Political Science Graduate Student Journal

Volume III

Challenges, Disconnects, and Clashes in Political Studies

Concordia University
Department of Political Science
Fall 2014

Political Science Graduate Student Journal

Department of Political Science

Volume III

Challenges, Disconnects, and Clashes in Political Studies

Concordia University
Montréal, Québec, Canada
2014-2015

Challenges, Disconnects, and Clashes in Political Studies

Volume III

Table of Contents

Foreword

This journal began as a conference project with a vision to move away from the seemingly dominant trend of globalization as a topic for graduate student conferences and target instead a wide diversity of other issues of interest to students in political studies. Hence, the title of *Challenges, Disconnects, and Clashes in Political Studies* was born, and the submissions did not disappoint. Conference papers ranged from abduction to aesthetics, from nuclear weapons to netnography, and as can be seen in this journal, from Canadian civic engagement to Stuxnet.

This project is the result of the hard work of many dedicated individuals. The final journal articles included in these pages are the culmination of a careful editorial process. First, the best conference papers were chosen by a committee and the panel discussants. Second, these papers entered a two-phased editorial process, which involved the revision and resubmission by the each potential author. The end result is a diverse journal with four high quality papers by both MA and PhD students in various fields of political studies.

We hope, considering the wide range of topics covered by this journal, that each of these pieces separately, and together, will provoke contemplation and dialogue on some of the most challenging topics currently facing the field of political studies. It is our honour to present this year's volume entitled *Challenges, Disconnects, and Clashes in Political Studies.*

Editorial Team

Acknowledgments

This project began with the input and advice from organizing members from the previous two years. Thanks to these building blocks, this project was technically already underway, thus enabling me to steer the project rather than build it from the ground up. Thanks especially to Kerry Tannahill and Osman Shah for their assistance at this stage. Given that this journal is the product of a lengthy review process beginning with the graduate student conference, I would be remiss not to mention all of the conference committee members for their work: Alex Léger, Özge Uluskaradag, and especially Randy Pinsky, as well as a number of undergraduate students who helped the conference run smoothly: Briana Musto, Vicky Theodore, Natalie Hodge and Heloise Martorell. Furthermore, the discussants for the conference not only provided great advice and comments to the presenters, but also played a pivotal role in the selection and editorial process of this journal. For this I thank Dr. Elizabeth Bloodgood, Dr. Marlene Sokolon, Dr. Mireille Paquet, and Jeremy Speight. The editorial team also did an excellent job in deeply analyzing the papers and offering a number of suggestions to improve the papers being considered for this journal. Thank you to Osman Shah, Maria Laham, and Alon Burstein for their continued efforts throughout this process.

In addition to those publicly involved, a lot of planning and strategizing went on behind the scenes, and for this I am thankful to administrators Julie Blumer, Kathryn Rawlings, and Sheila Anderson. Moreover, I would like to thank the Chairs of the Political Science Department, Dr. Csaba Nikolenyi and Dr. Marlene Sokolon for their wisdom and insight to make this project a reality. For financial support I would like to thank the Department of Political Science, the Political Science Graduate Student's Association, the Faculty of Arts and Science, and the Small Grants Program under the Office of the President.

Finally, I must thank our Faculty Advisor, Dr. Elizabeth Bloodgood, for her advice throughout every single stage of this process. You kept me sane throughout the entire development, which certainly is no small feat! I am forever in your gratitude.

Jocelyn McGrandle

‘Watchdog’ or ‘Junkyard’ Dog? The Influence of the News Media on Civic Engagement in Canada

James Gamblin and Kevin Marple, Concordia University

Introduction

In western democracies, in the last three decades, a discourse regarding declining levels of civic engagement has become prominent. The idea of a significant decline in civic engagement in the United States was popularized by the work of Robert Putnam’s *Bowling Alone* (2000). Civic Engagement refers to how active citizens are in contributing to the social and political life of their communities (Stolle and Cruz 2005, 82) According to Putnam, we should be alarmed by declining levels of civic engagement as they contribute to the degradation of political systems and democratic institutions (Stolle and Hooghe 2005, 153; Stolle and Cruz 2005, 82). It appears as though the phenomenon of declining civic engagement, particularly among younger generations, is not unique to the United States, as evidence has pointed to similar trends in Canada (Stolle and Cruz 2005, 84). While declining levels of civic engagement have been observed, some authors have argued that the news media plays a significant role in this decline due to increasing negative coverage of political and social issues. Is exposure to news media alone significantly associated with levels of civic engagement? If it is not, what other factors may be associated with levels of civic engagement? Instead might we look to the drivers of cognitive mobilization: access to information, education, and political sophistication?

The purpose of this paper is to investigate levels of exposure to different forms of news media in Canada and analyze the effect that news media exposure may have on different measures of civic engagement amongst voting age Canadians who participated in the 2011 Canada Election Study. The paper will seek to determine whether a relationship exists and what the nature of the relationship may be.

The study is relevant because declining levels of civic engagement have been identified as a fundamental impediment to the health of democratic society in Canada (Nadeau and Giasson 2003, 4). The debate over the relationship of the news media and levels of civic

engagement has been studied extensively in Europe and the United States. In Canada, however, political communications literature has focused mainly on content analysis of news coverage and campaign effects such as "game frames." This analysis will seek to reconcile this gap in the Canadian literature by focusing on the relationship between news media exposure and levels of civic engagement directly, and will seek to examine the role of the news media in this perceived "democratic malaise" (Nadeau and Giasson 2003).

It is assumed that in post-industrial democracies, the media plays an important role in informing and shaping citizen's views about politics; some commentators have noted a negative change in media coverage of political and public affairs. In Canada, some observers maintain that the news media has contributed to declining levels of civic engagement including political trust, mobilization, and political knowledge (Nadeau and Giasson 2003, 4). This paper will seek to investigate whether or not levels of exposure to news media are linked to increased or decreased levels of civic engagement in voting age Canadians. The question that this paper will seek to answer is whether or not news media exposure is itself significantly linked to levels of civic engagement, and if it is not, what other factors might we look to?

Literature Review

The theoretical guidance for the above research puzzle is derived from literature on the subject of civic engagement and political communications, and cognitive mobilization. Various perspectives have emerged from these separate bodies of literature and this paper seeks to evaluate where the Canadian case fits within the debate.

Civic Engagement Literature

The literature on civic engagement can be organized into two camps, modern and post-modern. There is acknowledgement within the civic engagement literature that the concept of civic engagement itself can be measured through a variety of indicators (Putnam 2000, 37). The indicators that different authors choose to measure civic engagement provide the basis for the divisions between the different camps. From a general perspective, modernists observe a generalized decline in levels of civic engagement through the lens of traditional

forms of political participation such as voter turnout, generalized trust and political party membership (Putnam 2000, 37). According to Putnam, a generational gap exists in overall civic engagement levels whereby younger generations are less inclined to be politically engaged when their participation levels are evaluated using traditional measures (Putnam 2000, 37). This decline in voluntary activity on the part of the younger generation is said to cause the overall erosion of civic culture and democracy in general (Putnam 2000, 37).

Post-modernists disagree with the modernist's "decline thesis" and point to the reliance on traditional measures of political participation as the flaw in the modernist analysis (Stolle and Hooghe 2005, 150; Inglehart 1999, 236). According to Stolle and Hooghe (2005, 164), declining levels of traditional political participation cannot be used as an exclusive indicator of civic engagement levels or overall democratic health, but rather other non-traditional forms of engagement must be examined. To post-modernists, the rise of younger, critical citizens instead represents a maturation of the political system where citizens observe and critique the political system from afar, deriving their information about the system from mass media sources and engage and critique when necessary, rather than routinely engaging in traditional forms of political participation (Stolle and Hooghe 2005, 164).

This paper focuses mostly on the traditional modernist measures of civic engagement in order to determine whether or not the media may play a role in declining levels of traditional civic engagement as identified by modernists. It is not within the scope of this paper to examine value change in the Canadian population, but rather to examine how traditional modernist measures of civic engagement are related to media exposure or other factors such as cognitive mobilization.[1]

Political Communications Literature

The relevant political communications literature can be divided into two camps: the media malaise perspective and the virtuous circle perspective. In general, media malaise scholars contend that the most informed citizens

[1] For an in depth examination of Canadian value change and postmaterialism, See Nevitte (1996).

tend to score lower on measures of traditional civic engagement and that exposure to the news media is a major factor in this finding (Capella and Jamieson 1996, 72). Through content analysis of the news media's portrayal of politics, media malaise scholars point to the focus on scandal, political "horse races", and a narrow actor-oriented framing of the policy process as contributing to the public cynicism and disaffection with democracy (Nadeau and Giasson 2003, 8-9). While the media should play the role of a "watchdog" by providing impartial, fact-based information to citizens in a democracy, it has instead assumed an aggressive role of a "junkyard dog" by focusing on superficial and overly negative issues (Nadeau and Giasson 2003, 8-9).

Conversely, virtuous circle scholars, most notably Pippa Norris (2000, 5), dispute the assumptions of the media malaise hypothesis. In fact, they seek to challenge "…the unquestioned orthodoxy," which has developed out of media malaise accounts. Virtuous circle scholars argue that the media malaise accounts rely too heavily on the historical development of the news industry as opposed to utilizing more robust individual level survey research (Norris and Inglehart 2009, 243). They argue that exposure to news media is actually positively associated with measures of civic engagement. Specifically, this literature tends to identify civic engagement as being comprised of political knowledge, political trust, and political mobilization/participation (Norris 2001, 217).[2] Through the use of panel as well cross-sectional survey data including national election studies, they find no systematic link between news media exposure and "civic malaise." Virtuous circle accounts claim that the use of news media may actually contribute to greater knowledge about politics and the community, which subsequently serves to reduce "cognitive barriers" and enable further civic engagement (Norris 2001, 242; Bennett *et al.* 1986, 579-602). One of the most common indicators of news exposure within this literature are survey questions which ask how many days per week respondents receive news from different mediums such as television, radio, newspaper or the internet. (Bennett *et al* 1986, 8).

[2] It should be acknowledged that Norris uses the terms "participation" and "mobilization" interchangeably across different works. See *Virtuous Circle*.

Cognitive Mobilization

When examining what drives civic engagement in Canada, other factors other than the media alone must be examined. There are a number of alternative explanations that may affect varying levels of civic engagement amongst Canadians. As noted by Norris, it is difficult to determine direct causality between individual levels of media exposure and levels of civic engagement (Norris 2000, 316). Individual survey research makes it difficult to discern between "media" effects, whereby media exposure directly impacts civic engagement, or "selection" effects where those who are already likely to be civically engaged seek out news media. Individuals pay attention to news media because of "prior predispositions" (Norris 2000, 18). While Norris uses prior interest in politics as a control for the effect of news media exposure on civic engagement (Norris 2000, 287-289), other literature focuses on declining levels of civic engagement to examine the broader concept of cognitive mobilization.

According to Inglehart (1970, 47) cognitive mobilization can be regarded as an accumulation of experiences and processes which increase an "…individual's capacity to receive and interpret messages relating to a remote political community." According to Dalton (2008, 19), significant societal and cultural changes since the 1950s are thought to have created citizens that possess more "political sophistication." This additional political sophistication is acquired through increased access to information about politics as well as access to education. As opposed to media exposure directly, it could be that those who are most educated and interested in politics are most likely to display high levels of civic engagement, and those who have little education, interest, and ability to interpret political information will be the most disengaged. While the literature points out that cognitive mobilization may be linked to "partisan dealignment" and value change (Dalton 1984), this paper will be concerned with how cognitive mobilization may impact modernist measures of civic engagement.

Other Explanations for Variation in Civic Engagement

Other possible explanations for variations in indicators of civic engagement may include individual perceptions political actors (Dalton 1999, 58), or the government's economic policy performance (McAllister 1999, 188-203). As previously discussed, authors such as Putnam (2000) and Newton (1999) also examine the extent to which general levels of social trust, such as trust in others might impact broader levels of civic engagement.

Hypothesis

Following the virtuous circle perspective, this paper will test the hypothesis that increased levels of news media exposure (IV) are positively associated with measures of civic engagement (DV). Conversely, lower levels of news media exposure are associated with lower levels of civic engagement. The independent variable of news media exposure can be understood as levels of intentional rather than passive exposure to news via television, print media, internet and radio. Consistent with how the concept is defined in the literature, civic engagement can be understood as an agglomeration of political knowledge, political trust and political mobilization. Within this aggregated concept, political knowledge is generally thought of as the knowledge regarding politics and public affairs that is required to make informed choices at the ballot box (Culbertson and Stempel 1986, 582). While political trust is a broad concept, Norris (2000) and others describe it as generalized levels of trust of the political system, such as the institutions of government. Political mobilization incorporates citizen's active engagement in both traditional and non-traditional forms of political participation (Norris 2001, 217), however, consistent with modernist measures of civic engagement, this paper will not focus on non-traditional forms of mobilization such as protests and demonstrations, but rather will examine traditional forms of political mobilization.

Second, this paper hypothesizes that increased levels of cognitive mobilization will be positively associated with higher levels of civic engagement, and conversely, lower levels of cognitive mobilization will be negatively associated with levels of civic engagement. Even using measures of civic engagement structured on modernist conceptions of civic engagement, we still should expect cognitive mobilization to lead to increased civic engagement as those who are more cognitively

mobile possess skills which reduce barriers for engagement.

Data and Operationalization

This analysis will draw cross-sectional data from the 2011 Canadian Election Study (CES). The CES, with a sample size of 4308, employs four waves of surveys to sample Canadians. This analysis will make use of the campaign period survey, post-election survey and mail back survey. The first two waves of surveys are conducted through structured interviews over the telephone and the mail back is completed in hard copy. Because of the low sample sizes, questions from the web survey were not used in this analysis. The data provided by the 2011 CES is useful for this analysis because, like other national election studies used in civic engagement and political communication literature, it contains questions which serve as reliable indicators for measuring news exposure as well our broader concept of civic engagement. There is also an inherent benefit to using national election surveys when attempting to measure levels of civic engagement. According to Robinson the effects of a media malaise should be more pronounced during election campaigns (Robinson 1976, 427-429). Therefore, should a media malaise exist, we should find evidence within this data. Consistent with previous studies which have used individual level survey research, we expect to discover that a media malaise is not detectable in the relationship of news media on civic engagement in Canada.

For the operationalization of the independent variable a news exposure additive index was created which included questions which asked respondents how many days per week they: watch news on the television, read news in the newspaper, listen to news on the radio, and read news on the internet. These survey questions did not define what constituted news, allowing that distinction to be made by what the respondents understood as news. For the dependent variable, three separate additive indexes were created for political knowledge, trust, and mobilization. The political knowledge index was created with questions that asked respondents if they knew the name of: the current finance minister, the last governor general, their provincial premier, and if they knew which level of government is responsible for education and healthcare.

This is similar to how political knowledge has been measured in other analyses (Stolle and Cruz 2005; O'Neill 2001) Choosing one of the most fundamental aspects of political trust identified by the literature, the political trust additive index includes questions which probe respondent's confidence in: the federal government, provincial government, the civil service, and the courts. The political mobilization additive index incorporates questions tapping traditional participation including whether respondents had volunteered for a party or candidate in the last 12 months and if they had ever been a member of a political party, signed a petition or bought products for ethical reasons in the last twelve months.

Consistent with the literature (Dalton 1984), a cognitive mobilization index was operationalized using questions regarding respondent's level of formal education as well as interest in politics (Alaminos and Penalva 2002, 2). The index was comprised of the questions which asked what the highest level of formal education respondents had completed, how interested they were in politics generally, how many days per week they discussed politics with family, and how many days per week they discuss politics with friends.[3]

Limitations of the Analysis

Consistent with virtuous circle literature, one of the most significant limitations of this study is attributing causality to the relationship between media exposure and civic engagement. Are those who are more civically engaged more likely watch the news, or does news exposure create civically engaged citizens? This question cannot be resolved through this analysis. Furthermore, this study arguably casts a wide net in its treatment of the broad concept of civic engagement. In our analysis, each component of civic engagement could be examined individually in order to uncover more specific determinants of variation. While we cast a wide net in an attempt to capture the three core components of civic engagement, through the use of additional indicators much more could be said about each sub-concept individually. Further analysis may benefit from utilizing other data sets with more robust measures of civic engagement.

[3] See Appendix for Coding of variables within the index.

The data of the Canadian Election Survey itself can be seen as a limitation to the analysis of the effect of news media exposure on civic engagement. The presence of questions more specifically related to attention paid to the news rather than just exposure would render this analysis more precise. Although there are certain survey questions that address attention to the news, they are located in the web portion of the survey and have extremely low sample sizes. Usable CES questions probe respondents' exposure, but not necessarily attention to news. Specifically, we do not know what kind of news Canadians were watching or reading. Unusable questions probe which television networks and newspapers respondents obtained the majority of their news from. This information might aid in identifying different types of news consumers. Furthermore, as our analysis uses only cross-sectional data, any discussion of trends over time cannot be undertaken. The study is therefore a snapshot of the relationship between news exposure and civic engagement during the period of 2011. Future analysis might benefit from using longitudinal CES data from other election years in order to examine trends in Canadian civic engagement over time, as well as what might be driving them.

Findings

Univariate Analysis: General Variation

When examining the general variation of the independent variable of news media exposure, the frequency results show that 69 percent of respondents that provided a valid answer indicated that they consume news through television 5, 6 or 7 days a week. What this result indicates is that there is an overwhelming amount of respondents that are exposed to the news through television at a high level in a comparison to high level exposure to other mediums (newspaper: 41 percent, radio: 56 percent, internet: 30 percent). Looking back to the literature, this result shows that Robinson's (1976) assertion that television is the dominant source of political information still holds true despite the proliferation of new forms of media such as the internet (Robinson 1976, 409).

General variation in the dependent variable of civic engagement is examined through three concepts of

political mobilization, political trust and political knowledge and are all coded on an index ranging from 0 to 4, with 0 representing low and 4 representing high. The results for the concept of political mobilization show that of the 3295 respondents that provided a valid response, only 1 percent score a 4 (high political mobilization) and 33 percent score a 0 (low political mobilization) when examined through the particular measures used. The results of overall political trust show that 21 percent of respondents scored 2 (moderate), 20 percent scored 3, and 29 percent scored 4 (high), indicating that of the 1507 Canadians that provided a valid answer to all questions, 70 percent have a moderate to high level of political trust when examined through the particular measures used. The results of the concept political knowledge show that show that 22 percent of respondents scored 2 (moderate), 30 percent scored 3, and 22 percent scored 4 (high), indicating that of the 3356 Canadians that provided a valid answer to all questions, 74 percent have a moderate to high level of political knowledge according to the measures used.

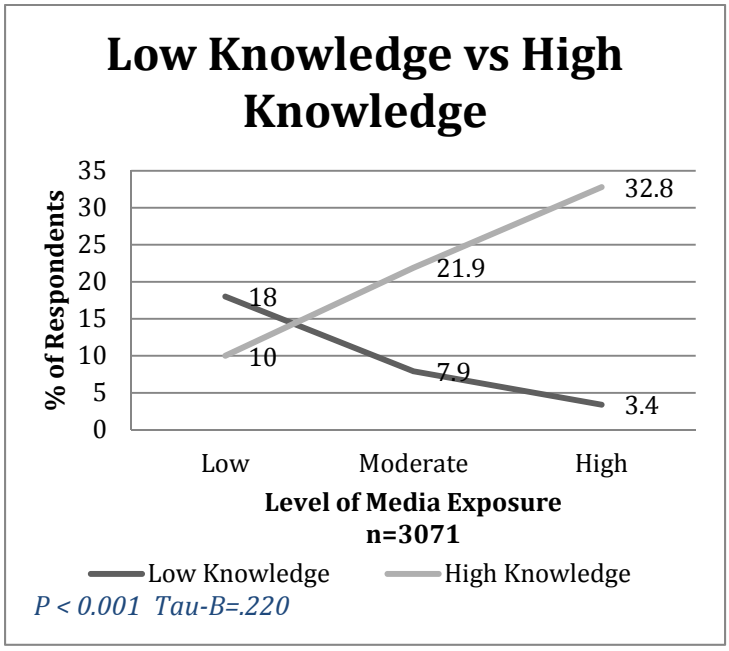
When these three concepts are combined into an aggregate index of civic engagement, the frequency results show that on a scale of 0 to 4 with 0 representing low civic engagement and 4 representing high civic engagement, 40 percent of respondents scored 2 (moderate), 42 percent scored 3, and 5 percent scored 4 (high), indicating that of the 1447 Canadians that provided a valid answer to all questions, 88 percent have a moderate to high level of civic engagement according to the measures used. However, it is important to note that only 5 percent of respondents have a high level of civic engagement, and that most respondents fall in the 2 to 3 range.

Bivariate Analysis

Moving beyond explaining initial variation observed across the variables incorporated in the analysis, the following section will present bivariate cross tabulation results measuring the relationship between the independent variable of news media exposure and the three indicators of civic engagement as well as the aggregated civic engagement index.

When examining an uncontrolled cross tabulation table examining the relationship between media exposure and political knowledge, there appears to be a

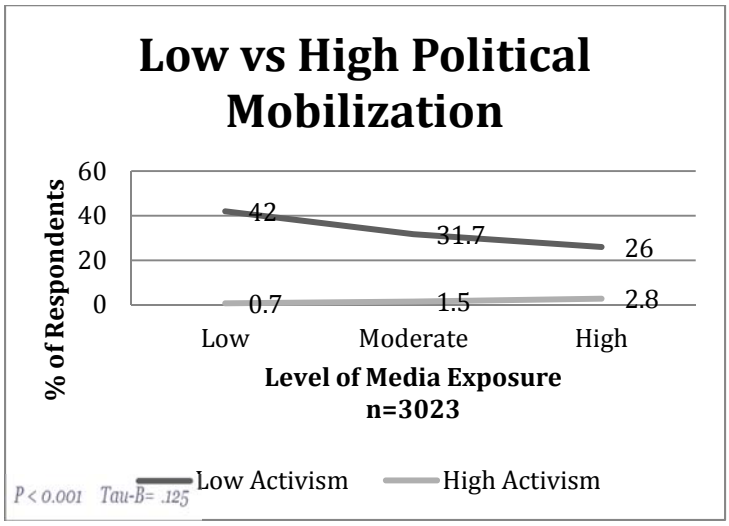
systematic relationship. The percentage of those with high levels of political knowledge more than triples as one moves from low to high media exposure. Of the 65 individuals who fell under low media exposure 10 percent also ranked high for political knowledge. However, of the 325 individuals who ranked high on media exposure, 32 percent of those also ranked high on the political knowledge index. Conversely, the percentage of those with low political knowledge decreases when moving from low to high media exposure. 18 percent of those with low media exposure also have low political knowledge, whereas of those with high media exposure, only 3 percent score low on political knowledge. This relationship is statistically significant with a confidence interval of 99.9 percent. The Kendall's tau-b value is .220 indicating a moderate relationship between the two variables.



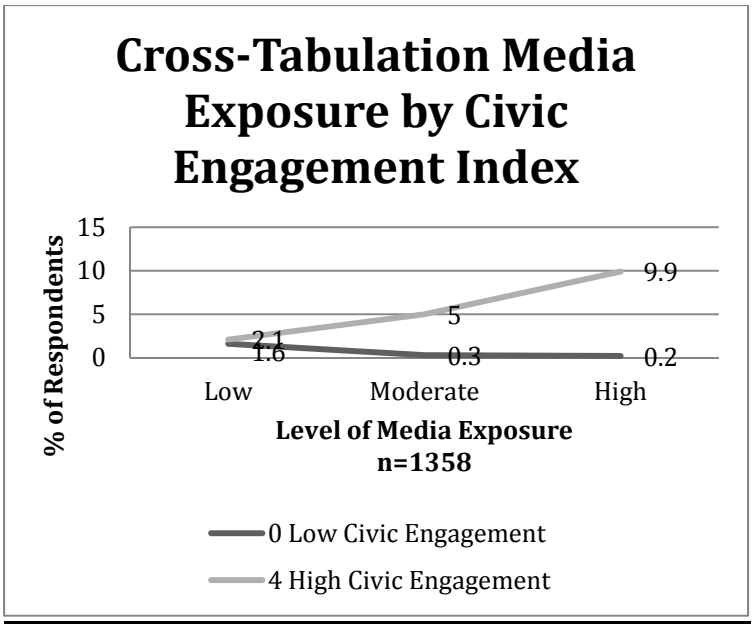
The cross tabulation of news media exposure and political trust, as measured by confidence in core government institutions, yields less conclusive results. The relationship does not meet the standard confidence interval of 95 percent, with a P value of 0.068. The Kendall's tau-b value is quite weak with a value of 0.041. This finding might indicate that media exposure directly does not have a significant impact on more diffuse political trust as measured by confidence in core

government institutions which has been identified as a component of civic engagement (Dalton 1999, 58).

