure of Social Movements. In D. McAdam, J. D. McCarthy, & M. N. Zald, *Comparative Perspectives on Social Movements: Political Opportunities, Mobilizing Structures, and Cultural Framing* (pp. 41–61). Cambridge: Cambridge University Press.

Thomas, T. (2004). Russia's Reflexive Control Theory and the Military. *The Journal of Slavic Military Studies*, 24(3), 237–256.

Thompson, W. R. (2001). Identifying Rivals and Rivalries in World Politics. *International Studies Quarterly,* 45(4), 557–586.

Thornton, R., & Miron, M. (2019). Deterring Russian cyber warfare: the practical, legal and ethical constraints faced by the United Kingdom. *Journal of Cyber Policy,* 4(2), 257–274.

Tilly, C., & Tarrow, S. (2015). *Contentious Politics* (2nd ed.). New York: Oxford University Press.

Toffler, A. (1980). *The Third Wave.* New York: Bantam.

Toffler, A., & Toffler, H. (1993). *War and Anti-War: Survival at the Dawn of the 21st Century.* New York: Little, Brown and Company.

Toft, M. D. (2014). Territory and War. *Journal of Peace and Research*, 51(2), 185–198.

Tomz, M. R., & Weeks, J. L. (2013). Public Opinion and the Democratic Peace. *American Political Science Review*, 107(4), 849–865.

Treharne, S.-A. (2015). *Reagan and Thatcher's Special Relationship Book.* Edinburgh: Edinburgh University Press.

Tripp, M., & Kubota, Y. (2020, March 3). Tim Cook and Apple Bet Everything on China. Then Coronavirus Hit. *Wall Street Journal*. Retrieved from https://www.wsj.com/articles/tim-cook-and-apple-bet-everything-on-china-then-coronavirus-hit-11583172087?mod=searchresults&page=1&pos=6

Trumbore, P. F., Boyer, M. A., Gibson, M., Harvey, F., & Wilkenfeld, J. (2000). International crisis decisionmaking as a two-level process. *Journal of Peace Research*, 37(6), 679–697.

Turcotte, J., York, C., Irving, J., Scholl, R. M., & Pingree, R. J. (2015). News Recommendations from Social Media Opinion Leaders: Effects on Media Trust and Information Seeking. *Journal of Computer-Mediated Communication*, 20(5), 520–535.

Urofsky, M. I. (2018, April 06). *Jim Crow law*. Retrieved from Encyclopedia Britannica: https://www.britannica.com/event/Jim-Crow-law

Valeriano, B., & Maness, R. C. (2014). The dynamics of cyber conflict between rival antagonists, 2001–11. *Journal of Peace Research*, 51(3), 347–360.

Valeriano, B., & Maness, R. C. (2015). *Cyber War vs. Cyber Realities: Cyber Conflict in the International System.* New York: Oxford University Press.

Valeriano, B., & Maness, R. C. (2015). The Dynamics of Cyber Conflict between Rival Antagonists. In B. Valeriano, & R. C. Maness, *Cyber War versus Cyber Realities: Cyber Conflict in the International System* (pp. 78–108). Oxford: Oxford University Press.

Valeriano, B., Jensen, B., & Maness, R. C. (2018). *Cyber Strategy: The Evolving Character of Power and Coercion.* New York: Oxford University Press.

Valeriano, B., Maness, R. C., & Jensen, B. (2017, July 13). Cyberwarfare has taken a new turn. Yes, it’s time to worry. *Washington Post*.

Valeur, F., Vegna, G., Kruegel, C., & Kemmerer, R. (2004). A Comprehensive Approach to Intrusion Detection Alert Correlation. *Institute of Electrical and Electronics Engineers (IEEE): Transactions On Dependable and Secure Computing*, 1(2), 146–169.

Valkenburg, P. M., Peter, J., & Walther, J. B. (2016). Media effects: Theory and research. *Annual Review of Psychology*, 67(1), 315–338.

Vasquez, J., & Leskiw, C. S. (2001). The origins and war proneness of interstate rivalries. *Annual Review of Political Science*, 4(1), 295–316.

Vatis, M. A. (2001). *Cyber Attacks During The War on Terrorism: A Predictive Analysis.* Hanover, New Hampshire: Institute for Security Technology Studies, Dartmouth College.

V Dem Institute. (2019). *VDem Codebook.* Gothenburg: University of Gothenburg.

Vegh, S. (2002). Hacktivists or Cyberterrorists? The changing media discourse on hacking. *First Monday*, 7(1), 1–11.

Vincent, J. E. (1979). *Project Theory: Interpretations and Policy Relevance.* Washington, D.C.: University Press of America.

Wagner, B. (2012). Push-button-autocracy in Tunisia: Analysing the role of internet infrastructure, institutions and international markets in creating a Tunisian censorship regime. *Telecommunications Policy*, 36(6), 484–492.

Wake, P. (2009). Narrative and Narratology. In S. W. Littlejohn, & K. A. Foss (Eds.), *Encyclopedia of Communication Theory* (pp. 14–27). Thousand Oaks: Sage Publications, Inc.

Walker, C., & Ludwig, J. (2017). The meaning of sharp power. *Foreign Affairs*, 9–23.