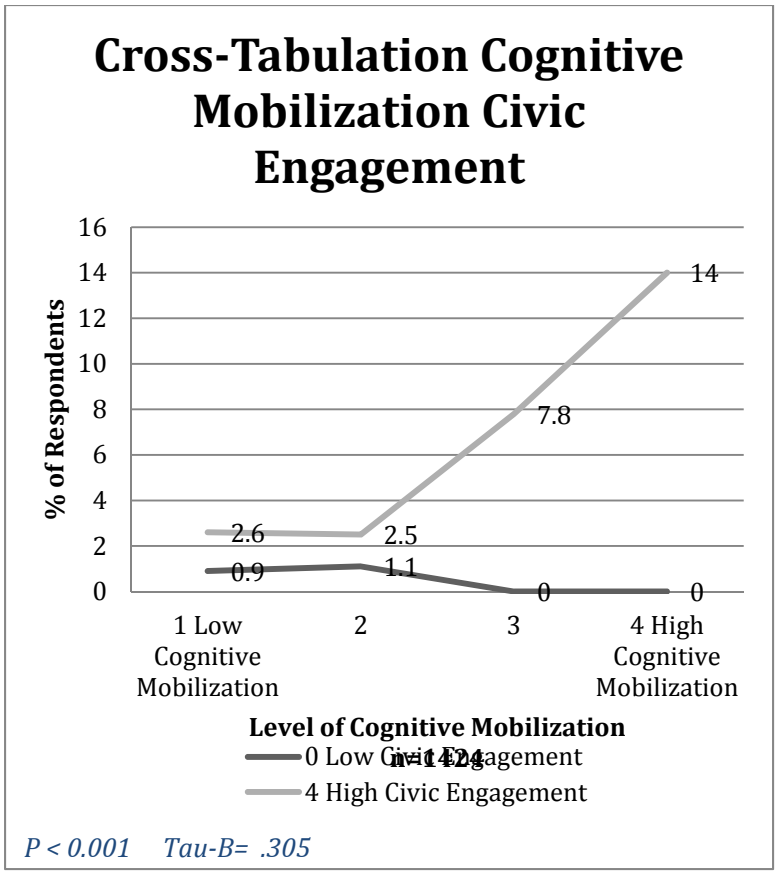
The relationship between news media exposure and levels of political mobilization appears to demonstrate a systematic relationship. The percentage of those with high political mobilization increases slightly when moving from low to high media exposure. It increases from 0.7 percent to 2 percent when moving from low to high media exposure. Of the 255 people with low media exposure, 42 percent also score low on the political mobilization index. This number decreases to 31 percent when examining the 253 people with high media exposure. The relationship is statistically significant with a confidence interval of 99.9 percent. The Kendall's Tau-b value for this relationship is 0.125 which indicates a moderate and positive relationship between the two variables.



The aggregate civic engagement index, which incorporates the three previously discussed variables, was also run in a simple cross tabulation against the independent variable of news media exposure. In the aggregate index, the percentage of those with high civic engagement increased from low (2 percent) to high media exposure (6 percent). We also observe that levels of low civic engagement decreases from 1.6 percent to 0.4 percent. The relationship proved statistically significant at $p<0.01$. The Kendall's Tau-b indicated a moderate relationship with a value of 0.173.



Based on the literature, we expected that cognitive mobilization may be a very important explanation of variation in levels of civic engagement, so a cross tabulation was run with cognitive mobilization (IV) against civic engagement (DV). This relationship was the strongest yet, with strong statistical significance at $p<0.01$ and a Kendall's Tau-b of .305 indicating a strong relationship. Before multivariate regression analysis, we already might expect that the impact of cognitive mobilization may be more significant than media exposure independently.



The next step of the analysis was to move beyond simple bivariate cross tabulations and utilize multivariate regression analysis. Four different regression formulas were run for this analysis. Each component of the aggregate civic engagement index (political knowledge, political trust, and political mobilization) was run individually in a regression analysis as the dependent variable. The fourth regression uses the final aggregate civic engagement index as the dependent variable. The regression model is comprised of our main independent variable in an addition to number of alternative independent variables. The alternative independent variables included in the regression model included: cognitive mobilization, individual feelings toward politicians, social trust, economic policy performance, gender, age, income, as well as region.[4]

[4] See appendix for operationalization of alternative independent variables. For the final regression analysis a dummy variable was inserted which ensured that each of the civic engagement indicators, when run individually, would have comparable samples. This

When examining political knowledge as the dependent variable we can see that media exposure does remain statistically significant and positively related to political knowledge. Those with higher media exposure may also have higher levels of knowledge about politics and public affairs. Despite this impact, it is clear that cognitive mobilization has a much stronger association with political knowledge. Additionally, social trust, gender, age, income, and region were also statistically significant, however with smaller impacts. This may indicate that there is weak but positive relationship between being: trusting of others, male, older, of higher income and living in Quebec with political knowledge. Feelings towards politicians, and perceived economic policy performance were not statistically significant.

News media exposure did not have a statistically significant impact on levels of political mobilization. Interestingly, cognitive mobilization was again statistically significant and had the strongest positive relationship with levels of political mobilization. It appears as though those who are the most cognitively mobilized might also be the most politically mobile as well. Social trust, gender and region were statistically significant indicating that there may be a weak relationship between: trusting others, being a male and higher political mobilization. Also there may be a weak yet negative relationship between living in Quebec and political mobilization.

For political trust, only feelings toward politicians and social trust were statistically significant. The results indicate that the more positive a person feels about politicians in general, the more confidence they will have in the core institutions of the government. Again, people who are more trusting of others may also have more confidence in the core institutions of the government which is considered a core component of political trust. Therefore, there may be a link between social trust and political trust.

When examining the final regression which

---

discrepancy needed to be addressed because the political trust index was drawn from mail back survey questions with a lower sample size than the other two indexes of political knowledge and mobilization. In addition, all of the values in the variables used in the regression model were standardized to range from 0 to 1 so that the B values could be interpreted and compared.

incorporates the aggregate civic engagement index, we are presented with few surprises. News media exposure remains statistically significant, while exhibiting a weak positive relationship with levels of overall civic engagement. However, caution should be taken when interpreting this value in the final regression. After having conducted individual regressions we know that the media's effect on political knowledge is driving up its value in the final regression. Not surprisingly, again we can see that cognitive mobilization appears to have the most significant impact on overall levels of civic engagement. The net impact of feelings toward politicians was more powerful than media exposure, however not as significant as cognitive mobilization.

Conclusion

Summary of Core Findings

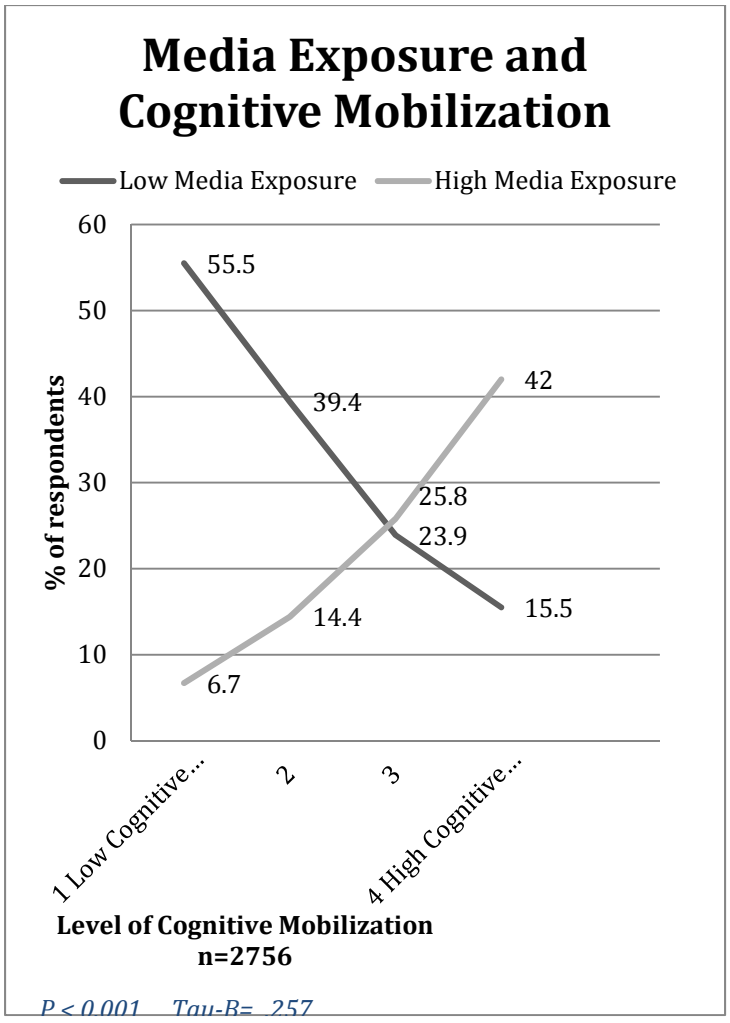
From the above analysis, it can be concluded that increased media exposure is associated with higher levels of civic engagement, with the concept of civic engagement derived from the additive index of political trust, mobilization and political knowledge. However, its impact is not consistent across the three components of the civic engagement index. After controlling for alternative explanations, media exposure can be said to have the greatest level of association with political knowledge but does not demonstrate a statistically significant impact on levels of political trust or political mobilization. Therefore, is there something else that may have a more pronounced influence on civic engagement as it has been defined than news media exposure? Of all of the explanations examined, cognitive mobilization appears to have the strongest positive impact on levels of civic engagement. This impact is strongest on measures of civic knowledge and political mobilization but not on levels of political trust. In our regression model, feelings toward politicians had the greatest impact on political trust, measured by confidence in core government institutions.

Reflecting Back on the Literature

Based on the above findings, the "media malaise" hypothesis can be called into doubt in the Canadian context. Through the use of multivariate regression, no evidence has been uncovered to support the idea that higher levels of exposure to the news media leads to

lower levels of civic engagement regardless of the quality of news media content. Furthermore, media malaise scholars contend that the negative effect of the news media on civic engagement should be most pronounced during election campaigns, yet no such effect has been observed using election period data, calling the presence of a media malaise in Canada into question. In every case where media exposure was statistically relevant, its effect was always a positive one.

There is a moderate relationship between cognitive mobilization and news media exposure. This finding falls into line with the virtuous circle hypothesis that contends that the media serves to "activate the active" by reducing the cognitive barriers for further engagement (Norris 2001, 229). Graph 5 demonstrates that as levels of cognitive mobilization increase, levels of media exposure also increase, while as levels of cognitive mobilization decrease, levels of media exposure also decrease. This relationship is moderate with a Tau-B score of .257. Based on these findings, it appears cognitive mobilization is significantly more related to civic engagement than media exposure alone.



So What?

This study fills a gap in the literature by examining the impact of news media exposure on civic engagement by situating the Canadian context within the virtuous circle and media malaise debate. The findings demonstrate that increased exposure to news media is positively associated with levels of political knowledge. This finding is important because political knowledge can be regarded as a key element of informed democratic participation on the part of the citizen, and the above analysis infers that the media may play a positive role in fostering political knowledge. This would call into question the premise of the media malaise thesis that negative media coverage alone contributes to ignorance of political actors and institutions among the Canadian citizenry.

From a policy perspective, if policy makers are seeking to understand what drives decreasing levels of civic engagement, they must look beyond the effect of media exposure and focus on other factors. Furthermore, to foster citizens that are more civically engaged in the political system, policy makers must focus on promoting even higher access to education and information about politics and public affairs, which can serve as the drivers of cognitive mobilization. It seems that the discussion should focus less on the tone of media coverage, and more on a concerted societal effort to create a more cognitively mobile citizenry, which includes increasing access to news media content. Based on the findings of our analysis, we agree with Norris who asserts that to continually blame the news media for society's problems is inherently harmful as it is a "perfect do nothing strategy" (Norris 2000, XV).

Appendix: Table 1: Regression Analysis of Canadian's Civic Engagement.

n=1567 *p < .05. ** p < 0.01 R-Square= .217

Variable	Civic Knowledge			Political Activism			Political Trust			Civic Engagement Index		
	B	*SE*	*Beta*	*B*	*SE*	*Beta*	*B*	*SE*	*Beta*	*B*	*SE*	*Beta*
News Exposure	.132**	.039	.11	---	---	---	---	---	----	.065**	.024	.086
Cognitive Mobilization	.312**	.049	.211	.425**	0.045	.316	---	----	----	.239**	.03	.253
Feelings Toward Politicians	-----	-----	-----	-----	---	---	---	.39**	.034	.354	.122	.017
Social Trust	.06**	.017	.087	.047**	.016	.092	.071**	.021	.105	.059**	.011	.165
Economic Performance	---	----	----	---	----	----	----	-----		---	---	---
Gender	-.064**	.017	-.116	.066**	.016	.132	----	----	----	---	---	---
Age	.085**	.031	.088	---	----	----	----	----	----	---	---	---
Income	.072**	.027	.087	---	---	---				.043*	.017	.08
Region	.101**	.019	.164	-.04**	.018	-.82	----	----	----	---	---	---

Works Cited

Alaminos, Antonio and Clemente Penalva. 2012. "The Cognitive Mobilization Index: Crises and Political Generations." *Sage Open:* DOI: 10.1177/2158244012440437.

Bennett, Stephen Earl, Staci L. Rhine, Richard S. Flickinger and Linda L.M. Bennett. 1999. "'VideoMalaise' Revisited: Public Trust in the Media and Government." *The Harvard International Journal of Press/Politics* 4: 8-23.

Cappella, Joseph N. and Kathleen Hall Jamieson. 1996. "News Frames, Political Cynicism, and Media Cynicism." *The Annals of the American Academy of Political and Social Science* 546: 71-84.

Culbertson, Hugh and Guido H. Stempel 1986."How Media Use and Reliance Affect Knowledge Level," *Communication Research* 13: 579-602.

Dalton, Russell J. 1984. "Cognitive Mobilization and Partisan Dealignment in Advanced Industrial Democracies." *The Journal of Politics* 46(1): 264-284.

Dalton, Russell J. 1999. "Support in Advanced Industrial Democracies," in *Critical Citizens: Global Support for Democratic Governance,* edited by Pippa Norris, 57-77. New York, NY: Oxford University Press.

Dalton, Russell J. 2008.*Citizen Politics: Public Opinion and Political Parties in Advanced Industrial Democracies*. Washington DC: CQ Press.

Inglehart, Ronald. 1970. "Cognitive Mobilization and European Identity." *Comparative Politics* 3: 45-70.

Inglehart, Ronald. 1999. "Postmodernization Erodes Respect for Authority, but Increases Support for Democracy," in *Critical Citizens: Global Support for Democratic Governance,* edited by

Pippa Norris. New York, NY: Oxford UP.

McAllister, Ian 1999. "The Economic Performance of Governments," in *Critical Citizens: Global Support for Democratic Governance,* edited by Pippa Norris. New York. NY: Oxford University Press.

Nadeau, Richard and Thierry Giasson. 2003. "Les médias et le malaise démocratique au Canada." *Choix* 9: 3-32.

Nevitte, Neil. 1996. *The Decline of Deference: Canadian Value Change in Cross National Perspective*. Toronto, ON: University of Toronto Press.

Newton, Kenneth. 1999. "Social and Political Trust in Established Democracies," in *Critical Citizens: Global Support for Democratic Governance,* edited by Pippa Norris. New York, NY: Oxford University Press.

Norris, Pippa and Ronald Inglehart. 2009. *Cosmopolitan Communications: Cultural Diversity in a Globalized World*. New York, NY: Cambridge University Press.

Norris, Pippa. 2005. *A Virtuous Circle: Political Communications in Postindustrial* Societies. New York, NY: Cambridge University Press.

Norris, Pippa. 2001. *Digital Divide: Civic Engagement, Information Poverty, and the Internet Worldwide*, New York, NY: Cambridge University Press.

O'Neill, B. 2001. "Generational Patterns in the Political Opinions and Behaviour of Canadians." *Policy Matters* 2(5): 1-41

Putnam, Robert. 2000. *Bowling Alone: The Collapse and Revival of American Community.* New York, NY: Simon & Schuster.

Robinson, Michael. 1976. "Public Affairs Television and the Growth of Political Malaise: The case of 'The selling of the Pentagon," *The American Political Science Review* 70: 409-432.

Stolle, Dietlind and Cesi Cruz. 2005. "Youth Civic Engagement in Canada: Implications for Public Policy." In *Social Capital in Action: Thematic Policy Studies*. Policy Research Initiative. Government of Canada.

Stolle, Dietlind and Marc Hooghe. 2005. "Inaccurate, Exceptional, One-sided or Irrelevant? The Debate about the Alleged Decline of Social Capital and Civic Engagement in Western Societies," *British Journal of Political Science* 35: 149-167.

Cultural Diplomacy beyond Governmental Control: A Museum Voice in seeding "Imperial" Cosmopolitanism

Natalia Grincheva, Concordia University

"It seems to me that the real political task in a society such as ours is to criticize the workings of institutions that appear to be both neutral and independent; to criticize and attack them in such a manner that the political violence that has always exercised itself obscurely through them will be unmasked ..." – Michel Foucault (Chomsky and Foucault 2013).

Introduction

In this paper I would like to consider Foucault's critique of institutions as a form of political power by looking at museums, which claim to operate independently on a global scale and indeed seem to be driven exclusively by institutional logic and interests outside the control of their nation states. However, their international communication and global public relations activities have significant implications in international politics and contribute to the official governmental efforts in cultural diplomacy. For example, the Guggenheim museum revolutionized the professional world of museums with new corporate politics of "global" museum franchise, based on the late capitalism logic. Though the Guggenheim has remained quite controversial in the professional museum world in terms of programming, exhibitions, and audience development, it brought significant transformations to the historical development of museums agency around the world through introducing such new processes as corporatization and global expansionism.

Acting on the international arena as a Multinational Corporation, the Guggenheim represents an ideal symbol of the U.S. market economy, promoting and transferring "capitalist" museum management practices and strategies to other countries worldwide. In this way, the museum can be understood as an independent political actor, (not commissioned by the government), that significantly contributes to the "soft" power of the United States in its efforts of promoting economic globalization and values of liberal economy and free market worldwide. Situating the research

within the neo-institutional theoretical framework and drawing on historical analysis, this paper explores the power and voice of American museums in the global projection of cosmopolitanism as the dominant frame of contemporary cultural reality. Specifically, the study looks at the privately funded Guggenheim museum, which positions itself as an independent global institution, promoting "universal" values among its large and diverse international audiences.

Literature review: cultural diplomacy in "transnational" world

Cultural diplomacy has traditionally been a political instrument of interacting with international publics. It is usually described through the notion of "soft power," coined and developed by Joseph Nye (2004), who argues that a country possesses "soft power" if it is capable of exploiting information to shape and inhabit the "mind space" of another country through the persuasive powers of attraction, by appealing to and promoting common cultural values (Nye 2004). The primary goal of cultural diplomacy activities has always been constructing a positive image of the country in the eyes of the foreign publics and creating a better climate for international trust and understanding. Since its inception, in the midst of the Cold War, cultural diplomacy has been exclusively governmental prerogative, exercised through the official high level diplomatic programs, facilitating international cultural exchanges across borders.

In recent years, in the conditions of increasing economic and cultural globalization, cultural diplomacy has acquired a strong cosmopolitan focus. Promotion of "universal" values within the cultural diplomacy discourse plays an important role in contemporary global society because it places the country within the international community and legitimates transnational activism and intervention in matters that would previously have been considered an exclusive domain of states and their citizens. Many scholars have observed that cosmopolitan rhetoric serves the interests of a particular group of the most influential political and economic actors/polities that promote themselves as global super powers. Being a "project of empires" (Calhoun 2003, 89), cosmopolitanism "is born out of privileges: economic; political; cultural; and even

linguistic" (Mendieta 2009, 242), and appreciates global diversity as long as it is based on advantages of wealth and citizenship in certain states (Kymlicka 1992; Ignatieff 1994; Calhoun 2003).

The discourses of "imperial" cosmopolitanism, promoting "universal" values of democracy, freedom, and liberal economy, are usually attributed to the diplomatic efforts of the most powerful political actors in the international arena, such as the USA (Spinelli 2000; Hauser and Grim 2004; Ish-shalom 2008; Crick 2010; Carothers 2011). Slaughter and Hale indicate, American "soft power" "has a deeply cosmopolitan dimension," promoting "a better life for all the world's citizens" (Slaughter and Hale 2010, 176). In opposition to this opinion, Beck argues, that the "cosmopolitanization of reality *is not the result of a cunning conspiracy on the part of 'global capitalists' or an 'American drive for world domination'* (Beck 2010, 60). In contrast, he sees the unprecedented growth of cosmopolitan discourse shaping the global cultural environments as "… an unforeseen social consequence … *within a network of global interdependence and its attendant risks*" (Beck 2010, 60). In line with this opinion, Nye also confirms that the forces of globalization and cosmopolitization are not "intrinsically American, even if much of its current content is heavily influenced by what happens in the United States" (Nye 2010, 168). Though, indeed, he emphasizes that in recent decades, the major forces of globalization were America-centric, which significantly enhanced the American "soft power" (Nye 2010, 170), it is simplistic to attribute it exclusively to the political will of the American government. He observes that, "…*organizations, groups and even individuals are becoming players,"* which push forward the forces of globalization and contribute to the development of cosmopolitan discourses (Nye 2010, 172).

Taking the same perspective, Iriye (1997) reveals, "*not all international relations consist of dealings among states and governments*." Various interactions outside this framework are based on the increasing international activity of independent organizations, which can reinforce global cosmopolitanism, by simply pursuing their own interests outside of the governmental agenda (Iriye 1997, 1). In this respect, I would like to explore the mechanisms,

which enable contemporary cultural institutions, such as large world-recognized museums, to become important actors in contemporary international politics, indirectly contributing to the national forces in cultural diplomacy and spreading cosmopolitan discourses.

The paper consists of four major parts, which methodically place the analysis of the Guggenheim international politics within the framework of neo-institutional theory. It starts with outlining the major principles of the theoretical foundations, which help to ground the analysis of the Guggenheim case, illustrating key theoretical claims of several neo-institutional theories. The following parts present empirical analysis situated within different dimensions of the theoretical framework and explore the Guggenheim international interactions from different angles. In this way, the paper discusses the museum's global activities driven by the logics of cosmopolitanism from the discursive institutional perspective and investigates the economic, cultural, and political drives behind the promotion of universalism as dominating frame of contemporary cultural discourse generated in the field of the "global" museums. Specifically, this study illuminates how various activities with apolitical intentions outside of the governmental control project strong political messages and exert political influences within a global environment of international communications.

Theoretical framework: "eclectic" approach in the study of institutions in contemporary international politics

The study is situated within the neo-institutional theory. It is one of the main theoretical perspectives used to understand organizational behavior, influenced by and influencing wider social and cultural environments, within which they operate. As Mayer indicates, it is one of the most suitable frameworks, which can provide a valuable perspective in exploring contemporary phenomena of the modern world, where "the old nation-state, with its passive bureaucracies, is reformulated as a modern organization, filled with agencies that *are to function as autonomous and accountable organizations… capable of the highly purposive pursuit of their own goals*" (Mayer 2007, 796). Furthermore, these rapidly expanding organizational structures in the world serve as agents for spreading "universal goods,

often at the global level" (Boli and Thomas 1999; Mayer 2007), thus creating conditions of increased cosmopolitization of cultural reality.

Within this framework, cultural and institutional forces are understood as institutionalized models exerting strong influences on the macro-social levels, including policies and practices in many countries (Bradley and Ramirez 1996; Ramirez et al. 1998; Mayer 2007). These institutional models "reflect successes and failures in organizational or international stratification systems, without necessarily reflecting the interests of the powerful bodies in that system" (Mayer 2007, 800). Considering that "globalization involves the construction of myths of underlying world similarity," the diffusion of successful organizational practices goes on as a matter of fashion (Strang and Meyer 1993), and reinforces universalism as the dominant frame of the social-cultural paradigm.

Specifically, I am drawing on the *discursive institutionalism* that can be better described as an accumulative and integrative approach comprising the theoretical foundations of earlier institutional perspectives in the study of international politics. *Discursive institutionalism* is an analytic framework that allows one to identify, describe, and analyze important phenomena through epistemological lenses of such foundational theories as *rational choice theory*, *historical* or *sociological institutionalisms*, and *phenomenological institutionalism* (Beyeler 2003).

Rational choice or realist institutionalism, arising particularly in economics and political science, stresses the importance of decisions and behaviors of "bounded, purposive, sovereign rational actors" (Mayer 2007, 790). These actors are usually described as organizations or polities with fixed preferences, which guide their strategic actions to maximize their economic or political advantages and lead to optimal solutions and results (Hardin 1982; Ostrom 1990; Mayer 2007; Schmidt 2010). From the economical angle, organizations are analyzed as independent institutions, operating in market-like environments, where the organizational strategic behavior is described through neo-liberal logic. This logic stresses the priority of the free enterprise, the system of competition, and the

independence of actors operating in a global market without the direct involvements of states (Mayer 2007, 790).

According to the *historical* or *sociological institutionalism* organizations are understood as historically predetermined paradigms of regularized practices, structures, actions, and outcomes. This theory predominantly draws on the path-dependencies and consequences of historical institutional development (DiMaggio and Powell 1983; Powell and DiMaggio 1991; Hall and Taylor 1996; Steinmo et al. 1992; Thelen 2003; Mayer 2007; Schmidt 2010). Within this framework, institutions' decisions and behaviors are shaped by institutional contexts, which have prior exogenous historical origins that can significantly influence cultural and organizational environments (Mayer 2007, 792).

Finally, within the *phenomenological institutionalism,* actors are seen not simply as influenced by wider contexts, but as constructed in and by it. Institutions, from this approach, "embody supra-individual abstract ideas, devices, and guiding ideas of what an institution is and what can legitimately be expected of it" (Beyeler 2003, 158). In this way, the world of international politics can be described in terms of *actorhood*, where appropriate actions are not seen as choices, decisions, or strictly prescribed historical conditions, but are understood as a complex interactions of the "culturally-specific practices, with institutions cast as the norms, cognitive frames, and meaning systems…" (Schmidt 2010). Rationality for *phenomenological institutionalism* is socially constructed and culturally and historically contingent, by which individuals *may be affected but not defined*. Instead, the theory stresses that norms, identities, and culture constitute interests, which are endogenous (Wendt 1987; Ruggie 1998; Schmidt 2010). The most important claim within that framework is that institutions can be changed "if the underlying values are eroding and identities with the previous institution get weaker." These changes occur through the processes of socialization and collective learning, resulting in the developments of new institutional identities (Börzel and Risse, 2000; Beyeler 2003, 158).

Discursive institutionalism does not exist apart from the described above neo-institutionalisms, but

differs from them in its logic of explanation, by offering a framework illuminating how and when ideas in global interactions of discourses empower actors to overcome constraints. "Rather than constituting an incommensurable, rival approach to the other three approaches, *discursive institutionalism* is complementary to them, by building upon these as it lends insight into the dynamics of change" (Schmidt 2010, 5). In the framework of the Guggenheim case study this approach is particularly instrumental. Considering the complexities of the cultural, historical, economical, and political reasoning behind the institutional behavior in the international arena, only *discursive institutionalism*, can provide insights into the dynamics of the institutional changes in the global environment, affecting the wider community. In this way, this study utilizes a more "eclectic" approach to the analysis, allowing the situating of the empirical findings within various foundational theories of neo-institutionalism.

Specifically, the *discursive institutionalism* provides a meaningful and valuable ground for exploring the Guggenheim international activities, because of its ability to place the research within the conditions of increasing globalization, empowering cosmopolitan discourses. As Beyeler indicates the impacts of globalization transcends across various dimensions, such as economical or cross-border market exchanges, international political exchanges, as well as the strengthening institutional powers within international integrations (Beyeler 2003, 158). The *rational choice* perspective helps to explain the economic interests of the Guggenheim within the global cultural markets. The *historical institutional* analysis provides valuable explanations of the national cultural conditions, under which the museum was founded and developed. Eventually, through *phenomenological institutional* lenses, it is possible to identify and explain the revolutionary forces of the Guggenheim within global discursive contexts, which not only influenced the museum field on the national level, but significantly affected museums' norms and canons on the global scale.

Realist institutionalism: Economic rationale of the global expansionism

The Guggenheim museum was established by one of the most successful American business dynasties, the

Guggenheim brothers, who immigrated from Switzerland and Germany around 1848 and in a short time managed to develop thriving mining businesses. Starting in Colorado, the family soon opened mining branches in Mexico, Alaska, and Chile. This international Guggenheim Empire gave rise not only to "the forces that shaped the emergence of multinational enterprises" and "modern world economy," spreading "the influence of technological innovation, capital markets, management, and the nation-state" around the world (O'Brien 1989, 124), but also provided some management models, which appeared applicable and successful in the world of contemporary museums.

In a professional museum world, the Guggenheim is known as an institution that significantly exceeded all other museums in successful application of the cultural logic of the late capitalist museum. It started a global brand building strategy and franchising museum movement as the most innovative museums practices, not only bringing exceptional revenues, but more importantly changing the global landscape of museum world, turning them into important nodes in a postindustrial economy (Conn 2010, 231). The Guggenheim in Bilbao was the first triumph of Krens, bringing more than $ 70 million to headquarters in New York through a Basque government donation and "rent fee," but more importantly giving birth to a whole new institution, such as transnational museum.

The strategies employed in Bilbao amplifies the corporate logic of the capitalist museum, which relies on impressive architecture, appealing to much larger audiences, including those who are not necessarily interested in art, commercial infrastructure around museums, and traveling collections, constantly circulating within the network and presented as dramatic performances through blockbusters exhibitions and shows (Rauen 2001, 291). More importantly, this formula, as Zulaika emphasizes, "can be marketed across the world from Wall Street/Manhattan, even becoming subject to a McDonaldized rationality… such international franchising makes the Guggenheim the most attractive museum for global capital" (Zulaika 2001, 112).

As many scholars indicate these successful experiences of the Guggenheim Museum have had tremendous impacts on the global practices in museums'

international and local activities, resulting in renovating museum architecture with attractive bold designs, expanding investment opportunities, and growing attention to enlarging audiences and enhancing visitor services (Dolan 1999, Brenson 2002). Furthermore, opening branches in other cities have been described by many analysts as one of the popular trends reflecting the culmination of the global changes in the management of museums (Werner 2005; Wu 2002; Vivant 2011, 99). As some cultural critics observe, the Guggenheim Foundation's growing international network has become "the leading model of globalization for museums," according to this model, a "global museum" is more competitive since it's able to attract sponsorship worldwide that a single-location museum could never hope to secure (Fraser 2006, 149). For example the museum franchising technology has been successfully deployed by the Tate Gallery, which now has branches in Cornwall and Liverpool, and even by "historically conservative Louvre," which has started building a new museum branch in Abu Dhabi (Sylvester 2009, 4).

This economic logic behind the museum global expansionism gives a premise to understand the international activities of the Guggenheim and its powerful influences over the international professional museum world in terms of *rationale choice theory*. In this perspective, the Guggenheim indeed can be described as a powerful, independent and economic interests-driven actor that is capable of developing and spreading new institutional museum models in the global arena. Furthermore, these institutionalized patterns, promoted on behalf of the Guggenheim museum, indirectly contribute to the U.S. governments' efforts in expanding global markets and supporting liberal economy. According to the official diplomatic discourse of the USA, an open world economy can push international relations in a cooperative direction, in this way leading not only to prosperity but also to peace. *Selling commercialism and liberalism* has been strategically and thoroughly integrated into the common logic and rhetoric of diplomacy aiming to establish good relationships with other nations (Ninkovich 1993, 54). Thus, tremendous influences on the international museum community, which transform museums into economic agents, operating under conditions of the

global liberal economy, clearly reflects the values and orientations of the American society.

In the age of globalization, institutional development, shaped by economic interests and global expansionism, results in "*universalization of policy logics*" (Drori et al. 2006a). As a result, various local, regional, and national social and organizational "traditions collide with the highly theorized universal claims for the application of social laws" (Gili at al 2009, 37). In search of financial stability and support from larger audiences and constituents, world recognized museums are relying less and less on their national heritage preservation and cultural traditions, while adopting and integrating the new models of franchise and capitalist museum, which "became more *uniform* on a global scale" (Delmestri 2009, 117). This shapes museums' public relations, marketing, and international cooperation activities in a more "universal" way, which happen to strongly resemble the canons of the American liberal economic standards. And at this exact point, the *rationale choice theory* fails to provide the required insights to uncover the complexities of the interaction between the national paradigms of American institutional economy with the global flows of ideological influence.

Within this theoretical model, the global changes are indeed pushed by major "protagonists," like the Guggenheim museum. However, these institutions are deeply involved in highly collective and cultural structures on different levels, which urge to go beyond a mere *realist institutional* way of reasoning. That's why in the assessment of global impacts of major powerful institutions it is important not only to consider a "zero-sum models, power and interest," provided above, but also engage in deeper explorations of the social roles and influences of larger contexts through the lenses of *historical institutionalism*.

Historical institutionalism: Commercialization logic in the American museum context

The worldwide spread of neoliberal ideologies is attributed by many scholars to the institutional logic specific to the U.S. cultural and economic contexts. Marketization and corporatization "carry with them the legitimacy and taken-for-grantedness of several hundred years of international theorizations about the efficiency

of markets" (Djelic and Sahlin-Andersson 2006). The Guggenheim museum is one of the most representative cultural institutions from the world of American museums that can showcase in the most expressive way the inherited ideology of liberalism and corporate structure of cultural institutions.

In the USA, a museum agency emerged notably due to individual initiatives, and not enforced by the public authority, like in other countries. Kimmelman indicates that from the very beginning the ideas around museums were closely linked to liberal economic values, which defined the social political context of the country:

> American museums, unlike most European ones, also have their roots in a strain of nineteenth-century political philosophy that specifically sought to *marry commerce with spectacle to achieve a form of social engineering (improving the middle class)*. They have always existed in a capitalist environment of winners and losers (Kimmelman 1999, 54).

This inherited commercialism within an American museum agency from the very beginning was also supported on the organizational or structural levels, because, museums were founded and run by economic elites. As Duncan reveals, the American public museum "is a monument to the powerful men who not only led the development of American finance capitalism, but also understood its cultural and ideological needs" (Duncan 1995, 70). Many historians indicate that a large amount of American museums were founded due to the considerable material and ideological contributions from financial magnates, who provided resources for acquiring art collections and also helped to establish museums' endowments:

> Andrew Mellon was collecting the paintings which would launch the National Gallery in Washington DC; JP Morgan's successors – the Havemeyers, the Rosenwalds, and other were filling New York's Metropolitan Museum. Samuel Kress, after building an empire on the basis of five-and-ten cent stores for Middle America, exercised his sense of stewardship by acquiring and distributing art both to major national collections and to smaller cities that had

> supporters his stores, donating fine art to dozens of provincial museums (Arndt 2005, 443).

These financial sources, on behalf of the American commercial elite, have retained their powers over museum agency through many generations "by setting the museum's general policy, governing all its programs and activities... caring of the museum's assets, including its collections and physical plant" (Glueck 1972, 119).

Outlining the current practices of American museums, the Report of the American Association of Museum Directors, emphasizes that commercial strategies within such an agency as an American museum have become even stronger in recent decades. Thus, the report stresses that earned income is becoming a larger part of the financial structure of all non-profit enterprises (AAMD 2006). Furthermore, the report highlights a stronger engagement of museums with for-profit companies, which extended from mere building infrastructures around museums, to organizing joint exhibition ventures (AAMD 2006). Andy Warhol once remarked, "All department stores will become museums and all museums will become department stores" (Gomez 2002, 43). However, as some museum scholars observe, many American museums have already established a strong tradition based on consumer psychology, according to which museums organize their spaces for the purpose of selling products, for example reproductions of the objects they possess. More importantly, these venues have become not only as a source of revenue, "but also as a defining factor in the public's museum going experience" (Toepler and Kirchberg 2006).

In this way, the museum sector in the USA has long established strong commercial strategies, promoted and supported in the cultural sector as an exclusively American way of museum management. This professional institutional nature shapes not only the peculiarities of how American museums interact with international counterparts, but, more importantly, defines the very essence and purpose of these interactions. In this sense, the Guggenheim is a museum, where inherited American commercialism, populism and financial adventurism achieves its highest level. Deborah Solomon, as cited by Sylvester, once described the

Guggenheim as "a *model* of frankness and *American pragmatism*… It does not pretend that art is religion or that the museum is church" (Sylvester 2009, 119). From the angle *of historical institutionalism*, the Guggenheim is a logical and expected product of social and economic interactions between institutions within the America environment.

This theoretical framework is heavily based on the Bourdieu's (1990) theoretical approach, which stressed historical social and material structures, defining institutional and individual behaviors within a particular society. He argued that social actors are produced by the interplay of their individual *habitus* and the structures of the particular field in which they are acting. According to Bourdieu, institutions cannot exist by themselves, but only through the practices related to them, institutions operating in the global arena cannot be taken separately from their "habitus," and the specific set of cultural practices integrated in the international context can be understood as a result of the constant dialectic exchange between the institutions and its national cultural economic surroundings. In this regard, on the international level Delmestri identifies so-called "institutional streams," or "disembedded institutional logics traveling as ideologies that are taken for granted" (Delmestri 2009, 115). These streams might influence interaction contexts within a global environment, providing institutional agents with symbolic elements, translatable and adaptable into local institutional arrangements. These translations can give rise to global institutional changes, which indirectly could serve the interests of the powerful actors, for whom promoting these institutional contexts can aid to spread specific political ideologies.

"Dominant transnational streams *may or may not* coalesce to form a global world order" (Delmestri 2009, 115). Because it is not clear how institutional streams as ideologies can be empowered to help the interests of the hegemonic projects (Delmestri 2009, 121), the *historical determinism in the institutional analysis* cannot fully and convincingly explain the institutional metamorphism taking place on the international level under the leadership of certain cultural agents. In this regard, the *phenomenological institutional* approach can prove to be more productive in exploring the global discursive

contexts, where cultural institutions operate, and influence each other.

Symbolic capital of the Guggenheim museum

As Mayer argues, in the international context, various institutional practices, which are naturally more linked to the world society in a globalized community, are more and more defined by the most powerful international professional discourses, "independent of the national state policies" (Mayer 2007, 803). Modern national organizational actors increasingly incorporate in their own structures and systems of conduct successful practices of the wider world cultures, so called "global standards" (McNeely 1995; Boli 1987; Mayer 2007). Furthermore, these institutional practices usually spread more "as cultural waves" promoting organizational structures in mutually constructed world discourses, "promulgated by professional consensus and associational advocacy" (Mayer 2007, 803). As a result, professionals and associations "generate highly rationalized and universalized pictures," which are being spread "*not principally via a power and incentive system*" of nation states, but through myriad of institutional discourses, promoted on behalf of independent professional actors (Mayer 2007, 804).

In the case of the Guggenheim, though the museum indeed in many ways reflects the national ideological paradigm of the American cultural management, more importantly it is influenced by its interconnection to the global economic environment, which largely shaped its revolutionary policies of international conduct. "Cultures, nationalities, and countries - the boundaries seem to be vanishing," the director of the Guggenheim, Krens stresses, explaining his vision on the development of the global expansion strategies: "The p*aradigm for me is to line up your institution with the international forces that are at work*" (Rauen 2001, 287). Trying to explain the main drives behind the development and success of the franchise museum model, which spread so widely and was adopted even by the museums, which severely criticized and rejected it, for example the Louvre, Krens repeatedly emphasized that institutional development was relying more on the exogenous factors in a larger international context. "Globalization is not an environment that we are shaping," Krens points out: "*It is being shaped around*

us. To try to resist these forces, or to somehow pretend they don't exist, I *think, is suicidal from an institutional standpoint*" (Krens 1999). In numerous interviews Krens stressed that "he did not create *the conditions he has been responding to*" (Brenson 2002, 6).

However, many scholars find such a position to be rather misleading, diminishing the important institutional role of the museum in promoting the American vision. These critics mainly interpret the Guggenheim transitional expansion as "the auratic miracle … the salvation of *American* culture" (Zulaika 2001, 113). Brensen describes the Guggenheim global phenomenon in more sharp terms as: "shaken by corporate corruption and led by an unilateralist president intent on promoting a Manichean world of 'moral clarity' in which *the American empire* is good and any individual, group, or nation that is not convinced of the inherent efficacy, decency, and wisdom of the free market and the corporate matrix on which it depends can be dismissed as adolescent, fanatical or other" (Brenson 2002, 6). From the theoretical stand point, Mayer confirms that these attacks on the most successful organizations, which are the most powerful engines of generating and spreading institutional models, are usually mistakenly associated with the "hegemonic" domination of particular nation states, such as the USA (Mayer 2007, 805).

In this critical literature, the Guggenheim museum is erroneously understood as an *active political agent* that significantly contributes to the "soft" power of the United States in its efforts of promoting economic globalization and values of liberal economy and free market worldwide. It is evident, however, that the Guggenheim has no direct connections with the U.S. government; in its international franchise activities, obviously, have different intentions in its international engagements. The museum has always stressed its independent nature, as the Guggenheim Deputy Director and Chief Curator emphasizes: "the *museum has traditionally been considered nonpartisan in terms of economic or political issues*, its only domain being that of quality…" (Spector 1993, 279). Addressing specifically the question of the Guggenheim place and role in the U.S. cultural diplomacy the Director of Curatorial Affairs at Guggenheim, Joan Young, shares: "I think, for the Guggenheim, *we are less*

*interested in U.S. cultural diplomacy in relation to our engagemen*t with audiences around the world. And our core collections predominantly feature the European artists …and throughout the history of our collection practices we focused more on international art rather than American … *our efforts in international programming, exhibitions and opening museums in different countries are not necessarily a contribution to the cultural diplomacy of the USA*, but more a contribution to the diplomacy of the *Arts*" (Young 2012).

Nevertheless, the museum indeed strongly projects the American values and conditions of liberal economy shaping the nature of national cultural institutions. As Spector further reveals "… like any social institution, it [the Guggenheim] *intersects with prevailing political ideologies and economic realities,* its purported neutrality providing a mask for *its own complicity with dominant social values and its reliance upon public patronage*" (Spector 1993, 279). Reflecting on that situation Kimmelman explains, "Mr. Krens was just taking advantage of an opportunity, which is the way of *the open marketplace*. It may be that he makes people uncomfortable precisely, because he is *pursuing the American cultural system to its inevitable conclusion*" (Kimmelman 1999, 54). As a result, many cultural critics describe the Guggenheim as a "superpower hegemon, seducing locals into paying through their noses for the 'privilege' of having its brand and its protection" (Sylvester 2009, 120). Sorking points out, the "brand strategy" of the Guggenheim expansion works well for spreading imperialistic powers, because "the value of the brand can only be defended, therefore, by greater and greater co-optation. *Branding is the medium of empire*" (Sorkin 2005, 31). As Rauen indicates, by embracing the "*Guggenheim concept*" cities and communities "disconnect from their geography," from their national cultural and local histories and connect to "particular *globally oriented ideology*" (Rauen 2001, 296). Thus, through cultural imports, such as collections and architecture, places of the Guggenheim franchises "undersell their own cultural identity," while trying to appeal to tourists and exhibit "their modernity, internationalism, and maturity" (Dolan 1999, 60).

However, in opposition to these accusations, Gili et al. observe that "*no one international organization –*

neither a corporation nor an intergovernmental agency – *has been particularly important in delivering the sweeping global changes,*" and the "*dominating participants in world society such as the leading national states* (e.g., the United States) and the *leading capitalist firms* have *by no means been special protagonists*" of imposing organizational and cultural ideologies worldwide and coercing institutions to adopt specific policies (Gili at al. 2009, 24). This group of authors argues that, there are complex processes of institutional socializations and mutual influences in the global discourses, identifying and promoting particularly successful practices and models, being further voluntarily adopted and integrated by organizations on a global scale.

In line with these claims, Go (2008) borrows Bourdieu's concept of the "*global field"* to describe a worldwide arena in which states and other actors, including corporations, nongovernmental institutions, and international organizations operate in a multidimensional "space of relations," and compete for various forms of capital, including economic, political, and symbolic (or institutional legitimacy). Furthermore, he stresses the crucial role of the symbolic capital, as the most powerful force that shapes international discourses, and influences the installment of "universalized" paradigms of professional and social cultural development among organizations. Symbolic capital in this way helps to generate and accumulate both, economic and political power (Go 2008, 208). In case with the Guggenheim museum, this, so called, symbolic capital has been understood by the museum in terms of its international significance, and global relevance. For example, Young stresses: "I think that the Guggenheim does have a global aspiration and global nature from the institutional perspective, despite of the fact that it was first found in the USA. I think it is more a global institution and we probably are better known in the world than among certain American audiences…" (Young 2012).

The principles of globalism have been closely integrated in the institutional philosophy from the first days of the museum inception. However, this symbolic capital has acquired a real power in the age of increasing globalization, when the Guggenheim could capitalize on its historical international connections to fully develop

the expansionism model of museum franchise. The museum has consistently positioned itself as a global, "universal" museum, which does not necessarily belong to the American context. By broadening its geographic scope and establishing worldwide alliances, the Guggenheim accumulates a powerful symbolic capital, which can position it "*to participate in*, *rather than merely represent*, *visual culture around the globe*" (Guggenheim Museum 2000). This museum discourse clearly emphasizes, that the museum's ambitions along with its practices go far beyond mere representing the U.S. ideologies of liberal democracy and cultural freedom of market economy. The Guggenheim aspires for being an independent international institution with an international mandate and authority to shape the global artistic development. In this way it significantly contributes to the articulation, formation and development of the international museum discourse, where the symbolic power of "global brands" helps to establish crucial connections to economic and human resources and accumulate a political power outside of the state authority.

Conclusion

Drawing on the case study of the Guggenheim museum and situating the analysis within the *discursive institutional* theoretical framework, this article illuminates the complex processes taking place in the contemporary international arena. The globalization of world affairs has had a strong impact on the dominant roles of institutions as "indirect" advocates of cultural, social, and professional norms and values, widely influencing domestic cultural policies, as well as global movements. First, the article demonstrates that the Guggenheim museum, as a modern organization, understood in terms of "bounded, purposive, and rationalized sovereign actor" (Gili at al. 2009, 17), has strong capacities to pursue its organizational interest in the international arena, which gives a premise to interpret its activities within the *rational choice* theoretical model of neo-institutionalism. However, the case study also proves that from the *historical institutional* perspective, the Guggenheim corporate structure of late capitalist museum is deeply grounded in the institutional context of the American cultural and economic situation. This national museum context in many ways shapes the Guggenheim practices, but does

not necessarily translate into the museum's direct intentions to spread or promote the American cultural paradigm in the global arena. From the *phenomenological institutionalism* angle, the study reveals that the Guggenheim museum is a part of the larger global environment, to which it responds through its international development strategies as an empowered agent, capitalizing on the symbolic capital of its international resources.

Returning back to our initial question of the role and place of the Guggenheim in the cultural diplomacy of the USA, it is important to note here, that the political power, attributed to the museum as an "agent of American ideology," should not be confused with the Guggenheim global leadership in establishing and building transnational museums networks. Incorporating cultural capital of national historical context, the Guggenheim pursues its individual institutional goals outside of the U.S. government's diplomatic agenda. However, the museum's tremendous success, as the first global museum, projects the victory of the neo-liberal economy and the power of the cosmopolitization in the postmodern globalized world, as a specific form of the symbolic capital.

Works Cited

Adam, T. 1939. *The Museum and Popular Culture*. New York: American Association for Adult Education.

Arndt, R. 2005. *First Resort of Kings, American Cultural Diplomacy in the 20th century*. Washington DC: Potomac Books.

Association of Art Museum Directors (AAMD). 2006. *Exhibition Collaborations between American Art Museums and For-Profit Enterprises*. Accessed January 14. http://bit.ly/17LVs7w.

Beck, U. 2010. "Realistic Cosmopolitanism How Do Societies Handle Otherness?" In: H. Moore and D. Held. *Cultural Politics in a Global Age*. Oxford: One World Press.

Beyeler, M. 2003. "Globalization, Europeanization and Domestic Welfare State Reforms: New Institutionalist Concepts." *Global Social Policy* 3: 153-172.

Boli, J. 1987. "World-polity sources of expanding state authority and organization, 1870- 1970." In: G. Thomas et al., *Institutional structure*. Beverly Hills: Sage.

Boli, J., and Thomas, G. 1999. *Constructing world culture: International non-governmental organizations since 1875*. Stanford: Stanford University Press.

Bourdieu, P. 1990. *In Other Words*. Cambridge: Polity.

Brenson, M. 2002. *The Guggenheim, Corporate Populism, and the Future of Corporate Museum*. New York: Vera List Center for Art and Politics.

Calhoun, C. 2003. "The Class Consciousness of Frequent Travelers: Towards a Critique of Actually Existing Cosmopolitanism." In: D. Archibugi and M. Koening-Archibugi. *Debating Cosmopolitics*. Verso.

Carothers, T. 2011. *Aiding Democracy Abroad: The Learning Curve*. Carnegie Endowment.

Chomsky, N. and Foucault, M. 2013. *The Chomsky - Foucault Debate: On Human Nature*. New York, NY: The New Press.

Conn, S. 2010. *Do Museums Still Need Objects?* Philadelphia: University of Pennsylvania Press.

Crick, N. 2010. *Democracy and Rhetoric: John Dewey on the Arts of Becoming*. Columbia, SC: University of South Carolina Press.

Delmestri, G. 2009. "Institutional Streams, Logics, and Fields." In: E. Renate, S. Meyer, and W. Ventresca. *Institutions and Ideology*. Bingley, UK: Emerald Group Publishing.

DiMaggio, P. 1988. "Interest and agency in institutional theory." In: L. Zucker. *Institutional patterns and organizations*. Cambridge: Ballinger.

DiMaggio, P.J., and Powell, W.W. 1983. "The iron cage revisited: Institutional isomorphism and collective rationality in organizational fields." *American Sociological Review* 48(2): 147–160.

Djelic, M., and Sahlin-Andersson, K. 2006. *Transnational governance. Institutional dynamics of regulation.* Cambridge: Cambridge University Press.

Dolan, D. 1999. "Cultural franchising, imperialism and globalisation: What's new?" *International Journal of Heritage Studies* 5(1): 58-64.