Walker, C., Kalathil, S., & Ludwig, J. (2020). The Cutting Edge of Sharp Power. *Journal of Democracy*, 31(1), 124–137.

Wallace, K. A. (2008). Online Anonymity. In K. E. Himma, & H. T. Tavani (Eds.), *The Handbook of Information and Computer Ethics* (pp. 165 – 189). Hoboken: John Wiley & Sons, Inc.

Walton, R. E., & McKersie, R. B. (1965). *A Behavioral Theory of Labor Negotiations: An Analysis of a Social Interaction System.* New York: McGraw-Hill.

Waltz, K. N. (1979). *Theory of International Politics.* Menlo Park: Wesley Publishing Company.

Walzer, M. (1977). *Just and Unjust War.* New York: Basic.

———. (1980). The moral standing of states : A response to four critics. *Philosophy and Public Affairs*, 9(3), 209–229.

Wang, S. S. (2012). China’s internet lexicon: The symbolic meaning and commoditization of Grass Mud Horse in the harmonious society. *First Monday*. 17(1), 1–10.

Wang, Y., & Minzner, C. (2015). The rise of the Chinese security state. *Chinese Quarterly*, 339–359.

Warren, T. C. (2015). Explosive connections? Mass media, social media, and the geography of collective violence in African states. *Journal of Peace Research*, 52(3), 297–311.

Webster, M. (2017, 04 07). *Webster Dictionary*. Retrieved from Merriam-Webster: https://www.merriam-webster.com/dictionary/

Weidmann, N. B. (2015). Communication, technology, and political conflict: Introduction to the special issue. *Journal of Peace Research*, 52(3), 263–268.

Werder, O. H. (2009). Media Effects Theories. In S. Littlejohn, & K. Foss (Eds.), *Encyclopedia of Communication Theory* (pp. 633–635). Thousand Oaks: Sage Publishing, Inc.

Whitten-Woodring, J., & James, P. (2012). Fourth estate or mouthpiece? A formal Model of media, protest, and government repression. *Political Communication*, 29(2), 113–136.

Whyte, C. (2016). Ending cyber coercion: Computer network attack, Exploitation and the case of North Korea. *Comparative Strategy*, 35(2), 93–102.

Wong, C. H. (2020, March 08). Beijing portrays President Xi Jinping as hero of Coronavirus Fight: Publicity blitz aims to blunt criticism that China's leader and Communist Party government were slow to respond to developing epidemic. *Wall Street Journal*. Retrieved from https://www.wsj.com/articles/beijing-portrays-president-as-hero-of-coronavirus-fight-11583678054.

The World Bank. (2019, October 1). *The World Bank: IBRD – IDA*. Retrieved from World Bank Data: https://data.worldbank.org/indicator/NY.GDP.MKTP.CD

World Population Review. (2020, March 19). *Internet Speeds by Country 2020*. Retrieved from World Population Review: https://worldpopulationreview.com/countries/internet-speeds-by-country/

Wu, Y.–L., Tao, Y.–H., & Chang, C.–J. (2017). A comparative review on privacy concerns and safety demands of closed-circuit television among Taiwan, Japan, and the United Kingdom. *Journal of Information and Optimization Sciences*, 38(1), 173–196.

Yadron, D., & Gorman, S. (2013, July 12). U.S. firms draw a bead on Chinese Cyberspies. Retrieved from Wall Street Journal Online: http://online.wsj.com/home-page

Yang, S. J., Stotz, A., Holsopple, J., Sudit, M., & Kuhl, M. (2009). High level information fusion for tracking and projection of multistage Cyber Attacks. *Information Fusion*, 10(1), 107–121.

Yang, S., Holsopple, J., & Sudit, M. (2006). Evaluating Threat Assessment for Multi-Stage Cyber Attacks. *MILCOM 2006* (pp. 1–7). New York: IEEE.

Yesil, B., Sözeri, E. K., & Khazraee, E. (2017). Turkey's internet policy After the coup attempt: The emergence of a distributed network of Online suppression and surveillance. *Internet Policy Observatory*, 24(3), 2–28.

Yin, R. K. (2009). *Case Study Research Design and Methods* (4th ed.). Thousand Oaks: Sage Publications Inc.

Yonamine, J. E. (2001). *Working with Event Data: A Guide to Aggregation Choices.* University Park, Pennsylvania: Pennsylvania State University.

Zeileis, A., Kleiber, C., & Jackman, S. (2015). Regression Models for Count Data in R . *Journal of Statistical Software*, 27(8), 1–25.

Zhukov, Y. M., & Baum, M. A. (2016). Reporting Bias and Information Warfare. *International Studies Association National Convention* (pp. 1–42). Atlanta: International Studies Association Annual Convention.

Zittrain, J. L., Faris, R., Noman, H., Clark, J., Tilton, C., & Morrison-Westphal, R. (2017). *The Shifting Landscape of Global Internet Censorship.* Cambridge: Berkman Klein Center for Internet & Society Research Publication.

Zurawski, N. (2004). “I know where you live!” – Aspects of watching, surveillance and social control in a conflict zone (Northern Ireland). *Surveillance and Society*, 2(4), 498–512.

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California