Drori, G. S., Meyer, J. W., and Hwang, H. 2006. *Globalization and organization: World society and organizational change*. Oxford: Oxford University Press.

Duncan, C. 1995 *Civilizing Rituals Inside Public Art Museums*. Psychology Press.

Fraser, A. 2006. "Isn't This a Wonderful Place? A Tour of a Tour of the Guggenheim Bilbao." In: I. Karp, L. Szwaja. *Museum Frictions*. Durham, NC: Duke University Press.

Glueck, G. 1972. "Power and esthetics: The trustee in O Doherty." In: G. Braziller. *Museums in crisis*. Ann Arbor, MI: The University of Michigan Press.

Go, J. 2008. “Global Fields and Imperial Forms: Field Theory and the British and American Empires.” *Sociological Theory* 26(3): 201-229.

Gomez, E. 2002. “If Art is a Commodity, Shopping Can Be an Art.” *The New York Times*, December 8.

Guggenheim Museum. 2000. The Global Guggenheim. Accessed January 14. http://bit.ly/1a5q927

Hall, P. and Taylor, R. 1996. “Political Science and the Three New Institutionalisms,” *Political Studies* 1(1): 952-973.

Hardin, R. 1982. *Collective Action*. Baltimore, MD: Johns Hopkins.

Hauser, G. and Grim, A. 2004. *Rhetorical Democracy*. Mahwah, NJ: Routledge.

Ignatieff, M. 1994. *Blood and Belonging: Journeys into the New Nationalism*. New York: Farrar, Straus & Giroux.

Iriye, A. 1997. *Cultural Internationalism and World Order*. London: John Hopkins University Press.

Ish-shalom, P. 2008. “The Rhetorical Capital of Theories: The Democratic Peace and the Road to the Roadmap.” *International Political Science Review* 29(3): 281–301.

Krens, T. 1999. “The Art Show, at Manhattan's Seventh Regiment Armory.” February 20, 1999.

Kymlicka, W. 1992. “Citizenship in an Era of Globalization: Commentary on Held.” *University of Michigan Journal of Law Reform* 25(3-4):112–126.

McNeely, C. 1995. *Constructing the nation state: International organization and prescriptive action*. Westport: Greenwood Press.

Mendieta, E. 2009. “From imperial to dialogical cosmopolitanism.” *Ethics & Global Politics* 2 (3): 241-258.

Meyer, J. 2007. “Reflections on Institutional Theories of Organizations.” In: R. Greenwood, C. Oliver, R. Suddaby, and K. Sahlin-Andersson. *The Handbook of Organizational Institutionalism.* Thousand Oaks, CA: Sage.

Ninkovich, F. 1993. Commercial and Cultural Internationalism after the Cold War Exporting America. In: R. Horwitz. *Exporting America:* Essays *on American Studies Abroad*. Michigan, Garland Pub: Political Science.

Nye, J. 2010. "Culture, Soft Power, and 'Americanization.'" In: H. Moore, and D. Held. *Cultural Politics in a Global Age*. Oxford: One World Press.

Nye, J. 2004. *Soft Power: The Means to Success in World Politics*. New York: Public Affairs.

O'Brien, T. 1989. "Rich beyond the Dreams of Avarice": The Guggenheims in Chile." *The Business History Review*, 63(1): 122-159.

Ostrom, E. 1990. *Governing the Commons*. New York: Cambridge.

Rauen, M. 2001. "Reflections on the Space of Flows: The Guggenheim Museum Bilbao." *The Journal of Arts Management, Law, and Society* 30(4): 283-300.

Schmidt, V. 2010. "Give Peace a Chance: Reconciling Four (Not Three) New Institutionalisms." In: D. Beland, and R. Cox, H. *Ideas and Politics in Social Science Research*. Oxford: Oxford University Press.

Slaughter, A. and Hale, T. 2010. "Calling All Patriots: The Cosmopolitan Appeal of Americanism." In: H. Moore, and D. Held. *Cultural Politics in a Global Age*. Oxford: One World Press.

Sorkin, M. 2005. "Brand Aid or The Lexus and the Guggenheim (Further Tales of the Notorious B.I.G. ness).: In: W. Saunders. *Commodification and Spectacle in Architecture*. Minneapolis, MN: University of Minnesota Press.

Spinelli, M. 2000. "Democratic rhetoric and emergent media." *International journal of cultural studies* 3(2): 268–278.

Steinmo, S., Thelen, K., Longstreth, F. 1992. *Structuring Politics Historical Institutionalism in Comparative Analysis*. Cambridge: Cambridge University Press.

Sylvester, C. 2009. *Art/Museums: International Relations Where We Least Expect It*. London: Paradigm Publishers.

Thelen, K. 2003. "How Institutions Evolve: Insights from Comparative Historical Analysis." In: J. Mahoney and D. Ruschemeyer. *Comparative Historical Analysis in the Social Sciences*. New York: Cambridge University Press.

Toepler, S. and Kirchberg, V. 2014. "Museums, Merchandising, and Non-Profit Commercialization." National Center on Non-Profit Enterprise. Accessed January 14. http://bit.ly/Pdgaoh

Vivant, E. 2011. "Who brands whom? The role of local authorities in the branching of art museums." *Town Planning Review*, 82(1): 99-115.

Werner, P. 2005. *Museum, Inc: Inside the Global Art World*. Chicago: Prickly Paradigm Press.

Wu, C. 2002. *Privatizing Culture. Corporate Art Intervention since the 1980s*. London: Verso.

Young, J. 2012. Telephone interview. Conducted by Natalia Grincheva, 11/9/2012.

Zulaika, J. 2001. "Krens's Taj Mahal: The Guggenheim's Global Love." *Museum Discourse* 23 (1): 100-118.

'*How* We Talk in Politics': A Critical Analysis of the American, Elitist Pro-Drone Political Discourse

Gabriel Boulianne Gobeil, University of Ottawa

I: Introduction

In a talk he gave at the University of Ottawa Faculty of Law, David D. Cole (2013) said that wars are won by either detaining the enemy long enough or by killing enough of its soldiers that it surrenders. Cole explains that killings are therefore unfortunate yet (almost) inevitable during wars. However, how can the United States' (hereinafter US) drone policy—regarded as one of targeted killings—be justified during peacetime, namely in countries where the US is not officially at war but has conducted strikes? This question also merits attention because the US, as a democratic state, should treat its citizens as "political equals" (Dahl 1971, 1). Yet, its drone program is responsible for the death of (at least) four US citizens, including one who was intentionally targeted and killed (Ackerman and Shachtman 2013). The US did not state for which crime Anwar Awlaki's teenage son was targeted (ibid.), suggesting that his death was arbitrary and his life not deemed as important as those of other American citizens.

What discursive rationale enables an alleged democracy to kill its own subjects, fully curtailing their rights? Analyzing how drone strikes are normalized by the US may help us find the answer to the previous inquiry. Hence, the purpose of this paper is to answer the following research question: what rhetorical mechanisms are at play in the US pro-drone political discourse?[5] It will attempt to examine "*how* [emphasis added] we talk in politics" (Saurette and Gordon 2013, 157).[6] Through an examination and a critical analysis of the official and unofficial US political discourse on drone strikes, this paper hypothesizes that the US pro-drone discourse is constituted by American exceptionalism, which

[5] In this paper, the US' political discourse includes Democrats, Republicans and Independents.

[6] This paper does not attempt to trace the history of the current US pro-drone discourse and situate it in the overall US foreign policy discourse of past presidencies. It merely aims to understand how the current discourse is being articulated.

subsequently reinforces that ideology.[7] To test this hypothesis, this paper will dissect the pro-drone discourse and attempt to show that the way it is articulated and framed contributes to the *normal*ization of strikes. This discursive logic is circular: exceptionalism allows the US to determine the exceptional (terrorist threat), emphasizing the normality of strikes, which then orients the emphasis on the exceptional anew.

Before going any further, why and how is this particular research relevant? First, the use of drones by the US government has increased significantly in the recent years. Although this intensification is slowing down, it shows no sign of stopping; robots in general and drones more specifically will be present in future wars and "they will take on greater roles" (Singer 2009c, 430). Given the revolutionary impact robots and drones have on war and politics, it is imperative to examine the logic behind their use. This is because this revolution "is forcing us to reshape, reevaluate, and reconsider what we thought we knew before" (ibid.). Thus, investigating the discourse behind their utilization is important, for it can inform us about potential uses of other similar technologies that may have not yet been invented.

Second, perusing the pro-drone discourse can tell us about the US' ideology. An "action-oriented sets of beliefs" (Eagleton 2007, 2) is a particularly interesting definition of ideology since strikes undeniably represents an 'action' and the pro-drone discourse must therefore characterize a 'set of beliefs' 'orienting' this action. Thus, analyzing this 'action-oriented' discourse should be revealing of US ideology. Discourse analysis is also useful to decipher how (ideological) beliefs are actualized (Wodak and Krzyżanowski 2008, 184); it shows how ideologies are put into practice.

II: Theoretical Approaches

Carol Cohn argues that assimilating a new "language is a transformative, rather than an additive, process" (1987, 716). If it were additive, learning a language would enable one to say more words and express oneself with a more diverse range of nuances. Because it is transformative however, the acquisition of language may

[7] The focus here is on the political elite—articulating the official US discourse—and those who can most influence this elite, voicing the unofficial discourse.

forestall linguistic overtones that would have been possible prior to the learning of that parlance. She argues: "language shapes your categories of thought [...] and defines the boundaries of imagination" (ibid., 714). Once she had learnt the technostrategic language—a language peculiar to nuclear strategic thinking—she was no longer able to express herself the way she would have prior to its learning (ibid., 713). This implies that language and the words it is comprised of matter. Cohn's work will be used in this research because the *way* the US frames its pro-drone discourse counts. Cohn explains that if the words "collateral damage" are substituted by those of "mass murder" the nuclear strategic experts then talk about two different things—conceptually speaking (ibid., 709). Factually speaking however, they talk about the same phenomenon: countless deaths. The important difference lays in the concepts. When US Attorney General Eric Holder (2012) claims that drone strikes are not "assassinations," but rather acts of "self defense," he engages in the same discursive mechanism as nuclear strategic experts, using a different language to expunge dissenting nuances. Language fashions the object it talks about while enabling those using it to act in ways that would be inconceivable were it not for that new language (Cohn 1987, 690). This argument will be used to assess the US pro-drone discourse.

George Lakoff's (2009) work may contribute to this research in two respects: firstly through his take on narratives and framing processes and secondly through his concept of biconceptualism. Lakoff explains that narratives are similar to stories present in our cultures, which our brains interpret (2009, 21). He gives the example of the Villain and the Hero (ibid., 24). While the former is perceived as bad, the latter is viewed as good. In this particular narrative, the Villain usually disturbs the peaceful balance by committing a crime on a Victim and the Hero restores that balance by saving the Victim and punishing the Villain. According to Lakoff, 'neural binding'—a process taking place in the brain—allows a person to associate the Hero, the Victim and the Villain from the fictional story to real life individuals (ibid., 25). Human beings make sense of the world around them by linking events to many narratives, together forming what he calls a "[c]omplex narrative" (ibid., 22). This process is called framing.

Two elements make these narratives crucial. First, our brains can only make sense of the world through narratives they already know even when framing is done unconsciously (ibid., 34). Second, once they have entered our brains narratives do not go away (ibid., 36). This is important because once the US lays out a given narrative to normalize its use of drone strikes, moving away from the narratives utilized and their associated frames becomes hard. The choice of the narrative being used matters. Lakoff notes that in 1991 president Bush attempted to justify the US' involvement in Iraq using a 'self-defense' narrative since Iraq's invasion of Kuwait jeopardized US oil supplies (ibid.). According to Lakoff, this narrative did not work because the American public did not want to send soldiers for oil; instead, Bush had to employ a 'rescue' narrative, which was a more palatable reason for intervening. The latter consisted of the US (Hero) rescuing Kuwait (Victim) that had been attacked (raped) by Iraq (Villain) (ibid., 36-37). When Barack Obama (2013) declares that "America does not take strikes to punish individuals; [it] act[s] against terrorists who pose a continuing and imminent threat to the American people" the president frames his drone program within the context of the US *counter*terrorism strategy, using a 'self-defense' narrative that can be more easily fed to the public.

Biconceptualism can be understood as the presence of both 'progressive' and 'conservative' views (regarding different issues) in the brain of the same individual (Lakoff 2009, 70). How can Obama (2009) "[ban] the use of so-called enhanced interrogation techniques by the United States [... and] order the closing of the prison camp at Guantanamo Bay"—decisions favorable to human rights—yet be willing to use drone strikes, arguably violating human rights? The concept of biconceptualism may help us understand why Obama seems to have a pro-human rights take on torture and Guantanamo while supporting drone strikes. Biconceptualism may contribute to the analysis of the pro-drone discourse in that it tells us how (not why) a certain thought process may be chosen over another antithetical one.

Sherene H. Razack's (2004) approach to racism in the Canadian peacekeeping mission in Somalia may prove insightful. She explains that 'colour line'—a notional divide between the 'civilized' First World and

the 'uncivilized' Third World—is a principle stemming from racism, constituting the mindset of the First World in its dealing with the Third World and having real world effects on the latter (Razack 2004, 7). Razack argues that, although it was present prior to the terrorist attacks of September 2001, colour line is now a permanent rudiment of the West's ideology in the post-9/11 era (ibid.). Regarding the resort to violence within the context of peacekeeping missions, she rejects the 'bad apple' argument, claiming that the use of violence is rather representative of a norm—grounded in racism (ibid., 12, 53). Peacekeeping missions are therefore a contemporary form of colonialism (ibid., 4). Razack even substitutes the term 'peacekeeping' for 'peace enforcement,' denoting the colonial nature of Canada's involvement in Somalia (ibid., 69). Razack claims that colour line offers a critical assessment of the colonial ideology manifested in peacekeeping missions (ibid., 86). It explains how violence is normalized in peacekeeping missions. It can also help us understand the increasing—and apparently normalizing—use of US drone strikes.

Razack's (2008) concept of 'race thinking' may add to the assessment of the US pro-drone discourse. Race thinking, defined as the separation of two groups of human beings and the subordination of one over the other, permanently characterizes the world within the overarching setting of the war on terror (Razack 2008, 6, 22). It is similar to colour line for Razack uses the latter concept to describe the former. The main difference is that race thinking involves the creation of two distinct legal spaces. The first space is that in which the majority of individuals finds themselves and enjoy its rights fully. The second is one of exception, which Razack compares to a camp, where only some individuals find themselves—with virtually no rights (ibid., 6). She adds that racism underlies the creation of these camps. The belief behind race thinking is simple; by removing the rights of those placed within camps the security of those outside is ensured (ibid., 9). When two such systems of law are added to race thinking, concentration camps are created, representing colonialism (ibid., 28).

Race thinking is behind the strategy of "profiling [...] on the basis of race, religion, and life history" (ibid., 35). Being *profiled* as a potential terrorist or as having possible connections with (a) terrorist organization(s) is

a sufficient ground to be interned (ibid., 40). Based on Obama's (2013) explanation of who is being targeted by drones, targets fit that exact description. This is because targets—individuals deemed to represent an "imminent threat" (Obama 2013)—need not have committed any crimes to be struck; they simply *may* have had they been left alive. Hence, by being deprived of habeas corpus and any other rights, drone targets are camped. Using race thinking, along with the other three theories presented above, may therefore help us appraise the US pro-drone discourse.

III: Methodological Choices

Given the contentiousness of the drone strikes issue, it is important to explain the first methodological choice of this research. The pro-drone discourse is the only side of the debate that will be under study. That is, the anti-drone discourse (in the US as well as elsewhere) is purposely absent from this paper. The desire to employ CDA exhaustively on the pro-drone discourse in conjunction with space constraints compelled that alternative. Using CDA on the anti-drone discourse—with different theoretical approaches—would constitute an interesting and valuable research project nonetheless, which could be the enterprise of future work. This, however, is not the endeavor of the present paper. Another reason for focusing on the pro- side of the discourse is based on the fact that ideologies have an action-oriented component. Because drones strikes *are* being conducted, the (in)action that the anti- side of the discourse tries to orient—the non-use of strikes—is *not* being implemented. However, the action promoted by the pro-side *is*. R. B. J. Walker explains that "[t]he line between the international and the imperial is very difficult to identify with any clarity" (2006, 67). Building on Walker, it is possible to understand that exceptionalism is the ability to determine what the exception is and to therefore normalize everything that is in reaction to it, but that would have initially been considered imperial were it not for exceptionalism. An example of exceptionalism is when the US declares the war on terror(ism) to be the exception and consequently normalizes the use of drone strikes as part of its counterterrorism strategy. Thus, it is worthwhile to look

at the *pro-* side of the drone discourse, as it is the one that is currently succeeding at defining the exception.

The second decision builds on Paul Saurette and Kelly Gordon who warn us that "[t]he first methodological challenge of *any* [emphasis added] discourse analysis project is to identify the raw data (that is, the sample of discourse) to be analyzed" (2013, 160). The sample under analysis here will be fourfold. Given that this research analyzes the US elitist[8] pro-drone discourse, it was evident that speeches delivered by top US officials had to be included. These include speeches from President Obama, Attorney General Holder, Department of State legal adviser Koh and current Director of the Central Intelligence Agency (hereinafter CIA) Brennan.[9] The discourse of these individuals will constitute the first quarter of the data, which will also be the larger part as they represent the *official* elite. The remaining of the sample is comprised of the *unofficial* elite, which is most able to influence the official elite. The second quarter will include US policy institutes. Only the *pro*-drone arguments set forth by think tanks—including Brookings Institution, Heritage Foundation and American Enterprise Institute—will be analyzed.[10] The third quarter will be comprised of manufacturers within the defense industry including iRobot, QinetiQ and Northrop Grumman, three companies engineering unmanned vehicles for military purposes (Singer 2009c, 21-28).[11] The last quarter will

[8] The focus here is on the political elite—articulating the official US discourse—and those who can most influence this elite, voicing the unofficial US discourse. Although the media may have a considerable level of influence over the political elite, it is not included in the unofficial discourse. This is because one aspect of its ideology is considered to be different than that of the elite itself, namely its "normative framework" (Gibbins and Youngman 1996, 6).

[9] The selection of the public speeches comprised in this sample was made on the basis that the US did not discuss its drone program openly in many instances and only started doing so recently. In other words, the speeches analyzed here represent the bulk of the US elitist pro-drone discourse.

[10] These particular think tanks were chosen on the basis that they are among the most influential ones in the US, the Brookings Institution ranking as *the* most eminent (Brookings Institution 2014).

[11] Producing martial robots as early as 1998, iRobot was a pioneer in the field (Singer 2009c, 21). Focusing solely on the military aspect of robots, Foster-Miller (bought by QinetiQ in 2004) has been the main rival of iRobot (ibid., 28). Both companies being still active, they offer an interesting sample representative of the defense

consist of scholars who have written in favor of the use of drone strikes by the US government. Considered jointly, these four parts should build a large enough sample, representative of the US pro-drone discourse and enabling Critical Discourse Analysis (hereinafter CDA) to offer a solid analytical purchase.

The last methodological choice relates to the actual analysis, which will be both qualitative and quantitative. The qualitative portion will allow the singling out of key words such as 'security' and '(counter)terrorism' that are recurrent.[12] It will be possible to use the works of Cohn (1987) and Lakoff (2009) to assess the function of these words. Saurette and Gordon explain that simply identifying arguments or words in a text or speech is not sufficient; it is useful to know how much importance these arguments or words are given (2013, 172). To meet this objective, they add that a complementary quantitative approach, consisting of a word count of key issues, may be employed. This quantitative approach will therefore be used to identify the main discursive elements of the pro-drone discourse.

IV: A Critical Analysis of the US Pro-Drone Discourse

I: Political Elite

In the opening of a speech he gave on national security, Obama (2009) claimed that his "single most important responsibility as President is to keep the American people safe [...] [a]nd this responsibility is only magnified in an era when an extremist ideology threatens our people, and technology gives a handful of terrorists the potential to do us great harm." This statement sets the stage for US exceptionalism, emphasizing the terrorist threat (the exceptional) to which the US is empowered to respond through counterterrorism (the normal). The normalization of this response is more apparent when Obama claims: "we must use all elements of our power to defeat it [the terrorist threat]" (ibid.). In what Cole (2013) considers to be Obama's most explicit and comprehensive enunciation of the US drone policy and counterterrorism strategy, the president declared: "[w]e must define the nature and scope of this struggle [with terrorism], or else it will define us" (Obama 2013).

---

industry in the domain of robotics, for the companies that came after them were merely competitors.

[12] For a complete list of these words, see footnote 10 or Table 1.

This is yet another manifestation of exceptionalism, Obama tacitly arguing that the US must determine the state of exception. Moreover, the fact that Obama uses the word 'must' implies a 'necessity' to react. This 'need' to respond is accompanied with a response that can only be 'normal.' This is because once the US faces a situation containing something exceptional (terrorist threat), the US has no other choice but to retaliate against it. As Obama puts it, "[w]e *have to* [emphasis added] take these threats seriously, and do all that we can to confront them" (ibid.). This sine qua non is also perceptible when Obama adds, "we *must* [emphasis added] finish the work of defeating al Qaeda and its associated forces" (ibid.). The presence of US exceptionalism allows us to turn to the pro-drone discourse, which it fuels.

How do drone strikes come to be included in the US' political discourse? It is through its effort at defeating terrorism. Discussing the counterterrorism strategy that the US ought to adopt, Obama explains that it must be "a series of persistent, targeted efforts to dismantle specific networks of violent extremists that threaten America" (ibid.). He adds that the preference of the US is to apprehend individuals belonging to these networks, but that some conditions eliminate the option of capturing them. Thus, "it is in this context that the United States has taken lethal, targeted action against al Qaeda and its associated forces, including with remotely piloted aircraft commonly referred to as drones" (ibid.). Drone strikes are a surgical alternative to the far less precise war on terror(ism). Obama employs that rationale to support the use of drone strikes, claiming that the US does not *want* to, but rather *has* to employ them to counter the threat posed by terror(ism). The president formulates his pro-drone discourse around the fact that "[the US'] actions are effective [...] strikes have saved lives [...] [s]o doing nothing is not an option" (ibid.) that the US can espouse.

Discussing drone strikes, Attorney General Holder (2012) claims that the US has "the clear authority – and, I would argue, the responsibility – to defend the United States through the appropriate and lawful use of lethal force." Because he uses the word 'responsibility,' Holder brings up the 'necessity' to respond to the terrorist threat—an exception determined by the US. Exceptionalism allows Holder to add: "we should not

deprive ourselves of any tool in our fight against al Qaeda" (ibid.) The state of exception permits the US to respond to terrorism in virtually any way it wants, reactions which will be deemed 'normal.' Moreover, the US frames strikes as a legal course of action if they meet the following three criteria: "[f]irst, the U.S. government has determined [...] that the individual poses an imminent threat of violent attack against the United States; second, capture is not feasible; and third, the operation would be conducted in a manner consistent with applicable law of war principles" (Holder 2012). Exceptionalism lies in the first criterion, which empowers the US to determine who poses a threat. As Walker (2006, 67) explains, it is the 'ability to determine' what *is* exceptional and what *is not* that enables one to initiate exceptionalism.

John Brennan was among the first Obama administration officials to publicly admit to the use of drone strikes by the US in a speech he gave as Assistant to the President for Homeland Security and Counterterrorism. He therefore contributed to the phrasing of the early pro-drone discourse, claiming that "in order to prevent terrorist attacks on the United States and to save American lives, the United States Government conducts targeted strikes against specific al-Qaida terrorists, sometimes using remotely piloted aircraft, often referred to publicly as drones" (Brennan 2012). Like Obama and Holder did to support the pro-drone discourse, Brennan argued that strikes were a response to the terrorist threat on the US and its people, normalizing them as they were conducted "in full accordance with the law" (ibid.), countering an exception(al threat). Brennan adds: "[the US] may also use force consistent with [its] inherent right of national self-defense" (ibid.). Brennan also touches upon James Der Derian's (2009) concept of virtuous war, maintaining that drone strikes allow the elimination of terrorists while pruning civilian casualties (ibid.). Der Derian refers to this moral aspect of virtuous war as "the sanitization of violence" (2009, xxxiii). Not only are drone strikes necessary to protect the US, they also enhance the safety of civilians where strikes are carried out by targeting specific individuals, reducing collateral damage.

At the American Society of International Law's 104th annual meeting, Department of State legal adviser

Harold Koh's (2010) speech gravitated around the argument that the US conducts drone strikes lawfully. Although Koh did not use a different rationale than Holder's or Brennan's to support the legality of strikes, it is worth looking at his discourse since it reinforces his colleagues' rhetoric simply by repeating it because "[saying] things not once, but over and over" (Lakoff 2009, 116) allows to embed them in people's minds. Koh reiterates that the US and the American people are under (an exceptional) threat (terrorism) and the US therefore has the (normal) responsibility to respond to that threat, using strikes as self-defense.

Saurette and Gordon (2013, 172) believe that a qualitative CDA can be complemented with the insertion of a quantitative take on the discourse, namely by using a word count of key issues within the discourse so as to determine which ones are emphasized by the speaker. Logically, an issue central to a discourse will occupy more space; more words will be employed to discuss it (ibid.). Table 1 (see appendix) looks at how many times certain key words—associated with three specific issues, namely *terrorist threat* (Issue 1), *self-defense* (Issue 2) and *drone strikes* (Issue 3)—appear in the four official pro-drone discourses qualitatively analyzed above. [13] Issue 1 is representative of the state of exception determined by the US and Issue 2 is the normal reaction to it. Together, Issues 1 and 2 represent exceptionalism. Thus, Issue 3 is the embodiment of this reaction of self-defense.

In all four speeches, the number of words devoted to Issue 1 is greater than that allocated to Issue 2. Moreover, more words are used to talk about Issue 2 than Issue 3. Also, the words that are used the most often across the four speeches are those associated with 'terror.' The speakers seek to emphasize the presence of terrorism. It is only once they have done so that they can claim to be acting—through the use of drone strikes—in self-defense, which is a normal response given the presence of terrorism. Therefore, it is not all that important to discuss the use of strikes in great length.

[13] Issue 1 is comprised of the following key words: *terror*, *terrorist*, (*counter*)*terrorism*, *threat*, *threatened*, *target*, *targeted* and *targeting*. Issue 2 is composed of the next key words: (*self-*)*defense*, (*self-*)*defend*, *protect*, *protection*, *security*, *secure*, *responsible*, *responsibility*, *save* (*lives*), *saving* (*lives*), *safe*, *safety* and *safeguard*. Issue 3 consists of the subsequent key words: *drone*, *unmanned* or *remotely piloted vehicle* and *strike*.

Why spend time and effort trying to explain something that is normal? This would account for the fact that the words comprising Issue 3 were utilized less often compared to those making up Issues 1 and 2. Even so, terrorism deserves attention, for it is not normal but exceptional. This explains why the number of words used by the four officials to discuss Issue 1 is significantly higher. The most striking about Table 1 is that Holder (2012) gives a discourse in which he defends the legality of US drone strikes, but does not use the word 'drone' once in his thirty-five minute speech. The same observation can be made of Koh's (2010) speech in which he explicitly argues that strikes are conducted legally, yet mentioned the word 'drone' only four times. This is revealing of what the US considers to be important in the pro-drone discourse. Based on these official discourses, drone strikes themselves are not what matters; the presence of terrorism *is*. This is exactly where top US officials draw their audience's attention. So how does the US talk in pro-*drone* politics? It does not; rather, it talks about terrorism and self-defense.

II: Think Tanks

James Jay Carafano (2013) of the Heritage Foundation explains that the US drone policy is part of the state's larger counterterrorism strategy. He says: "[t]hat strategy places a premium on using missile-armed unmanned aerial vehicles to whack the leadership of Al Qaeda and its affiliates" (Carafano 2013). This implies that drone strikes are the actualization of self-defense. They are part of the larger umbrella of counterterrorism—itself a strategy of self-defense against the terrorist threat. Carafano defends the legality of these strikes, arguing that they are done in accordance with Just War Theory. He asserts that "[e]xisting rules of war accommodate new technologies [drones] perfectly well" (ibid.). Steven Groves concurs that strikes are legal, contending that the US is faced by the threat of terrorism and therefore "has an inherent right of self-defense" (2013). Lisa Curtis (2011), another pro-drone advocate, defends the use of strikes on the basis that they are successful, killing top al Qaeda affiliates and protecting the US and its people. The title of her article—"Drone Strikes Protect America from al-Qaeda's Terror" (Curtis 2011)—could hardly be more representative of the self-defense argument. In this case, self-defense goes hand in hand with exceptionalism

because the response is normal. It is a reaction to an exceptional.

American Enterprise Institute's Sadanand Dhume (2011) maintains that drones are the US' most surgical counterterrorism instrument. He goes as far as saying that the US should not only continue to employ them, but use them even more than it already does. Laying out his reasoning plainly, he argues: "drones offer a practical way to eliminate some terrorists and keep others on the run" (Dhume 2011). This pro-drone rhetoric gravitates around the idea that strikes defeat the threat posed by terrorism. John Yoo (2012) praises Holder's (2012) discourse on defending the legality of drone strikes, but tightens his pro-drone (legal) rhetoric by pointing to a flaw in the Attorney General's discourse. According to him, "[Holder] made a fundamental mistake by conceding that terrorists on the battlefield have due process rights at all" (Yoo 2012). Yoo believes that granting terrorists due process rights would only tie the hands of the US, preventing it from making quick and efficient decisions regarding strikes. He claims that foreign and domestic enemies should not be granted the rights laid out in the US Constitution. The fact that he labels terrorists 'enemies' of the US means that the action the latter undertakes by striking the former is merely one of defense. Yoo therefore embraces the self-defense discourse, a discursive mechanism allowing him to argue that all actions are normal against the determined threat or enemy.

Peter W. Singer of the Brookings Institution claims that Obama's (2013) speech on counterterrorism, in which he openly discussed the issue of strikes, gave the president an opportunity "to set the terms of the debate" (2013). Singer believes that the May 23 discourse allowed Obama to determine the place drone strikes should occupy within the US counterterrorism agenda. This means that it is *up to the US* to decide, giving Singer's argument a pro-exceptionalism flavor. As Daniel L. Byman claims, "drone strikes remain a *necessary* [emphasis added] instrument of counterterrorism" (2013). The 'necessity' of using drones implies a responsibility from the US to counter terrorists. It *must* respond. Drones are a 'normal'—and perhaps the most obvious—response for that task, for and as Byman bluntly puts it when its comes to targeting individual terrorists and eliminating the threat they pose

on the US, "they work" which is why "they will likely remain [the Obama] administration's weapon of choice" (ibid.). Byman also champions Der Derian's notion of virtuous war and therefore one of Brennan's arguments, basing his pro-drone position on the fact that drones have fulfilled their task "at no risk to U.S. forces, and with fewer civilian casualties" (ibid.).

III: Defense Industry

The respective statements of the three defense manufacturers are brief, yet germane to the overall pro-drone discourse. iRobot's motto incarnates the concept of virtuous war stating that "[its] combat-proven robots protect those in harm's way and save lives every day. The robots perform multiple missions for troops and public safety professionals, enhancing situational awareness, reducing risk and increasing mission success" (iRobot 2013). Put differently, the company's robots allow the soldiers using them to be safe. Although the above quote does not speak explicitly about drones, it still tells us something about iRobot's pro-drone discourse: drones are used because they get the job done more efficiently than human beings. QinetiQ's pro-drone(/robot) discourse is straightforward; its unmanned vehicles "help [soldiers] stay out of harm's way" (QinetiQ 2013). QinetiQ's robots 'protect' soldiers against 'danger' and enemy threat. They are used for self-defense in a virtuous war fashion, keeping threats and soldiers distanced from one another. Finally, Northrop Grumman's unmanned vehicles "help reduce risk to both national security and human lives" (Northrop Grumman 2013). Not only are they used to protect the US they also make virtuous war possible, allowing US soldiers to counter terrorism from afar. In short, all three manufacturers tacitly champion Der Derian's concept in their pro-drone(/robot) discourse.

IV: Academics

Peter W. Singer (2009a) points out that drones and other types of robots helped saving US soldiers' lives, undertaking the high risk tasks soldiers would otherwise have to do themselves. He gives the example of the PackBot, a robot that disarms roadside bombs representing a lethal threat to US soldiers. However, the PackBot neither strikes nor kills enemies, it simply protects soldiers. Nevertheless, he claims that the new

deadly technology may *actively* eliminate the threat, noting that "robots are killing America's enemies and saving American lives" (Singer 2009b, 30). Singer reiterates that point, arguing that "[i]t's not hard to see the appeal of robots to the Pentagon. Above all, they save lives" (ibid., 36). Laura Sullivan (2012) concurs with the lifesaving aspect of robots, claiming that not only do they protect soldiers themselves, they also "[keep] the people around them safer" (Sullivan 2012, 22). This is violence sanitization rhetoric. Robots therefore become a necessity without which the US cannot 'safely' counter terrorist threats. Sullivan insists, "we absolutely *need* [emphasis added] these kinds of robots" (ibid.). Singer sums up the pro-drone(/robot) argument forthrightly: "[w]ho is going to complain, after all, about trying to find a better way to save soldiers' lives" (2010, 95)? In Singer and Sullivan's discourse, robots and concomitantly drones are therefore understood as a normal response to the danger or threat posed to US soldiers by the (terrorist) enemy that, itself, is an exception.

V: Making Sense of the US Pro-Drone Discourse

Now that a critical analysis of the US pro-drone discourse has been carried out, it is possible to undertake an assessment of this analysis. This effort can be best understood when expressed as an attempt at answering the following question: what do the theories presented in Section II tell us about the manner in which the discourse analyzed above is fashioned? Cohn's (1987) work regarding the complexity of language can help us answer it. Although the US elite does not use a language as sophisticated as technostrategic language,[14] it employs a particular vocabulary that has the effect of a barrier to dissenting voices. When the elite repeatedly emphasizes the presence of a 'threat' under the form of 'terror(ism)' (see Table 1), it becomes difficult to speak of drone strikes as anything other than a (normal) reaction of self-defense. This discursive barrier is rooted in a discourse

[14] The technostrategic language used by the defense intellectuals in Cohn's article is deliberately complex precisely because intricacy makes it very difficult for non-experts to partake it the discussion if they do not master the language used. While not as complex as the technostrategic language that used in the pro-drone discourse still prevents non-professionals from partaking in the debate about the use of drones because it uses specific words to draw attention on certain aspects of the issues being discussed and screen others.

fueled by exceptionalism. Once the US sets the state of exception, which it has itself determined, a particular language accompanies and supports it. Words such as *terror*, *threat*, and (*counter*)*terrorism* lead to words like (*self-*)*defense*, *responsibility*, *protection*, *security* and *saving* (*lives*). Unlike those of technostrategic language, the words above are relatively easy to learn and yet, once assimilated, they too "shapes your categories of thought" (Cohn 1987, 714), making it not necessarily impossible, but surely more difficult to articulate the issue of strikes in other terms.

Lakoff's (2009) explanation of narratives and framing processes has an obvious contribution to the understanding of the pro-drone discourse; the US elite and think tanks blatantly frame their discourse using a self-defense narrative. Exceptionalism is the driving force behind this narrative, and the narrative itself re-intensifies this part of the US' ideology. By dictating what the exception is—in this case, a terrorist threat to the US—the US has to coherently frame its response with that menace, thus framing a self-defense line of reasoning. Given that articulated narratives are permanently installed in brains, once that logic is set into motion, it becomes a reference of choice, making it knotty not to employ when discussing drone strikes (Lakoff 2009, 36). The repetition of that narrative in every speech or article by the US elite and think tanks, respectively, only makes it more likely that it will become the dominant one (ibid., 116). Thus, given the preponderance of that particular narrative, it simply makes sense for the US to keep on defining the exception, for after all, it is merely defending itself.

As Lakoff explains, no individual can be purely conservative nor entirely progressive; a little bit of both views is present in every person's brain and one or the other manifests itself in specific contexts (ibid., 69-70). This is what Lakoff terms biconceptualism. It is the manifestation of a certain view in a given situation and the absence thereof in other circumstances where it is replaced by another stance. Biconceptualism, along with exceptionalism, can help us understand why the Obama administration gives immense importance to saving the lives of Americans while allowing some of them to be droned when they are alleged terrorists. If, as Obama (2009) pointed out, his prime responsibility is to protect the Americans, why did the Obama government

intentionally drone (at least) one American (Ackerman and Shachtman 2013)? Given the pro-drone discourse gravitating around a self-defense narrative itself fueled by exceptionalism, the US, having both the 'protect Americans' and 'kill a few Americans to protect more Americans' views at its disposal, is inclined to choosing the latter given the state of exception. Under normal circumstances, killing an American would be unacceptable.[15] Under a state of exception however, it is simply normal. Both options being available to the Obama administration's 'mind' along with exceptionalism, the most radical alternative—that of killing an American based on a utilitarian calculation that it will save more Americans—can be chosen normally.

Colour line, according to Razack (2004, 7), is the separation of two groups that stems from a racial ideology. She maintains that Canada went into Somalia on the basis of this logic, arguing that peacekeeping violence is *norm*alized through it (ibid., 12). US drone strikes are yet another example of such racial project because what is qualified as exceptional is, before being labeled as such, imperial (Walker 2006, 67). For instance, droning an individual in Yemen or Pakistan is, without the context of the terrorist threat against which one defends itself, an assassination or an act of imperialism. The state of exception changes the same strike into an act of self-defense. Through exceptionalism, the US is able to change an imperial action into a normal one, because it becomes a mere reaction to an exception. But the fact that the US is the one to determine the state of exception implies an inequality between It and an Other, which it strikes. This is where colour line lies, in the separation of two groups—the US and an Other, comprised of terrorists—which is done by the group deeming itself superior to the other. Like Canada was civilizing Somalia, the US is refining the Muslim world while defending itself, taking down terrorists one strike at the time—a normal undertaking underlaid by a racial tone.

Razack's (2008) concept of race thinking best captures the logic behind the US pro-drone discourse. As Razack intelligibly puts it, "[i]n the 'war on terror,' race

[15] Biconceptualism does not necessarily involve two ideologies. Rather, it refers to two or more thought processes that contradict one another, yet exist in parallel in a person's brain.

thinking accustoms us to the idea that the suspension of rights is warranted in the interests of national security" (2008, 9). Race thinking drives Yoo (2012) to claim that enemies ought not be granted any rights. Yoo is forthright: "[e]xtending due process [to enemies/terrorists] would hamstring [the US'] armed forces and intelligence in combat" (ibid.). In advancing this argument, Yoo places the presumed enemies in a lawless space. Droning individuals and taking away their rights is like placing them in a space where the law does not apply, Razack's concentration camp. Thus, both the self-defense line of reasoning, championed by the US elite and think tanks, and the virtuous war argument, implicitly advanced by the defense industry and academics, can be understood through race thinking. First, because the US is in a self-defense mode, droning enemies/terrorists is done so as to protect the US and the American people. Second, Der Derian (2009, xxxi) explains that virtuous war is about killing the enemy in a manner that minimizes risks to soldiers and reduces collateral damage, yet the state engaging in such a war still kills the enemy to *protect itself*. Thus, in an attempt to assure its security it willingly places the individuals it chooses to drone in a space where law is nonexistent.

VI: Concluding Reflection

What conclusions can be drawn from the assessment of the US pro-drone discourse? First, this paper concurs with Saurette and Gordon (2013, 179) on the argument that CDA cannot tell us about the motives behind a given discourse. The approach employed here was unable to provide any information regarding the reason(s) Obama or iRobot, for instance, are pro-drone proponents. An attempt at determining such motivations is at best an informed guess and at worst conducive to erroneous results. Second, there is a noticeable difference between the way the official elite articulates its discourse compared to the unofficial elites. While the official elite eschewed mentioning words such as *drone* and *unmanned vehicle*, instead directing its audience's attention on words like *threat*, (*counter*)*terrorism* and *security*, the unofficial elite employed them overtly. Future work could try to understand why this is the case. Third, combining this paper's hypothesis with the four theoretical approaches, enabled CDA to get a comprehensive grip on the elitist pro-drone political

discourse. In short, the analysis conducted above allowed to answer the *how* of the pro-drone discourse, but not the *why*. That is, while CDA enables us to expose the way in which a discourse is enunciated, it cannot tell us the reason(s) behind that particular articulation.

To conclude, this paper critically analyzed the US, elitist pro-drone discourse. It sought to comprehend the types of discursive mechanisms employed by the speakers of that discourse, namely the political elite, think tanks, defense contractors and academics. That these individuals and organizations *do* support drone strikes was taken as a given. This paper strove to explain *how* they vocalize that position (Saurette and Gordon 2013, 157), asking *how* the US talks in its pro-drone discourse. It argued that exceptionalism is the part of US' ideology constituting that discourse. Exceptionalism's effect on the discourse is circular: because there is an 'exceptional,' there is its accompanying 'normal' and because that 'normal' is normal, talking about it is trivial so the emphasis goes back on the 'exceptional'—conspicuously underlined by the US, which directs the attention on a (terrorist) threat.

Works Cited

Ackerman, S., and Shachtman, N. 2013. *Holder: We've Droned 4 Americans, 3 By Accident. Oops*. Brookings Institution. Available from: http://www.brookings.edu/research/opinions/2013/05/22-drones-targeted-killings-shachtman [Accessed November 20, 2013].

Brennan, J. 2012. *The Efficacy and Ethics of U.S. Counterterrorism Strategy*. White House. Available from: http://www.wilsoncenter.org/event/the-efficacy-and-ethics-us-counterterrorism-strategy [Accessed November 20, 2013].

Brookings Institution. 2014. *Brookings's Reputation*. Available from: http://www.brookings.edu/about/reputation [Accessed July 28, 2014].

Byman, D. L. 2013. *Why Drones Work: The Case for Washington's Weapon of Choice*. Brookings Institution. Available from: http://www.brookings.edu/research/articles/2013/06/17-drones-obama-weapon-choice-us-counterterrorism-byman [Accessed November 20, 2013].

Carafano, J. J. 2013. *Drone Strikes and Just War*. The Heritage Foundation. Available from: http://www.heritage.org/research/commentary/2013/2/drone-strikes-and-just-war [Accessed November 20, 2013].

Cohn, C. 1987. "Sex and Death in the Rational World of Defense Intellectuals." *Signs* 12(4): 687-718.

Cole, D. D. 2013. "Drone Strikes: Are They President Obama's Guantanamo?" Speech, Ottawa, ON, November 14.

Curtis, L. 2011. *Drone Strikes Protect America from al-Qaeda's Terror*. The Heritage Foundation. Available from:

http://blog.heritage.org/2011/08/29/drone-strikes-protect-america-from-al-qaedas-terror/?ac=1 [Accessed November 21, 2013].

Der Derian, J. 2009. *Virtuous War: Mapping the Military-Industrial-Media-Entertainment-Network*. New York, NY: Routledge.

Dahl, R. A. 1971. *Polyarchy: Participation and Opposition*. New Haven, CT: Yale University Press.

Dhume, S, 2011. *The Morality of Drone Warfare*. American Enterprise Institute. Available from: http://www.aei.org/article/foreign-and-defense-policy/regional/middle-east-and-north-africa/the-morality-of-drone-warfare/ [Accessed November 20, 2013].

Eagleton, T. 2007. *Ideology: An Introduction*. New York, NY: Verso.

Gibbins, R. and Youngman, L. 1996. *Mindscapes: Political Ideologies Towards the 21st Century*. Toronto, ON: McGraw-Hill Ryerson.

Groves, S. 2013. *Drone Strikes: The Legality of U.S. Targeting Terrorists Abroad*. The Heritage Foundation. Available from: http://www.heritage.org/research/reports/2013/04/drone-strikes-the-legality-of-us-targeting-terrorists-abroad [Accessed November 20, 2013].

Holder, E. 2012. *Attorney General Eric Holder Speaks at Northwestern University School of Law*. YouTube. Available from: http://www.youtube.com/watch?v=aZX8rtuqMiw [Accessed November 20, 2013].

iRobot. 2013. *Defense & Security*. Available from: http://www.irobot.com/us/learn/defense.aspx [Accessed November 22, 2013].

Koh, H. 2010. *Defense Measures: Harold Koh Explains Foreign US Combat*. YouTube. Available from:

http://www.youtube.com/watch?v=Y9qPYjK_n00 [Accessed November 20, 2013].

Lakoff, G. 2009. *The Political Mind: A Cognitive Scientist's Guide to Your Brain and Its Politics*. New York. NY: Penguin Books.

Northrop Grumman. 2013. *Unmanned Systems*. Available from: http://www.northropgrumman.com/Capabilities/Unmannedsystems/Pages/default.aspx [Accessed December 7, 2013].

Obama, B. 2009. *President Obama: Our Security, Our Values*. White House. Available from: http://www.whitehouse.gov/video/President-Obama-Our-Security-Our-Values#transcript [Accessed November 20, 2013].

Obama, B. 2013. *President Obama Speaks on the U.S. Counterterrorism Strategy*. White House. Available from: http://www.whitehouse.gov/photos-and-video/video/2013/05/23/president-obama-speaks-us-counterterrorism-strategy#transcript [Accessed November 20, 2013].

QinetiQ. 2013. *Unmanned Systems*. Available from: https://www.qinetiq-na.com/products/unmanned-systems/ [Accessed December 8, 2013].

Razack, S. H. 2004. *Dark Threats and White Knights: The Somalia Affair, Peacekeeping, and the New Imperialism*. Toronto, ON: University of Toronto Press.

Razack, S. H. 2008. *Casting Out: The Eviction of Muslims from Western Law and Politics*. Toronto, ON: University of Toronto Press.

Saurette, P. and Gordon, K. 2013. "Arguing Abortion: The New Anti-Abortion Discourse in Canada." *Canadian Journal of Political Science* 46(1): 157-185.

Singer, P. W. 2009a. *Military Robots and the Future of War*. TED Talks. Available from: http://www.ted.com/talks/pw_singer_on_robots_of_war.html [Accessed November 20, 2013].

Singer, P. W. 2009b. Robots at War: The New Battlefield. *Wilson Quarterly* 33(1), 30-48.

Singer, P. W. 2009c. *Wired for War: The Robotics Revolution and Conflict in the Twenty-first Century*. New York, NY: The Penguin Press.

Singer, P. W. 2010. "Meet the Sims: ... and Shoot Them. The Rise of Militainment." *Foreign Policy* 178: 91-95.

Singer, P. W. 2013. *Finally, Obama Breaks His Silence on Drones*. Brookings Institution. Available from; http://www.brookings.edu/research/opinions/2013/05/23-drones-obama-singer [Accessed December 7, 2013].

Sullivan, L. 2012. "Robots to the Rescue." *Risk Management* 59(1): 20-24.

Tully, J. 1988. *Meaning and Context: Quentin Skinner and his Critics*. Princeton, NJ: Princeton University Press.

United States Department of Justice. 2013. *Attorney General Eric Holder Speaks at Northwestern University School of Law*. Available from: http://www.justice.gov/iso/opa/ag/speeches/2012/ag-speech-1203051.html [Accessed November 8, 2013].

Waever, O. 1995. "Securitization and Desecuritization." In: R. D. Lipschutz, ed. *On Security*. New York, NY: Columbia University Press, 46-86.

Walker, R. B. J. 2006. "Lines of Insecurity: International, Imperial, Exceptional." *Security Dialogue* 37(1): 65-82.

Wodak, R. and Krzyżanowski, M. 2008. *Qualitative Discourse Analysis in the Social Sciences*. New York, NY: Palgrave Macmillan.

Yoo, J. 2012. *The Good and Bad in Eric Holder's Drone Defense*. American Enterprise Institute. Available from: http://www.aei.org/article/politics-and-public-opinion/the-good-and-bad-in-eric-holders-drone-defense/ [Accessed November 20, 2013].

Appendix: Table 1 - Key Issues by Official Speech

Speeches → **Key Issues / Words** ↓	**The Efficacy and Ethics of U.S. Counterterrorism Strategy (Brennan 2012).**	**Attorney General Eric Holder Speaks at Northwestern University School of Law (Holder 2012).**	**Defense Measures: Harold Koh Explains Foreign US Combat (Koh 2010b).**	**President Obama Speaks on the U.S. Counterterrorism Strategy (Obama 2013).**	**Total**
Terror / Terrorist / (Counter) Terrorism	52	32	1	50	**135**
Threat / Threatened	15	16	2	23	**56**
Target / Targeted / Targeting	43 Total Issue 1: **110**	11 Total Issue 1: **59**	17 Total Issue 1: **20**	19 Total Issue 1: **92**	**90** Total Issue 1: **281**
(Self) Defense / (Self) Defend / Protect / Protection	10	19	5	13	**47**
Security / Secure	17	23	0	20	**60**
Responsible / Responsibility	10	4	1	3	**18**
Save (Lives) / Saving (Lives) / Safe / Safety / Safeguard	13 Total Issue 2: **50**	8 Total Issue 2: **54**	0 Total Issue 2: **6**	6 Total Issue 2: **42**	**27** Total Issue 2: **152**
Drone / Unmanned *or* Remotely Piloted Vehicle	11	0	4	14	**29**
Strike	30 Total Issue 3: **41**	1 Total Issue 3: **1**	0 Total Issue 3: **4**	26 Total Issue 3: **40**	**57** Total Issue 3: **86**

International Law and Cyber Warfare: The Case of Stuxnet

Chris Masciotra, University of Windsor

Introduction

Cyber warfare is an emerging field of study that weighs the effects of cyber attacks against the principles and customs of international law. Many questions have developed regarding whether the traditional practices of international law are capable of regulating unprecedented cyber attacks. The purpose of this paper is to explore the characteristics that define the cyber world and analyze how the varying interpretations of international law are applicable to the growing use of cyber weapons. The unique cyber weapon known as Stuxnet will be studied to ascertain whether existing international law could have been applied to this attack against the Iranian nuclear program in 2009. This paper argues that international law deriving from both the United Nations and Law of Armed Conflict could not have regulated the Stuxnet cyber attack and is incapable of governing the use of similar cyber weapons.

This essay is divided into two parts. Part I reviews the literature surrounding cyber activity as well as the wide range of views linking international laws and customs to cyber attack. Part I begins by identifying the primary laws and institutions relevant to cyber attack. This section will explore the UN Charter including Articles 2(4), 39, 41, 42, and 51[16] as well as the *jus ad bellum* and *jus in bello*[17] principles comprising the Laws of War and the Law of Armed Conflict. Part II of this essay examines the Stuxnet cyber weapon and offers an analysis of how and whether the international laws and institutions defined in Part I apply to the cyber attack. Part II begins with a review of Stuxnet, followed by a five-conclusion analysis. First, Article 2(4) of the UN

[16] Article 2(4) refers to the United Nations prohibition of the use of force; Articles 39, 41 & 42 stipulate when the UN Security Council may intervene during international conflict; Article 51 identifies when a state may engage in self defence.

[17] *Jus in bellum* is a convention outlining when states are permitted to engage in war; *Jus in bello* is law regulating how states may behave during conflict. For more information, see Hehir (1992) and Holliday (2003).

Charter did apply to the 2009 Stuxnet attack revealing that Stuxnet did constitute a use of force. Second, Articles 39, 41 and 42 were not capable of responding to the virus owing to UN Security Council weaknesses. Third, the Stuxnet attack[18] was consistent with the self defence terms outlined in Article 51 and complied with the notion of anticipatory self defence. Fourth, the *jus ad bellum* paradigm could have justified the use of Stuxnet engaging in international conflict. Lastly, the Law of Armed Conflict and the *jus in bello* principle would have fallen short of regulating the cyber attack because of a lack of identity. Overall, the results suggest that even if the Stuxnet attack did constitute a violation of international principles, current international law could not have regulated the cyber weapon. As a result, this analysis suggests that future aggressors in the cyber realm will likely evade the consequences of their actions, an important development at a time when more activities are conducted in cyber space.

Part I

International Law & Cyber Language

The applicability of international law to cyber attack depends largely on the wording and language that together define the cyber domain. Scholars have long debated the precise meaning and interpretation of specific elements comprising a wide array of cyber definitions leading to disagreement on which characteristics comprise cyber activity (Andress and Winterfeld 2000; Vatis 2006; Rosenfield 2009; Kechichian 2002; Harley 2010). Broad and narrow understandings of concepts such as cyber weapons and cyber attack divide experts and the international community serving as an inherent challenge over how to approach international regulation of the cyber world. Identified below are two terms, cyber weapons and cyber attacks, that illustrate the difficulty in defining cyber activity.

Cyber Weapons

[18] This attack is widely believed to have been carried out by Israel and the United States. For more information, read David Sanger's comment in the *New York Times* (2012).

As states become increasingly comfortable and familiar with cyber space, so do their ambitions to develop cyber weapons. States are learning that cyber weapons are inexpensive, accurate, and can be deployed from various locations around the world often with impunity and without consequences (Rustici 2011). The growing interest in cyber technology has called for increased efforts at defining what elements form a cyber weapon. Many scholars claim that only certain features comprise a weapon while others argue that different characteristics must be included. One definition classifies a cyber weapon as an instrument that is capable of causing physical harm, death, or damage to property (Bayles 2001). Cyber instruments that do not produce these specific effects may still be dangerous in different applications but cannot be classified as a weapon (Randall 2010).

A second interpretation of cyber weapons is broader. Many argue that while conventional arms such as guns, tanks, and artillery seem to fulfill the physical dimension of a weapon, cyber weapons are inherently different. Cyber weapons are weapons that do not cause mass destruction and/or bodily harm. For instance, a cyber weapon may disrupt and impede foreign computer networks without causing physical damage to institutions (Kelsey 2008). Under this view, a cyber weapon need only interfere with computer networks to qualify as a weapon. Any additional physical destruction caused by a cyber weapon only serves to reinforce this notion.

Still other experts contend that the world has yet to experience a true cyber weapon. Scholars in this camp assert that cyber tools, regardless of their intentions and capabilities, have not performed the horrendous effects achieved by their conventional weapon counterparts (Rid 2012a). Even cyber devices that occasionally interfere with computer networks only amount to cyber crime. As a result, the term “cyber weapon” cannot describe any existing cyber devices.

This paper will employ a narrow definition of cyber weapons because of the reality that certain cyber devices carry the potential to inflict harm and danger onto others. Cyber instruments that are capable of targeting water purification facilities leading to severe

health consequences; misrouting trains causing collision; disrupting air traffic control units; triggering unintentional opening of water dams; or sparking a nuclear meltdown in a power plant are all examples of how a cyber instrument may be used as a weapon (Ophardt 2010). These effects are comparable to the results of conventional weapons and illustrate why a narrow understanding of cyber weapons is necessary.

Experts have been careful in distinguishing between varying offensive capabilities held by certain types of cyber weapons. Cyber weapons are often categorized into two groups: syntactic and semantic. Cyber weapons with syntactic capabilities are able to disrupt an electronic operating system, triggering a failure in computer functions (Hathaway *et al.* 2012). A syntactic weapon causes cyber networks to malfunction through one or a combination of different methods. Malicious code, viruses, worms, Trojan Horses, Distributed Denial of Service (DDoS) attacks, spyware, or botnets all contain syntactic characteristics that infect computer networks. A DDoS attack, for instance, intrudes into a foreign electronic network by overloading specific websites and servers by continuously flooding them with traffic (Platt 2012). DDoS weapons are effective in taking down vital communication networks and critical infrastructure (Waxman 2011). Coupled with DDoS attacks are "botnet" weapons. Botnets target computers and cease operative control, leaving the original computer programmer incapable of managing the cyber network. Botnet attacks are powerful, relatively inexpensive, and may be deployed from numerous locations around the world (Ophardt 2010). Academics have noted that a medium-sized botnet holds the potential to interrupt the entire cellular communications network in the United States (Kelly and Almann 2009). It is a cyber weapon of growing concern and illustrates the destructive potential of syntactic weapons.

Alternatively, cyber aggressors may also employ the services of semantic weapons. Semantic weapons differ from syntactic methods in that the former covertly infiltrate computer networks, leaving the operating system functioning normally, but tampering with the

accuracy of information presented to its operator. This type of weapon is used to mislead computer workers into believing their networks are functioning correctly despite suffering from secret manipulation by the attacker (Hathaway *et al.* 2012). The most familiar types of semantic attacks are performed by malicious software (malware) that often go unnoticed in computer networks for extended periods of time.[19] Creators of cyber weapons may also combine semantic and syntactic designs to incorporate the offensive capabilities from both styles of weapons (Swanson 2010). This process unites the potential disruption rooted, for example, in DDoS attacks with the stealthy nature of semantic malware to produce large-scale disruption. Cyber weapons taking on this form are growing increasingly difficult to detect or defend against.

Compounding the element of stealth in semantic attacks is the potential off-line capability found in this type of cyber weapon. While syntactic devices are highly dependent on the Internet to infect globally connected computer networks, malware may be launched against isolated cyber systems through USB drives or other direct forms of contact (Clarke and Knake 2011). Off-line computer systems, also referred to as air-locked networks, are generally more secure than online systems because of the greater possibility of detecting intrusions. However, computer infrastructures that abstain from Internet connectivity are still vulnerable to attack. Recent developments of cyber weapons equipped with off-line capabilities have questioned the security of air-locked computer systems and reveal the vulnerability of isolated networks.[20]

Cyber Attacks

The use of cyber weapons shapes the contentious concept of cyber attack. Presently, there is no universally accepted definition of what constitutes a cyber attack. Scholars are divided over the specific intent, action, and outcome of cyber weapons necessary to define what

[19] Stuxnet is an example a cyber weapon that achieved this effect.
[20] Stuxnet is an example of a cyber weapon with off-line capabilities (defined in Part II).

behaviour qualifies as an attack.[21] Discussions regarding the characterization of cyber attacks generally fall into three schools of thought. Each school contains a similar approach towards classifying cyber attacks though each focus on separate outcomes.

The first rests on the idea that a cyber weapon need only undermine the operations of a computer network for political or national security reasons in order to qualify as a cyber attack (Hathaway *et al.* 2012). This school allows for the broadest interpretation of what features comprise a cyber attack as it relies on the vague term "undermine" to distinguish between cyber behaviour that is offensive and non-offensive. Supporters of this view stress that attacks must encompass a political purpose as well. Therefore, the release of a cyber weapon must have political motivations or attempt to spark political reaction in order to be deemed a cyber attack.

The second school posits that the use of cyber weapons may be labeled as a cyber attack so long as the latter produces violence, physical destruction, or death (Dunlap 2011; Schmitt *et al.* 2013). Proponents of this camp emphasize the importance of studying the results of a cyber offence as a method of classifying cyber attacks (Swanson 2010). Cyber weapons that do not yield harmful or destructive consequences cannot produce a cyber attack. Likewise, a cyber weapon that holds the potential to cause violence, death, or destruction but does not carry out this potential also cannot be a cyber attack. Any employment of a cyber weapon that falls short of producing the above results may not necessarily be considered an attack. Without these results, the use of a cyber weapon may only amount to a cyber crime.

Finally, the third school of thought suggests that a cyber attack need not commit the violent destruction sought in the second school, but only require a cyber weapon to target and interfere with the information

[21] It is important to distinguish between a cyber weapon and a cyber attack. Cyber weapons are the means by which states may perform a cyber attack. State possession of a cyber weapon does not necessarily translate into a cyber attack. Rather, the use of a cyber weapon must fulfill one or more of the criteria defined below.

stored in computer networks in order to be recognized as a cyber attack. Supporters of this approach refer to this action as a computer network attack (CNA) where cyber weapons aim to disrupt, deny, or degrade foreign computer networks (Rustici 2011; Waxman 2011). Any attempt to tamper with the information held in computer systems qualifies as a cyber attack. Whether this action triggers violent or destructive consequences is irrelevant under this approach unless accompanied by a manipulation of computer information. Often backers of this school assert that the non-violent effects of cyber attacks may surpass the harms of violent ones (Waxman 2011). This notion challenges the physical element present in the second school of thought and further contributes to the ongoing debate over what behaviour constitutes a cyber attack. Several non-governmental organizations subscribe to the third approach and argue that attacks in the cyber domain need only target information systems to be offensive. One scholar cites the position of the U.S. National Academy of Sciences, which defines a cyber attack as an intended action to rework, disturb, mislead, or corrupt computer networks (Malaware 2010).

The distinction between cyber attacks and cyber espionage is a highly important factor when determining if a weapon performs a cyber attack. Although scholars disagree over which uses of a cyber weapon constitute an attack, experts tend to concur that the practice of cyber espionage is different. A cyber instrument probing cyber space for the purpose of obtaining classified information is an example of cyber espionage (Platt 2012; Ophardt 2010). The use of a cyber instrument to perform reconnaissance, information gathering, or investigation does not qualify as a cyber attack (Farwell and Rohozinski 2012). These types of cyber devices are built solely for spying or conducting surveillance operations and do not alter the function of a computer network (Hathaway *et al.* 2012). Although rarely admitted, it is often assumed that countries partake in cyber espionage missions frequently because they recognize that this type of behaviour is not bound by international law (Gervais 2012). Espionage is readily practiced outside the cyber realm where participants are

not subject to restrictions or punishment under international law (Brown and Poellet 2012).

This essay will draw on key aspects of all three schools when referring to a cyber attack. The undermining characteristic in school one, combined with the kinetic violence and destruction from the second view as well as the information manipulation ingrained in the third approach will represent a cyber attack. This definition satisfies a diverse range of scholarly opinion on the issue and will assist in determining the relationship between international law and the use of the Stuxnet virus.

International Law

Prior to the development of cyber space, international law had long endured questions regarding its effectiveness in regulating interstate relations. Although many maintain that much progress has been made within global governance, the relationship of international law with long-standing state principles such as sovereignty has proven to be a challenge. The pressure of cyber warfare further exacerbates these challenges leading to conflicting views on how to approach cyber regulation or whether this task is even feasible (Randall 2010). Outlined below are the primary queries relating to various aspects of international law that scholars debate. They include the role of the United Nations and its Charter, specifically Articles 2(4), 39, 41, 42, and 51; *Jus ad Bellum* laws dictating when states may engage in conflict; and *Jus in Bello* principles that govern how states act during conflict.

UN Charter: Article 2(4)

Since the emergence of cyber space, many have claimed that the UN Charter holds the authority to regulate this new domain while others contend that it does not. As a reference point, scholars frequently cite UN Charter Article 2(4) to determine if the use of a cyber weapon violates international law. Article 2(4) states, “All Members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the Purposes of

the United Nations" (United Nations Charter, Article 2). The controversial expression in this article is the "threat or use of force." Because the interpretation of this phrase is difficult to define, applying this principle to cyber attacks becomes more complex. Statesmen persistently refer to relevant international case studies and precedents for guidance on how to employ Article 2(4) when assessing cyber and non-cyber international law violations (Gjelton 2010).

Scholars divided over the relationship between Article 2(4) and cyber attacks fall into two separate categories: those defending the inherent applicability of 2(4) and those who are skeptical of the power resting with 2(4). Supporters of Article 2(4) argue that, regardless of how the outcome is measured, cyber attacks producing physical and aggressive results are in clear violation of Article 2(4) because they breach the peaceful purposes the UN stands for and are harmful to individuals (Graham 2010). This notion applies to all types of weapons, cyber or otherwise, that threaten the integrity of a country (Farwell and Rohozinski 2012; Schmitt *et al.* 2013). This basic understanding of the Charter is complemented by the rulings of the International Court of Justice (ICJ). The ICJ has stated that Article 2(4) is applicable to all uses of force and pertains to all weapons that may achieve this effect (Schmitt *et al.* 2013). Proponents of this view believe that new technology, including cyber weapons, are not exempt from the law simply because they operate differently than traditional ones. Any weapon causing injury or damage to others is capable of exerting force (Bayles 2001).

Conversely, other scholars contend that the meaning and wording of Article 2(4) is unclear and unable to fully govern the transactions in cyber space. Those following this approach maintain that there is no universally accepted definition of a use of force and that its interpretation depends largely on the reader's subjectivity (Foltz 2012). Some states have informally agreed that certain actions comprise a cyber use of force although this belief is not law. The language "use of force" is unequivocally broad and undermines the usefulness of the phrase when examining different types

of force (Hoisington 2009). Leaving Article 2(4) intentionally or unintentionally ambiguous does not serve to strengthen its purpose. Interpreting the use of force too broadly only to include cyber weapons may also expand the Article's jurisdiction to other traditionally non-forceful actions (Gervais 2012). For instance, political or economic coercive behaviour is conventionally unbound by 2(4) (Optard 2010) though may be suddenly exposed to it if the law is broadened to include cyber weapons (Schmitt *et al.* 2013).

Finally, the most frequently employed argument criticizing Article 2(4) asserts that cyber weapons only restrict the behaviour of states (Hoisington 2009). Governments negotiate international law for the purpose for all to obey. Article 2(4) reaffirms this notion by stating at the outset "All members of the Organization…" referring to all state parties to the UN Charter. Skeptics of Article 2(4)'s relationship to cyber weapons hold that individuals or non-state actors performing cyber attacks are not restricted under the law thus rendering Article 2(4) incapable of regulating cyber attacks.

There are three different methods used by the international community to assist in clarifying the term "force." The first approach requires a strict understanding of international law and the founding logic of the UN Charter (Waxman 2011). Scholars subscribing to this approach believe that only military attacks on a given target represent a use of force prohibited by Article 2(4). For example, a drone strike against foreign banking infrastructure is considered a use of force while the exercise of other means such as economic sanctions or cyber attacks to accomplish the same task are not bound by the same rule. Generally, those who hold this view are in the minority; however these scholars maintain that Article 2(4) was negotiated in the period immediately following World War II and was intended to apply to traditional military weaponry utilized during this time (Waxman 2011). Observers in this camp proclaim it is difficult to simply apply a set of laws that were an explicit response to the use of conventional arms during the 1930s and 1940s to an

entirely different domain that was inconceivable during its creation.

A second theory attempting to explain the meaning of Article 2(4) examines the instrument or tool used to exert force. This view asserts that any instrument performing coercion is in violation of the UN Charter (Waxman 2011). This interpretation of the Charter highlights the founding principle of Article 2(4) at the time of its creation and dismisses any literal understanding of the "use of force" (Waxman 2011). It acknowledges that the means of using force are capable of changing and does not discriminate between the types of tools that may violate the Article. Though some scholars evaluate the brand of instrument used when determining whether a weapon exhibits a use of force, much of the instrument-based approach is employed to establish which weapons qualify as an "armed attack" under Article 51.[22]

Deciphering which characteristics constitute a use of force has led numerous scholars to offer their own assessment techniques. Michael Schmitt's seven-factor analysis is an example of one method that is widely cited by scholars to study Article 2(4) (Hathaway *et al.* 2012; Foltz 2012; Waxman 2011; Schmitt 2010). Schmitt proposes seven criteria that are critical to evaluating if a state has employed the use of force in its international relations. The severity, immediacy, directness, invasiveness, measurability, presumptive legitimacy, and responsibility of an attack all must be considered when establishing the basis for the use of force (Schmitt *et al.* 2013). The first factor, severity, is the most important assessment criterion. It examines the type and scale of harm inflicted by a weapon. Immediacy analyzes how swiftly the attack takes place; directness reviews the length of time between the initial attack and resulting harm; invasiveness assesses the degree of penetration in a state's territory; measurability gauges the level of damage; presumptive legitimacy studies international approval of the attack; and responsibility investigates the conductor of the offence. This type of analysis is flexible and may be applied on a case-by-case basis whereas

[22] Article 51 and the concept of self defence is discussed in detail below.

precedent-employed evaluations are confined to the uniqueness of each case (Foltz 2012).

UN Charter: Article 39, 41, & 42

The role of the United Nations Security Council (UNSC) in responding to violations of the UN Charter is governed under Articles 39, 41, and 42. Article 39 describes the various scenarios in which the UNSC may act or respond. Article 41 provides guidance on how the UNSC may react to any violation of the parameters set in Article 39 with diplomatic resolutions. Finally, Article 42 articulates that in the absence or failure of the diplomatic efforts imposed by Article 41, the UNSC may authorize the use of armed forces to resolve conflict.

Similar to the debate surrounding "use of force," understanding the roles of Article 39, 41, and 42 in relation to cyber warfare is a difficult task. A popular argument criticizing the ability of the UNSC to carry out its duties outlined in Article 39 revolves around the phrase "threat to the peace, breach of the peace, or act of aggression." Many claim that a threat or breach of the peace is akin to the term "use of force." That is, the phrase is exceedingly subjective and difficult to measure against cyber attacks (Schmitt 2010). Attacks that produce harmful consequences may certainly qualify as a breach of peace, but do cyber attacks falling short of fulfilling this arbitrary requirement fall under the jurisdiction of the UNSC? Not all uses of cyber weapons are breaches of peace and thus cannot trigger a response from the Security Council, particularly if a cyber attack's primary goal is to enforce international peace and security.

Moreover, any and all attempts to enact UNSC resolutions under Article 39 are susceptible to the veto power embedded in each of the five permanent members of the Security Council. Because the veto frequently triggers gridlock in the UNSC, attempts to garner a consensus during conflict (cyber or otherwise) are difficult owing to the lack of clarity in Articles 39, 41, and 42 (Graham 2010). Analysts of the role of the Security Council suggest that assessing the validity of a threat or breach of international peace boils down to how the UNSC decides to label any particular event (Schmitt

2010). This behaviour is vulnerable to political decision-making where veto-wielding states may disagree with certain characteristics defining a cyber threat or breach of peace in order to uphold strategic international alliances or economic benefits.

UN Charter: Article 51

A third section of the UN Charter that draws attention to the application of international law to the use of cyber weapons is Article 51, commonly referred to as the notion of self defence. This Article states, "Nothing in the present [UN] Charter shall impair the inherent right of individual or collective self-defence if an armed attack occurs against a Member of the United Nations" (United Nations Charter, Article 51). Cyber experts present opposing arguments that either defend or condemn the right to cyber self defence permitting a state to defend itself. Much of the criticism surrounding the ability of Article 51 in rationalizing self defence rests with the interpretation behind the fundamental term "armed attack." Many suggest that specific characteristics represent an armed attack while others are unsure of which type of attack qualifies.

Deciding how to interpret Article 51 has resulted in the development of different approaches that assist in determining which actions constitute an armed attack (Gervais 2012; Hathaway *et al.* 2012; Waxman 2011). It is important to note that events leading to an armed attack are much more limited than those actions that constitute a use of force (Hathaway *et al.* 2012; Waxman 2011; Dunlap 2011). In other words, state actions that may trigger UN intervention under Article 2(4) may not necessarily qualify as an armed attack as mentioned in Article 51.

The first technique views the attack through the lens of outcome. This effects-based approach assesses the overall damage inflicted by a weapon and evaluates, based on total net damage, whether or not the action qualifies as an armed attack (Graham 2010). The effects-based approach proclaims that if a cyber attack yields the same results as a conventional armed attack, the use of the cyber weapon is considered an armed attack (Hoisington 2009). For example, if a cyber attack is

capable of manipulating machinery causing a fire, and conventional artillery could produce the same effect, then the use of the cyber weapon is an armed attack. The Schmitt analysis most closely resembles the effects-based approach by evaluating the seven characteristics necessary to identify an armed attack (Hathaway *et al.* 2012). Because Schmitt's seven criteria are all used to measure the effects of a weapon, the analysis coincides with the effects-based interpretation of a cyber armed attack.

The second technique is referred to as the "instrument-based" approach. This method studies the explicit device or tool utilized in a cyber attack to learn if an armed attack has occurred. Some scholars argue that the instrument-based model was the approach adopted by the creators of the United Nations when establishing Article 51 (Schmitt 2010; Foltz 2012). The UN founders intended for future generations to perform assessments of the types of weapons used to carry out an attack and believed that this assessment would determine whether an attack qualified as being "armed." According to this approach, a cyber attack must assume the physical characteristics associated with traditional weaponry in order to satisfy the armed attack condition (Hathaway *et al.* 2012).

The third model is known as the target-based approach. As its name suggests, the target-based approach classifies armed attacks based on the objective that the cyber weapon strikes (Hathaway *et al.* 2012). According to this view, targets are a more accurate measurement of an armed attack than outcomes or instruments because targets are easily defined and identified (Hathaway *et al.* 2012). Identifying lawful targets on traditional battlefields and in the cyber domain are recognizable to the extent that they are better indicators of when a weapon has risen to the status of an armed attack. If a cyber attack occurred against a country's critical infrastructure, the victim state retains the right to respond under Article 51 (Jensen 2010).

An additional perspective concerning the legality of Article 51 involves victim state recognition of the attack. A state must publicly announce if it has endured an armed attack in order to invoke the right to respond in

self defence (Brown and Poellet 2012). Some believe that without this acknowledgement, a state cannot expect the international community to intervene or respond to an attack (Foltz 2012). The same theory holds true in the cyber domain where victims of a cyber attack that fail to denounce the strike are unprotected by international law. Despite this claim, the vast majority of cases involving self defence are recognized by the injured state thus invoking international law and the right to self defence.

The final issue related to Article 51's self defence principle revolves around the concept of anticipatory self defence. Anticipatory self defence (or preemptive self defence) is the practice of states employing force, in some circumstances in the form of an offensive attack, prior to suffering from an imminent armed attack (Waxman 2011). Advocates of anticipatory self defence are convinced that states need not wait until they experience an attack before resorting to retaliatory measures. Instead, countries may preemptively strike and deter foreign states from executing their assaults. Some interpret Article 51 as exclusive law that may only be enacted after experiencing an armed attack while others contend states are permitted to prepare beforehand (Hoisington 2009). Those defending the use of cyber anticipatory self defence argue that because of the instantaneousness of cyber attacks, states no longer possess sufficient time to defend themselves after experiencing the effects of a cyber weapon (Jensen 2010). Critical infrastructures that are dependent on computer systems may not respond or be capable of engaging in defensive measures after a cyber attack has been absorbed. As a result, states may engage in anticipatory cyber offensives that preserve national computer networks and retain the ability to strike first.

Skeptics of the anticipatory self defence theory still recognize a state's right to defend itself in advance of a forthcoming attack; however, they stress the need to confirm that an impending attack is indeed imminent and real (Dunlap 2011). In order to participate in anticipatory self defence, states must hold evidence proving that they will inevitably suffer an approaching cyber or non-cyber attack before conducting preventative operations. Without this evidence, anticipatory self defence is

contrary to Article 51 and international law (as was seen by the U.S. attack against Iraq in 2003). It is widely accepted that the U.S. did not possess sufficient evidence linking terrorist attacks to Iraq and that fear alone did not justify the use of preemptive force (Crawford 2003). To be justified in engaging in preemptive self defence, countries must be publically threatened by potential aggressors and establish that adversaries are mobilizing their forces into attacking positions (Crawford 2003).

Laws of War: Jus ad Bellum

Common approaches towards assessing the principles of international law in relation to cyber attack include referring to the rules entrenched in the Laws of War.[23] The *jus ad bellum* paradigm is a convention that outlines when states are lawfully permitted to engage in war. The *ad bellum* principle governs permissible transition from peace to conflict (Foltz 2012) and establishes standards and procedures that dictate when countries may use force to resolve disputes (Graham 2010).

A state response to any type of armed attack must satisfy several criteria in order to justify going to war (Hoisington 2009). Legitimate authority, just cause, last resort, reasonable hope for success, and immediacy are all factors that must be taken into consideration before engaging in conflict. Each element must be fulfilled in order for a state to justify going to war and are applicable to all cases of conflict including cyber attack. Legitimate authority refers to the collective acceptance of the international community supporting a state's decision to participate in conflict (Megret 2006). Just cause alludes to the reasoning and justification behind entering war (Deller and Burroughs 2003). The last resort rule states that force may only be used after countries have fully exhausted all diplomatic channels to resolve conflict (Hathaway *et al.* 2012). Fourth, according to *ad bellum*, a state may only engage in battle if it possesses a reasonable hope for success prior to

[23] The concept of *jus ad bellum* was developed by classical Greek and Roman philosophers seeking to establish guidelines for justified war. Among its contributors were Aristotle, Cicero, St. Augustine, Thomas Acquines, and Hugo Grotius. Each philosopher offered his own views of permissible war that together have defined the current understanding of the law. For more information, see Kolb (1997).

declaring war. Finally, immediacy refers to the length of time by which a state is entitled to respond in the name of self defence (Hughes 2010). A country may immediately defend itself if attacked and may not postpone its retaliatory strike to an unreasonable time in the future.

One can argue that a cyber response was justified during the 2008 cyber attack against Georgia. Similar to the conflict in Estonia, in this case Georgia suffered a massive cyber attack that crippled the country's national communications networks. The attack was allegedly conducted by the Russian Business Network and used botnets to overload cyber networks that denied the government communication with its citizens or other countries (Swanson 2010; Ophardt 2010). Had Georgia still held the required weaponry to launch a strike after absorbing the Russian attack, it would have been justified in retaliatory measures in order to preserve any remaining national cyber infrastructure. A hypothetical Georgian response to the attack would have satisfied the criteria outlined above and is an example of a circumstance where a country could justifiably react to a cyber attack under the *ad bellum* laws.

Law of Armed Conflict: Jus in Bello

The bulk of debate concerning the legality of cyber weapons stems from the Law of Armed Conflict (LOAC), also referred to as international humanitarian law (IHL). International humanitarian law is the arm of public international law that attempts to minimize the harm and suffering that occurs during war (Swanson 2010). IHL and the LOAC put forth a set of rules that dictate permissible state behaviour during wartime. These regulatory principles are reflected in the *jus in bello* principles governing actions during international conflict. *Jus in bello*[24] includes both the Geneva and Hague agreements, the former deriving from the 1949

[24] Similar to the origin of *ad bellum*, the *in bello* principle stems from contributions of classical Greek and Roman philosophers striving to define moral and permissible war. The notions and principles established by these philosophers set the foundation for future 20th century treaties, including the Law of Armed Conflict aiming to regulate conflict as well as the Geneva and Hague Conventions.

Geneva Conventions and 1977 Additional Protocols while the latter originate from the 1899 and 1907 Hague Conventions outlining the methods of warfare and conduct of hostilities (Swanson 2010). Presently, there is no scholarly or international consensus on the application of *in bello* principles to the cyber world (Hughes 2010). Some scholars remain hesitant to fully accept the ability of an old-style LOAC to regulate ongoing cyber warfare citing attribution difficulties while others insist that the LOAC is adaptable to all forms of interstate conflict.

First, experts unsure of the relationship between the LOAC and cyber weapons stress that these international customs are outdated, ambiguous, and unclear on how to effectively monitor and control the use of contemporary cyber weapons (Korns and Kastenberg 2009). Similar to criticism of the UN Charter, the Geneva Conventions were last updated in the midst of World War II where traditional weaponry dominated the battlefield. Drafters of the Geneva Conventions were unconcerned with the ability of international treaties to regulate cyber attack, an unheard of concept at the time of its establishment (Hathaway *et al.* 2012). This argument claims that half-century old, specific goal-oriented treaties are incapable of supervising a phenomenon that was inconceivable at the time of drafting. Moreover, those opposed to the LOAC's cyber regulatory power underline the disconnection between modern warfare techniques and conventional methods of combat. The distance isolating cyber combatants from their weapons' effects triggers a detachment from customary humanitarian tendencies that are much more greatly apparent when engaging in traditional armed conflict (Hughes 2010). Finally, individual state interpretation of war makes it extremely difficult to blanket one uniform set of rules to govern all state-sponsored cyber behaviour (Kanuck 2010). Put differently, states have their own view of how the LOAC applies to their militaries (Nakashima 2012) and will act according to how the law serves their national interests.

In contrast, several experts defend the ability of the LOAC to govern cyber attack or allege that parts of the law are applicable while others require more study.

These scholars believe that the core features of the law are effective and that minor details questioning the principles of the law are not sufficient to discredit their intent (Dunlap 2011; Geib 2010). While the language used in the LOAC is important, the principles entrenched in IHL hold a higher priority when examining the legality of a cyber attack.

Counter arguments proposing that not all cyber attacks are physical in nature and therefore escape the jurisdiction of the LOAC overlook Article 2 of the Geneva Convention that explains that all principles in the convention are applicable to all cases of war, regardless of whether that war is officially recognized by a state-party (Swanson 2010). This vision held by *in bello* supporters contends that the LOAC rules apply to all cases of war notwithstanding a state's willingness or unwillingness to acknowledge certain behaviours during combat. Overall, the LOAC regulates the very phenomenon its name suggests, armed conflict, and so long as cyber weapons qualify, the LOAC is fully capable of imposing restrictions on actions of states during war.

One of the most frequently discussed components of the LOAC as it relates to the use of cyber weapons during conflict is the 1977 Geneva Convention amendments referred to as the Additional Protocols. The Additional Protocols were added to ensure the protection of victims and civilians during armed conflict. Additional Protocol I identifies permissible and illegitimate targets during wartimes including hospitals, places of worship, essential services, and other civilian used facilities and resources (Randall 2010). Certain aspects of the 1977 amendments only apply to state parties and exclude non-state actors. According to some, the omission of non-state actors fails to protect founding principles of IHL and may limit the LOAC's ability to protect civilians when non-governmental organizations participate in cyber attacks (Swanson 2010).

The major themes of Additional Protocol I include the principles of distinction, proportionality, military necessity, unnecessary suffering, and perfidy (Richardson 2011; Graham 2010; Hathaway *et al.* 2012). Additional Protocol I states that countries engaged in

armed conflict must at all times distinguish between civilian and military targets where the former are prohibited from being attacked while the latter are acceptable (Kelsey 2008; Schmitt 2010; Hughes 2010; Kanuck 2010). The rule of distinction has difficulty regulating cyber weapons attacking civilian infrastructure because of their growing military applications (Hughes 2010). For instance, privately owned communications networks are often contracted out to state militaries, which raises questions as to whether or not such civilian-intended resources are sanctioned by the LOAC.

Secondly, the proportionality law refers to the balance between the amount of damage or loss of life a state inflicts during its attack and its military objective (Hathaway *et al.* 2012). In other words, an attack must not be excessive in relation to the perpetrator's goal. In the cyber realm, an attack against a foreign communications network primarily utilized by the military may nonetheless infect civilian networks triggering unintended yet illegal casualties or even death to civilians (Jenson 2010; Schmitt *et al.* 2013). This phenomenon is commonly referred to as the "spill over effect" where a cyber attack is anticipated to produce a specific outcome upon a military target but leaks out into the public domain prompting civilian casualties (Richardson 2011).

Third, Article 52 of Additional Protocol I outlines the premise behind military necessity noting that states are permitted to attack military targets only in circumstances that offer a "definite military advantage." [25] Article 52 provides that states may conduct attacks that establish an effective military advantage on objects, which by their nature, location, purpose or use, affect civilian life. In this light, a cyber attack may be considered unlawful should the attack affect civilians without bolstering a country's military advantage (Hathaway *et al.* 2012).

A fourth key highlight of Additional Protocol I includes restrictions on intentional deceiving efforts to mislead adversaries into believing combatants are

[25] Article 52 (2) Additional Protocol, I Geneva Convention 1977.

protected by international law from attack. This practice, referred to as perfidy, is difficult to apply to cyber space because of the challenge of assigning labels or markings to acceptable or unacceptable targets (Kanuck 2010). For instance, hospitals are clearly marked with a red cross to inform offensive attackers that the facility is protected by international law. The same cannot hold true for cyber networks where identification and labeling of computer systems becomes lost in the ubiquity of the Internet and cyber networks.

Lastly, the final two issues that spark the most debate regarding the applicability of the LOAC and Additional Protocol I to cyber attacks are the notions of attribution and neutrality. Beginning with attribution, analysts of international law and cyber weapons note the highly significant role of ascribing an action to an actor. Article 51 of Additional Protocol I affirms that in order for a state to act in self defence, that state must first fully prove the identity of the perpetrator before responding (Farwell and Rohozinski 2011). Without attributing an attack to a specific entity, approaches and techniques employed to assess the use of force are limited in their application (Foltz 2012). As a result, unattributable attacks, although perhaps unlawful under international law, are not necessarily violations of the LOAC (Schmitt *et al.* 2013). It is for this reason that many contend that international law is incapable of governing cyberspace because of the lack of concrete proof that link cyber attacks to states.

Compounding the attribution problem is the role of non-state actors (NSAs) in cyber space. The vast majority of scholars claim that correctly identifying actors in cyber space is becoming increasingly difficult because of the large number of NSAs operating in this domain (Harknett *et al.* 2010; Glennon 2012; Farwell and Rohozinski 2011; Gjelton 2010; Geib 2010; Platt 2012; Meyer 2011; Kelly and Almann 2009). In addition to determining which NSAs may be behind a hypothetical cyber attack, locating these NSAs and ascertaining their intent of using a cyber weapon is difficult (Bayles 2001; Hoisington 2009). Many cyber experts note the potential for states to intentionally employ the services of NSAs to conduct cyber attacks

while denying involvement on the international stage. This action is referred to as "plausible deniability" where states dictate a cyber task to a NSA and deny responsibility to onlookers (Geers 2010; Randall 2010; Jenson 2010; Hathaway *et al.* 2012). States planning a cyber attack can carry out their operations via a non-state actor and comfortably hide behind the identity of that organization. Scholars are concerned that states using NSAs as "scapegoats" may become a common practice that eludes international law (Manson 2011; Randall 2010).

The second major issue is neutrality. Currently under international law, uninvolved states, or countries not a party to a specific conflict, are obligated to prevent their neutrality from becoming a launching pad used by foreign states (Prescott 2012). Failure to safeguard one's state from external military operations may forfeit a state's neutrality and characterize it as a contributor to the attack. Monitoring neutrality in cyber space is difficult because of the substantial amount of network interconnectivity between countries. The ubiquity and free flow of cyber content makes it nearly impossible to establish the fundamental principle of territoriality during conflict, a principle that is vital in establishing whether a country remains neutral during war (Hughes 2010; Jenson 2002).

Presently, states are forbidden from intentionally allowing others to use domestic cyber infrastructure for conducting an illegal cyber attack (Schmitt 2013). However, unintentional or unknown exploitation of domestic computer systems is difficult to govern. There is general agreement that cyber attacks are fully capable of being routed through neutral countries (Jenson 2002), triggering the question of how a state is expected to know if its cyber infrastructure is being exploiting by foreigners during external conflict. Or, what may be worse, if a state did learn that its computer systems were being used as a gateway for foreign conflict, the question arises of whether the neutral state would be obligated to shut down its cyber infrastructure at the risk of severely damaging its own governmental operations or economy (Kanuck 2010). Although the answer to this question may be unclear, a mere passage of information through a

third party's computer infrastructure is not sufficient evidence to attribute that state's involvement to a cyber attack (Schmitt 2010).

Part II

Cyber Weapon: Stuxnet

The Stuxnet weapon is a precedent-setting cyber attack that illustrates the challenges of applying traditional notions of international law to cyber warfare (Talbot 2011; Ashford 2010). Stuxnet is a computer virus that was allegedly developed in 2009 by Israel in partnership with the United States to sabotage the Iranian nuclear weapons program (Sanger 2012; Waxman 2011; Esposito 2011; Banks 2012). It is the world's most sophisticated cyber weapon (Farwekk and Rohozinski 2011; Rid 2012a; 2012b; Hoffman 2011) and is capable of secretly infiltrating the operating systems of critical infrastructure while gradually destroying its components without alerting operators (Farwell and Rohozinski 2011).

The virus targets computer-based devices that control and monitor the daily activities of machines in factories, industrial plants and other types of major facilities that are dependent on complex computer systems for management. Specifically, Stuxnet infects Microsoft's Windows operating system and latches on to a supervisory control and data acquisition (SCADA) system (Gross 2011) manufactured by the engineering and electronics company Siemens (Sugrue 2010; Brown and Poellet 2012; Rid 2012a). Though SCADA systems are capable of servicing a number of different devices and electronic instruments, Stuxnet's primary targets are programmable logic controllers (PLCs), a popular operating mechanism employed by industrial plants to run machinery. In the case of Iran, it has been alleged that between 2009-2010 the virus was directed at the nuclear centrifuges engaged at producing enriched uranium. The malware aims to manipulate, hinder, or prevent PLCs from directing the operations of electrical hardware (Collins and McCombie 2012).

To avoid detection, Stuxnet contains a number of different types of anti-virus evasion techniques, each designed to mislead computer protection software and

elude firewall services. For instance, the malware is capable of duplicating itself on multiple removable drives, conceal its identity during PLC inventory procedures, and destroy itself from machines that are not affiliated with the intended target (Ashford 2010; Rid 2012a; Foltz 2012). Another distinguishing feature of Stuxnet is that the virus can fulfill its objective without the use of the Internet. Unlike most cyber weapons, Stuxnet may only be launched through USB sticks or by introducing the malware directly to the target (Farwell and Rohoninski 2011; Ashford 2010; Hoffman 2011). It operates independent of the Internet and does not require computer networks to be linked together in order to complete its task.

Stuxnet infected many computer systems in a number of different countries, however the weapon's primary targets were Iranian centrifuges at the country's nuclear enrichment facility in the city of Natanz. Over sixty-two thousand computers were infected in Iran, with the second highest infection rate being thirteen thousand computers found in Indonesia (Richardson 2011). The Iranian uranium enrichment facility operates using a number of PLCs required to spin centrifuges at very high speeds in order to converge uranium isotope into light water reactors for energy, or perhaps to form fissile material for a nuclear weapon (Nakashima 2010; Farwell and Rohozinski 2011). Stuxnet targeted the facility's operating PLCs, eventually manipulating the rate of rotation of each centrifuge over a lengthy but consistent period of time (Foltz 2012). The effects of Stuxnet drastically decelerated Iran's uranium enrichment process and forced the state to replace nearly one thousand centrifuges (Esposito 2011; Hoffman 2011; Foltz 2012; Sanger 2012). International inspectors monitoring the status of the Iranian enrichment program confirmed the damage done to the centrifuges (Richardson 2011). The International Atomic Energy Agency (IAEA) reported that for one full week in November 2009, Iran had fully ceased delivering uranium into its centrifuges, citing a substantial breakdown in the operations of each one (Farwell and Rohozinski 2011). Following the attack, Iran refused to admit the seriousness of the damage caused by Stuxnet

and denied that its nuclear program suffered any delay. State officials as well as leaders of Iran's Atomic Energy Department insisted that operational setbacks in its nuclear program were the sole result of technical difficulties and rejected any claim that they had been attacked (Sugrue 2010; Brown and Poellet 2012).

Although neither Israel nor the United States has ever officially accepted responsibility for the attack, there are several indicators that suggest both countries were involved. Firstly, analysts of the weapon speculate that the designers of Stuxnet likely manufactured a simulated uranium enrichment facility to test the weapon and perfect its technology (Rustici 2011; Rid 2012a; Richardson 2011). The architects behind the virus possessed the essential intelligence and information necessary to build an exact replica of the Iranian uranium site in order to ensure the accuracy of Stuxnet's objective. Experts believe that the only actors capable of performing this task are well resourced, technologically advanced, and intelligence-yielding Western states (Richardson 2011). Secondly, in addition to the abundance of resources required to manufacture Stuxnet, only politically motivated countries were likely to launch the weapon against Iran (Hoffman 2011). Both Israel and the United States are alleged to possess the key intelligence and funding required to develop such a precise cyber weapon and both have a national interest in terminating the Iranian weapons program in order to maintain international peace and security (Talbot 2011).

It is important to note that unlike other cyber or conventional weapons, Stuxnet behaves differently and may produce negative consequences. Stuxnet can gain access to its target, complete its objective, and exit discretely without causing large explosions or damage associated with conventional military weapons (Banks 2012; Sanger 2012). Cyber weapons such as Stuxnet are also significantly cheaper than traditional weaponry (Farwell and Rohoninski 2011). Whereas most weapons are expensive to manufacture and may contain risky side effects during construction, the creation of Stuxnet was relatively inexpensive (Coll 2012) and was built without the worry of hazardous byproducts being created. The cost of constructing a cyber weapon, even one as

sophisticated and advanced as Stuxnet, is considerably less than acquiring fighter jets or constructing precision drone missiles (Lewis 2010; Farwell and Rohoninski 2011). Finally, the most notable difference between the Stuxnet virus and conventional weapons is that once launched, Stuxnet cannot be easily controlled (Gjelton 2010). The creators of Stuxnet are unable to monitor or precisely evaluate the damage caused by the virus. Unlike a bomb, those struck by the Stuxnet weapon may harness the worm, reverse engineer it and relaunch it back at its creators (Nakashima 2010; Farwell and Rohoninski 2011; Sanger 2012).

Analysis: International Law and Stuxnet

The review of existing international law in Part I, and the above background of Stuxnet, will assist in analyzing how international laws and customs could have applied to the 2009 Stuxnet attack against Iran. A careful examination of each law reveals that some international institutions had some relevance to Stuxnet while others did not. Article 2(4) of the UN Charter is applicable to Stuxnet and would characterize the cyber attack as a use of force. Second, UN Articles 39, 41 and 42 would each have struggled in responding to Stuxnet because of gridlock in the Security Council. Third, Stuxnet may have amounted to an armed attack; however, it would not have warranted a response under Article 51 because of a lack of identity. Fourth, the *jus ad bellum* principle justifies the motive behind the deployment of Stuxnet. Finally, despite complying with the fundamental rules of the LOAC, the *jus in bello* paradigm could not have controlled the behaviour of Stuxnet against Iran.

Stuxnet and Article 2(4)

Stuxnet did violate the prohibition on the threat or use of force as outlined in Article 2(4) of the UN Charter. Two out of the three approaches examined in Part I confirm that Stuxnet used force against the Iranian nuclear facility to undermine the territorial integrity and political independence of Iran. The first approach is the lone dissenting view that the Stuxnet attack did not use force. The strict approach immediately dismisses this

claim because it argues that force can only be exerted onto foreign states through direct military strikes. Stuxnet was not a use of force through traditional military means and therefore could not have violated Article 2(4) (Chen 2010). Conversely, the second approach places heightened emphasis on the instrument used during a potential use of force. According to this approach, Stuxnet was a violation of Article 2(4) because the virus was capable of performing the same task as conventional weaponry (Foltz 2012). The cyber attack damaged the territorial integrity of an independent state and is not exempt from the law solely because the instrument operates in the cyber domain.

The third approach is the Schmitt analysis. This model also verifies that the Stuxnet attack was a use of force because the attack fulfilled several criteria on the seven-factor scale. The first factor, severity, was displayed by the physical damage Stuxnet inflicted in the Iranian nuclear facility (Foltz 2012). Over one thousand centrifuges were damaged and ultimately replaced owing to the virus. Second, the immediacy factor suggests that Stuxnet did not employ a use of force because the attack was a slow process that transpired over a span of ten months (Foltz 2012). The directness factor claims Stuxnet was a use of force because of the direct correlation between the use of the weapon and the resulting centrifuge damage. Fourth, invasiveness, which measures the degree of weapon penetration, would not have classified Stuxnet as a use of force because of the weapon's limited targeting capabilities (Richardson 2011). The fifth element, measurability, suggests Stuxnet displayed a use of force because of the high number of centrifuges requiring replacement (Richardson 2011). Sixth is the notion of presumptive legitimacy. Stuxnet's objective was justified because it targeted an unlawful nuclear program condemned by the United Nations (Glennon 2012; Foltz 2012). The final criterion, responsibility, cannot be used to evaluate 2(4) because the creator of the cyber attack has yet to be confirmed (Foltz 2012).

In sum, the Stuxnet attack against Iran did amount to a use of force prohibited by Article 2(4) of the UN Charter. With the exception of the first strict

interpretation, other guidelines and indicators set in place by scholars to measure when a cyber attack amounts to a use of force reveal that Stuxnet did violate Article 2(4). This analysis will be useful to ascertaining whether similar cyber attacks amount to use of force and may assist in deterring states from launching using cyber weaponry. Depending on the type of Article 2(4) definition employed, this provision of the UN Charter may serve as a mechanism offering greater accountability to countries contemplating such attacks. However, it, in conjunction with previous precedents of states going unpunished when violating the prohibition of the use of force, cannot negate other aspects of international law incapable of governing similar cyber attacks.

Stuxnet and Articles 39, 41 & 42

Although the Stuxnet attack has not officially been attributed to any particular actor, if the United States and Israel were deemed to be lawfully responsible, would the UNSC retain the authority to issue a diplomatic or military response under Article 39, 41 and 42 of the UN Charter? The UNSC may make recommendations on how to respond to threats or breaches of peace in order to maintain international security (United Nations Charter, Article 39). However, the use of Stuxnet against the Iranian nuclear program to slow down or halt the potential development of nuclear weapons did not represent a threat or breach of peace to the international community. The UNSC assesses suspected breaches of international peace on a case-by-case basis (Lourdes 2011). In order for any case to be labeled as a breach of peace, the alleged action must violate the purposes and principles of the United Nations (Lourdes 2011). Stuxnet's purpose aligned with the peaceful principles of the UN by denying Iran access to enriched uranium for nuclear weapons. [26] UNSC Resolutions such as 1737, 1747, 1803, and 1929[27] all

[26] See the *jus ad bellum* section below for further details regarding previous UNSC resolutions imposing economic sanctions against Iran.

[27] Security Council Resolutions 1737, 1747, 1803, and 1929 are discussed further in the subsequent sections. For further

contain peaceful mechanisms that aim at terminating the Iranian nuclear program.

If, in the unlikely event that the UNSC had decided the Stuxnet cyber weapon did represent a breach of international peace, the UNSC may have responded in one of two ways. First, the UNSC could have developed recommendations that call for non-uses of force to reprimand the offence. Alternatively, the Security Council could have used force to restore the peace. In both cases, efforts to curb the Stuxnet attack through diplomatic or uses of UN force could not have been established until the malware was discovered, which was long after the attackers deployed the cyber weapon and out of the creator's control (Collins and McCombie 2012). The damage would have already occurred, leaving any recommendations put forth by the UNSC ineffective in preventing or circumventing the Stuxnet attack.

Compounding this challenge is the power of the veto possessed by the United States. It is unrealistic to assume the U.S. would willingly permit UNSC action, even diplomatic resolutions, against its own infection. Bear in mind that each of these hypothetical situations may only occur assuming the identify of Stuxnet's owners is confirmed and thus further contribute to the inability of the Article 39, 41, and 42 to regulate the Stuxnet cyber attack. Unless the UNSC was able to identify the cyber weapon during the course of its attack; legally attribute responsibility to the Stuxnet inventors; and override the expected use of the U.S. veto throughout the resolution development process, Articles 39, 41, and 42 were all incapable of regulating the Stuxnet attack.

Stuxnet and Article 51

The final feature of the UN Charter that could have affected the outcome of the Stuxnet attack is Article 51 and the notion of self defence. Recall that Article 51, the inherent right to self defence, is interpreted by three different approaches. The effects-based, instrument-based, and target-based approaches

---

information, visit the UN Resolution webpage: http://www.un.org/en/sc/documents/resolutions/2013.shtml

are all used to determine if a state is suffering an armed attack. According to the effects-based approach, the Stuxnet attack may be classified as an armed attack against Iran because of the overall damage and harm inflicted by the cyber weapon against Iranian sovereign territory (Richardson 2011). Because Stuxnet yielded the same result that could have been achieved by a conventional military strike (Sanger 2012), the cyber weapon qualifies as an armed attack. Altering the rotation speeds of centrifuges could have been accomplished by physical insurgence of military personnel, an electro-magnetic pulse, or through a ballistic missile strike, all of which are regarded as an armed attack under the effects-based approach (Nakashima 2010; Ashford 2010).

Conversely, the instrument-based approach analyzes the tool used during a strike to ascertain if the attack is considered an armed attack. In the view of this approach, Stuxnet was not an example of an armed attack because the virus is not an "armed" weapon as understood in relation to traditional weaponry (Richardson 2011). Finally, the target-based approach holds that an armed attack did occur by Stuxnet and would have permitted the use of self defence. This is because Stuxnet targeted the cyber infrastructure of Iran's military program, assuming the uranium enrichment facilities Stuxnet infected were intended to fuel a nuclear weapons program (Richardson 2011). Should Stuxnet have struck a military procurement project in any other country, the target-based approach would recognize that action as an armed attack as well. As a result, Iran would have been justified in responding in self defence under Article 51.

In addition to the various approaches analyzing Stuxnet's relationship to Article 51, the Stuxnet attack was not officially recognized by the Iranian government (Sanger 2012), leading to a lapse in self defence protocol. In order for a state to act in self defence, the victim country must publicly renounce the instigating attack (Brown and Poellet 2012; Foltz 2012). In the Stuxnet case, Iran did not announce that its nuclear program was injured as a result of any cyber weapon (Waxman 2011). The Iranian government remained

relatively quiet during the attack period suggesting that it did not consider Stuxnet to be an armed attack or punishable under international law (Brown and Poellet 2012; Foltz 2012).

Publically acknowledging that the virus successfully damaged its nuclear program would have exposed Iran as vulnerable. Likewise, admitting to suffering a cyber attack would have diminished Iran's nuclear threat and deterrent throughout the Islamic world. Because Iran chose not to condemn Stuxnet, it forfeited the opportunity to denounce the virus as an armed attack. The most likely explanation for Iran's silence was that the state was embarrassed of damage suffered by the attack and feared that acknowledging the attack would have been perceived as an admission of weakness.

Though indicators on both sides of the debate provide convincing evidence, ultimately, the use of Stuxnet against Iran did not constitute an armed attack because the designer of the cyber weapon remains unknown and unconfirmed (Platt 2012). Certainly Iran could have been justified in defending itself given the damage the country suffered; however, any defensive action would be meaningless without a particular entity to direct a defensive strike against (Talbot 2011). If the owners of Stuxnet were confirmed and self defence could be performed with confidence, then perhaps the 2009 use of Stuxnet would constitute an armed attack triggering self defence. However, the facts prove otherwise and conceal the identity of the attacker, rendering Article 51 ineffective in relation to Stuxnet.

Though not explicitly stated in Article 51, many have assumed that the concept of self defence described in the UN Charter includes the notion of anticipatory self defence where states retain the right to defend themselves preemptively when confronted with an imminent attack. The concept of anticipatory self defence is unique when applied to Stuxnet because the phenomenon may be used to describe the reasoning behind the launch of the cyber weapon in the first place. As mentioned above, many propose that the development and deployment of Stuxnet was precipitated by the relentless and uncooperative

progression of the Iranian nuclear program (Banks 2012). The creators of Stuxnet were acting preemptively when attempting to sabotage the enrichment facility in order to prevent the development of illegal nuclear weapons. Stuxnet's purpose was consistent with numerous UN resolutions aimed at discontinuing the Iranian nuclear program (Foltz 2012). The recent tightening of sanctions against the Iranian regime is an example of a preventative measure employed by the international community aiming to halt the nuclear program. Although not specifically outlined in Article 51, the Stuxnet attack was lawful under the anticipatory notion of self defence.

Stuxnet and the Jus ad Bellum Principle

The *jus ad bellum* application to Stuxnet is similar to that of Article 51's and offers interesting insight into whether or not the use of Stuxnet was permitted under the Laws of War. According to the *ad bellum* principle, Stuxnet did not violate international law and was justified. The utilization of the virus satisfied four of the five most frequently cited criteria permitting states to use force. The first gauge is legitimate authority and is the only measure by which Stuxnet failed. Although Stuxnet was used preemptively, the weapon was not sanctioned by the international community or by any international organization, thus failing to comply with the legitimate authority requirement (Gross 2011). However, the Stuxnet attack satisfied the second *ad bellum* prerequisite, just cause, because the cyber weapon aimed to sabotage the development of an illegal nuclear program, which would pose an existential threat to Israel (Cook 2010).

The third criterion is last resort. Stuxnet was only launched after several diplomatic efforts by the international community geared at ending the Iranian nuclear program failed. Throughout the past decade, Iran has continually ignored Security Council Resolutions 1737, 1747, 1803, and 1929 (Kimball 2010), all of which contained different types of peaceful sanctions against Iran including an arms embargo, freezing financial assets, and heavy monitoring of state transactions. Despite their crippling effects, Iran continued to disobey

the UN resolutions and carried on enriching uranium, calling for alternative methods to enforce the UN's directive.

Fourth, Stuxnet survived the "reasonable hope of success" test for permissible war because the weapon successfully completed experiments prior to its release in 2009 (Broad *et al.* 2011). Recall that analysts of the virus have repeatedly confirmed that Stuxnet was tested in mock enrichment facilities to ensure the virus could produce the desired results (Sanger 2012).

Finally, the immediacy component of the *jus ad bellum* principle is inapplicable in the Stuxnet case because the cyber weapon was used preemptively, disqualifying the attack from the short time measurement required by the immediacy rule. In other words, because Stuxnet was used before the Iranians were able to develop and launch a nuclear weapon, the length of time by which the hypothetical victim state is entitled to respond is void because Stuxnet was used in anticipation beforehand. Each factor measuring the legality of going to war indicates that Stuxnet was consistent with the *ad bellum* paradigm and did not violate the rules set in place to regulate when states may or may not go to war.

Stuxnet, Jus in Bello, and the Law of Armed Conflict

The final area of international law used to examine the Stuxnet cyber attack is the LOAC and *jus in bello* model. Would the LOAC have been capable of governing the use of Stuxnet during the cyber attack in Iran? Recall that the *in bello* principle regulates the actions and behaviour of parties in war. The law outlines how states are permitted to act during attacks and forbids parties from engaging in non-humanitarian wartime conduct.

The Stuxnet attack was consistent with the LOAC and complied with the principles ingrained in international humanitarian law. The attack respected the humanitarian *in bello* laws that are exhibited in the Geneva Conventions and Additional Protocols and complied with the major principles stated in each statute. Principles such as distinction, proportionality, military necessity, unnecessary suffering, and perfidy were all met throughout the Stuxnet attack demonstrating that the

virus did not violate the long standing rules embedded in international law (Foltz 2012).

Before examining each factor, it is important to recognize that the LOAC is applicable to Stuxnet and can be applied to the cyber attack in 2009 (Glennon 2012). This is because the LOAC regulates all brands of conflict, including the destructive characteristics of Stuxnet (Glennon 2012), and is not limited to specific types of warfare. Cyber attacks are not exempt from the LOAC simply because they are an unfamiliar source of conflict. Article 2 of the Geneva Convention explicitly states that the rules and laws highlighted in the convention are applicable to all cases of conflict (Swanson 2010). Critics arguing that the LOAC does not apply to cyber warfare because attacks are new and unconventional have overlooked the overall intent of the LOAC and fail to understand that cyber conflict is still a form of conflict (Cook 2010). Reinforcing this theme are the studies conducted by different research institutions that aim to ascertain the role of the LOAC in relation to cyber attacks. The United States National Research Council confirms that the overlying principles rooted in the LOAC do pertain to cyber attacks, particularly concerning the law controlling wartime actions (Hughes 2010). Similarly, a major study carried out by a committee of the U.S. National Academies concluded that all cyber attacks are bound by *jus in bello* laws and are expected to abide by the specific rules and litmus tests defined in LOAC statutes (Meyer 2011). Some cyber attacks may not necessarily survive the LOAC requirements for a legal cyber attack; however, they are each accountable to those rules and are required to obey them.

First, the Stuxnet attack fully complied with the notions of distinction and proportionality by avoiding all civilian targets in Iran and solely directing its attack against the Iranian nuclear program. Stuxnet satisfied the distinction test by taking all precautions to ensure that the weapon steered away from civilian cyber networks and only targeted military infrastructure (Gervais 2012). The virus was designed to only affect PLCs in the Iranian enrichment facility and if latched onto anything but its target, would self-destruct and cause no harm or

damage (Rid 2012b; Gervais 2012). Arguments pointing out the difficulty with distinguishing between civilian and military targets in cyber space may be dismissed because the Iranian uranium enrichment facilities operated in an air-locked environment where computer networks were sealed from the Internet and denied access to any online interaction which could have leaked out into the public (Sanger 2012). The "spill over effect" was not a concern in the Stuxnet case because of the weapon's targeting capabilities. As a result, the Stuxnet attack was careful to only affect centrifuges, obeying the distinction rule (Richardson 2011).

Second, Stuxnet did not violate the military necessity principle. This rule questions Stuxnet's need to attack Iran in order to gain a military advantage while affecting civilians. As already determined, Stuxnet only targeted centrifuges while attacking the Iranian nuclear program and did not leak out to the public domain (Chen 2010; Collins and McCombie 2012). Likewise, the attack did not attempt to bolster the creators' military position, but rather was deployed to ensure the safety of civilians susceptible to a future Iranian nuclear attack. This is especially evident since no state or entity has taken responsibility of the attack suggesting that garnering military strength was not the objective of the virus.

Third, Stuxnet did not induce any unnecessary suffering among civilians owing to the limited targeting techniques of the weapon (Richardson 2011). Indeed, no suffering of any kind occurred during or following the attack, clearing the malware of the unnecessary suffering test. Finally, perfidy, the concept of intentionally deceiving an opponent into believing that a legitimate target is a civilian-protected institution safeguarded by international law, is not applicable to the Stuxnet case because the cyber weapon was an offensive attack and did not hide behind sanctuary. Stuxnet did operate covertly, but did not use civilian status as a smoke screen to execute its task.

Two final characteristics of the LOAC, the issues of neutrality and attribution, were also respected by Stuxnet and further illustrate the legality of the cyber attack. The matter of neutrality was relatively

inapplicable to the Stuxnet case because of how the cyber weapon was used. Stuxnet did not make use of the Internet when infecting the Iranian nuclear equipment. Recall that the virus infected the Iranian facilities by hard-drive and was not dependent on global interconnected computer systems in order to achieve its mission (Collines and McCombie 2012). As a result, the principle of neutrality was unaffected by the cyber weapon because third party states were not exposed to the malware potentially sifting through cyber infrastructure and servers in foreign countries (Schaap 2009). States were not concerned that their territories were used as a launching pad for the Stuxnet weapon because the malware did not operate in that fashion. The issue of neutrality was uninfluenced by the cyber attack.

The dilemma of attribution, on the other hand, was widely apparent in the Stuxnet case, revealing the difficulty of applying the LOAC to the attack. As discussed above, the identity of Stuxnet's creators is unknown. There is no official acknowledgement of who developed or launched the cyber weapon (Arquilla 2012). Although it is highly likely that the U.S. and Israel were behind the Stuxnet attack, neither government has admitted responsibility (Stevens 2012; Sanger 2012; Glennon 2012; Hoffman 2011; Chen 2010). Because Article 51 of Additional Protocol I calls for the identity of perpetrators during conflict in order to authorize retaliatory action, Stuxnet could not have been responded to by the Iranians owing to the unknown identity of the weapon's developers. Iran needed to prove the identity of Stuxnet's designers in order to justifiably mount a response (Meyer 2011). A war originating from the Stuxnet attack could not be governed without attributing responsibility. Thus, despite complying with each of the LOAC criteria evaluated above, any action by Iran or the international community to prevent, end, or punish the Stuxnet attack would be ineffective and render the LOAC ineffective in regulating the cyber attack. In sum, although Stuxnet obeyed the law, the LOAC would have been unable to control the action of the cyber weapon because of the lack of identity (Cook 2010).

Although a significant amount of evidence suggests that multiple states were involved, it is important not to entirely rule out the possibility of non-state actor participation in the cyber attack. If Stuxnet was discovered to be launched by a non-state actor, perhaps at the behest of a state, this scenario would have also evaded the regulatory powers of the LOAC and block Iran's ability to respond because of the additional restraints and challenges associated with binding non-state actors to international law. Additionally, a hypothetical scenario whereby a country was responsible for the attack but deflects responsibility to a NSA would hinder the LOAC's ability to delegate accountability and regulate the Stuxnet attack. The responsible state would enjoy plausible deniability while watching the international community struggle to apply LOAC to the Stuxnet attack. Both non-state actor scenarios would present inherent challenges to the LOAC in governing the Stuxnet attack. They further demonstrate how the LOAC would have been ineffective in regulating Stuxnet.

States must take care to recognize the inability of international law to regulate the Stuxnet cyber attack and act accordingly. The failure of international law to identify and locate cyber perpetrators leaves a gaping hole in cyber international governance that aggressors may exploit should the proper precautions be overlooked. Any country dependent on mass computer network infrastructure for daily activities should seek out the essential cyber security safeguards required to shield computer-driven facilities and block external intrusions. Today, there are numerous cyber security companies and software that offer continuous and uninterrupted firewalls that alert owners of critical infrastructure to potential breaches in their computer systems. Because of the lethal potential held by cyber weapons, states are encouraged to legislate domestic laws that force critical infrastructure to employ the services of vetted and credible cyber defence that are proven to withstand the attacks of future Stuxnet weapons and similar strikes. However, implementing such a system requires further research into the technical side of cyber weapons and the specific breaches weapons such as Stuxnet are capable of

achieving even in air-locked computer networks. The vast amounts of research and high level of complexity involved with implementing such a plan should not be underestimated. Only once states on a national level have learned to grapple with this issue and develop a robust cyber defence strategy capable of warding off similar cyber attack can the international community contemplate negotiating an intergovernmental agreement that works to harmonize the strongest national cyber defence laws in pursuit of cyber security.

Conclusion

The application of international law to cyber attacks will remain a contentious issue that will evolve as the world becomes more exposed to "virtual" weapons. Although much more study of cyber warfare is required to effectively determine how international law applies to cyber attack, the outcome of the Stuxnet attack against Iran is clear - international law could not have regulated the use of the weapon.

Part I of this essay examined the literature surrounding cyber warfare in order to provide the foundation for the analysis in Part II. Different readings into the phrase "use of force" assist in determining which characteristics constitute a violation of UN Charter Article 2(4). Scholars defend the inherent applicability of 2(4) to cyber weapons, deny it, or are unsure of the relationship between the two. Additionally, UN responses to cyber attack are restricted under Articles 39, 41, and 42 owing to frequent indecision and gridlock within the Security Council. Article 51's contentious term "armed attack" is interpreted with three different approaches. The effects-based, instrument-based, and target-based approaches are all used to analyze which cyber weapons rise to the level of an armed attack during conflict. The *jus ad bellum* rule evaluates the legality of engaging in conflict through different measures. Notions of legitimate authority, just cause, last resort, reasonable hope for success, and immediacy are all determinants that ascertain whether or not a state is justified in going to war. Lastly, the *jus in bello* and LOAC principles explore the humanitarian effects of war. The *in bello* rules examine factors such as

distinction, proportionality, military necessity, unnecessary suffering, and perfidy to determine whether a use of force violates international law.

Part II evaluated how the 2009 Stuxnet virus avoided regulation under international law to successfully sabotage the Iranian nuclear program. The three different interpretations of a "use of force" prohibited by Article 2(4) reveal that Stuxnet did amount to a use of force against the Iranian enrichment facility. Articles 39, 41, and 42 each would have failed to sanction a response to the attack because of a sluggish UNSC and owing to the late discovery of the virus. Third, some assessments of Article 51 deem the use of Stuxnet an armed attack while other gauges do not. The effects and target-based approaches suggest that Stuxnet did constitute an armed attack. However, the instrument-based approach and lack of victim acknowledgement indicate that Stuxnet did not violate Article 51. Despite this uncertainty, Stuxnet did operate preemptively illustrating signs of anticipatory self defence. The *ad bellum* application to Stuxnet justified the virus' right to engage in war based on the criteria outlined in Part I. Finally, the Stuxnet attack obeyed the principles of distinction, proportionality, military necessity, unnecessary suffering, and perfidy embedded in the Law of Armed Conflict and did not violate the *in bello* rules governing the behaviour of states during conflict.

This author is skeptical of the ability of existing international laws to regulate emerging cyber weaponry. Many laws and conventions are highly subjective, rarely agreed upon, and require identifying aggressors in order to deter and attribute penalties for illegal activity. As seen by the Stuxnet attack, new technology is changing the way war is fought and thus must be met with an equal and appropriate response. New intergovernmental treaties that aim to prevent future Stuxnet-like attacks are a reasonable start but are limited in their effectiveness as consensus is often difficult to obtain. This challenge is illustrated with the controversial language in both Article 2(4) and Article 51, both of which hinder the UN's ability to address cyber attacks.

One route to overcoming the loopholes ingrained in international treaties is for states to increase their

national defences, particularly their cyber security efforts across all critical infrastructure. Though the Stuxnet weapon appears to have been used in good faith by terminating a potentially lethal Iranian nuclear program, its exposure to the world has set a precedent that both state and non-state actors may attempt to exploit knowing perfectly well that the attack has gone without punishment. States concerned with their own cyber security do not need to wait for the slow and burdensome treaty negotiation processes found within international institutions in order to defend themselves against unknown threats. Instead, while waiting for international laws including the UN Charter and Law of Armed Conflict to modernize, vulnerable countries are encouraged to pursue national efforts that aim to increase public safety and compensate for the current lack of international security embedded across all branches of international law. In a final analysis, this examination reveals both the opportunities and limitations of using international law to regulate an emerging world of warfare.

Works Cited

Andress, Jason and Steve Winterfeld. 2011. "Cyber Warfare Techniques and Tools for Security Practitioners." *Syngress Publications*.

Arquilla, John. 2012. "Rebuttal: Cyberwar is Already Upon Us." *Foreign Policy.* 84-85.

Ashford, Warwich. 2010. "Stuxnet: Demolition Machine for the 21st Century?" *Computer Weekly*. 16-18.

Banks, William. 2012. "Shadow Wars." *Journal of National Security Law & Policy* 5(2): 315-318.

Bayles, William. 2001. "The Ethics of Computer Network Attack." *Parameters* 31(1): 44-58.

Broad, William, John Markoff, and David Sanger. 2011. "Israeli Test on Worm Called Crucial in Iran Nuclear Delay". *New York Times.*

Brown, Gary and Keira Poellet. 2012. "The Customary International Law of Cyberspace." *Strategic Studies Quarterly*. 126-145.

Chen, Thomas. 2010. "Stuxnet, The Real Start of Cyberwar?" *IEEE Network Magazine.*

Clarke, Richard and Robert Knake. 2011. "Securing the GCC in Cyberspace." *The Emirates for Strategic Studies and Research.* 1-42.

Coll, Steve. 2012. "The Rewards and Risks of Cyber War." *The New Yorker*.

Collins, Sean and Stephen McCombie. 2012. "Stuxnet: The Emergence of a New Weapon and its Implications." *Journal of Policing, Intelligence, and Counter Terrorism* 7(1): 84.

Cook, James. 2010."Cyberation' and Just War Doctorine." *Journal of Military Ethics* 9(4): 411-423.

Crawford, Neta. 2003. "The Slippery Slope to Preventive War." *Ethics and International Affairs* 17(1): 30-36.

Deller, Nicole and John Burroughs. 2003. "Jus ad Bellum: Law Regulating Resort to Force." *Human Rights* 30(1): 8-11.

Dunlap, Charles. 2011. "Perspectives for Cyber Strategists on Law for Cyberwar." *Strategic Studies Quarterly.* 5: 81-99.

Esposito, Michele. 2011. "Quarterly Update on Conflict and Diplomacy." *Journal of Palestine Studies* 40(3): 145-181.

Farwell, James and Rafal Rohozinski. 2011. "Stuxnet and the Future of Cyber War." *Survival: Global Politics and Strategy* 43(1): 23-40.

Farwell, James and Rafal Rohozinski. 2012. The New Reality of Cyber War. *Survival: Global Politics and Strategy* 54(4): 107-120.

Foltz, Andrew. 2012. "Stuxnet, Schmitt Analysis, and the Cyber 'Use of Force' Debate." *Joint Force Quarterly* 67: 40-48.

Geers, Kenneth. 2010. "The Challenge of Cyber Attack Deterrence." *Computer Law & Security Review.* 26: 298-303.

Geers, Kenneth. 2010. "Cyber Weapons Convention." *Computer Law and Security Review.* 26: 547-551.

Geib, Robin. 2010. "The Conduct of Hostilities in and via Cyberspace." *American Society of International Law.* 104: 371-374.

Gervais, Michael. 2012. "Cyber Attacks and the Laws of War." *Berkeley Journal of International Law.* 30(2): 525-579.

Gjelten, Tom. 2010. "Shadow Wars: Debating Cyber 'Disarmament.'" *World Affairs.* 173(4):

33-42.

Glennon, Michael. 2012. "State-level Cybersecurity." *Policy Review.* 171: 85-102.

Graham, David. 2010. "Cyber Threats and the Law of War." *Journal of National Security, Law & Policy*. 4: 87-102.

Gross, Michael. 2011. "A Declaration of Cyber War." *Vanity Fair*. 1-6.

Harknett, Richard *et al.* 2010. "Leaving Deterrence Behind: War-Fighting and National Security." *Berkeley Electronic Press*. 7(1): 1-24.

Harley, Brian. 2010. "A Global Treaty on Cyber Security?" *Science and Technology Law Review*.

Hathaway, Oona *et al.* 2012. "The Law of Cyber Attack." *The California Law Review*. 100(4): 817-886.

Hehir, Brian. 1992. "Just War Theory in a Post-Cold War World." *Journal of Religious Ethics*. 20(2): 237-257.

Hoffman, David. 2011. "The New Virology." *Foreign Policy* 185: 77-80.

Hoisington, Matthew. 2009. "Cyber Warfare and the Use of Force Giving Rise to the Right of Self-Defence." *Boston College International Comparative Law Review* 32: 439-454.

Holliday, Ian. 2003. "Ethics of Intervention: Just War Theory and the Challenge of the 21st Century." *International Relations.* 17(2): 115-133.

Hughes, James. 2010. "China's Place in Today's World." *The Journal of Social, Political and Economic Studies.* 35(2): 167-223.

Hughes, Rex. 2010. "A Treaty for Cyberspace." *International Affairs.* 86(2): 523-541.

Jensen, Eric. 2002. "Computer Attacks on Critical National Infrastructure: A Use of Force Invoking the Right to Self-Defence." *Stanford Journal of International Law.* 38: 207-240.

Jenson, Eric. 2010. "Cyber Warfare and Precautions Against the Effects of Attacks." *Texas Law Review.* 88(7): 1533-1568.

Kanuck, Sean. 2010. "Sovereign Discourse on Cyber Conflict Under International Law." *The Texas Law Review.* 88: 1571-1597.

Kechichian, Joseph. 2002. "Strategic Warfare in Cyberspace." *Perspectives on Political Science.* 31(1): 63.

Kelly, John and Lauri Almann. 2009. "eWMSs." *Policy Review.* 152: 39-50.

Kelsey, Jeffery. 2008. "Hacking into International Humanitarian Law: The Principles of Distinction and Neutrality in the Age of Cyberwar." *Michigan Law Review.* 106: 1427-1451.

Kimball, Daryl. 2010. "Dealing With Iran's Uranium." *Arms Control Today.* 40(5): 4.

Korns, Stephen and Joshua Kastenberg. 2009. "Georgia's Cyber Left Hook." *Parameters*. 60-76.

Lewis, James. 2010. "Multilateral Agreements to Constrain Cyber Conflict." *Arms Control Today* 40(5): 14-19.

Lourdes, Monica. 2011. "Interpretation of Article 39 of the UN Charter (Threat to the Peace) by the Security Council." *Mexican Journal of International Law.* 11: 147-185.

Malawer, Stuart. 2010. "Cyber Warfare: Law and Policy Proposals for U.S. and Global Governance." *International Practice Section.* 58: 28-31.

Manson, George. 2011. "Cyberwar: The United States and China Prepare for the Next Generation of Conflict." *Comparative Strategy.* 30: 121-133.

Megret, Frederic. 2006. "Jus in Bello and Jus ad Bellum." *American Society of International Law.* 100: 121-123.

Meyer, Paul. 2011. "Cyber-Security through Arms Control." *Royal United States Institute Journal.* 156(2): 22-27.

Nakashima, Ellen. 2010. "Stuxnet Malware is Blueprint for Computer Attacks on U.S." *Washington Post.* 1-3.

Nakashima, Ellen. 2012. "When is a Cyber Attack an Act of War?" *Washington Post.* 1-3.

Ophardt, Jonathan. 2010. "Cyber Warfare and the Crime of Aggression: The Need for Individual Accountability on Tomorrow's Battlefield." *Duke Law and Technology Review.* 3: 1-52.

Platt, Pictor. 2012. "Still the Fire-Proof House? An Analysis of Canada's Cyber Security Strategy." *International Journal.* 155-167.

Prescott, Jody. 2012. "U.S. Cyberspace Strategy and International Humanitarian Law." *Royal United States Institute Journal.* 156(6): 32-39.

Randall, Dipert. 2010. "The Ethics of Cyberwarfare." *Journal of Military Ethics.* 9(4): 384-410.

Rid, Thomas. 2012a. "Cyber War Will Not Take Place." *Journal of Strategic Studies.* 35(1): 5-32.

Rid, Thomas. 2012b. "Think Again: Cyberwar." *Foreign Policy.* 92: 80-84.

Richardson, John. 2011. Stuxnet as Cyberwarfare: Applying the Law of War to the Virtual Battlefield. 1-37.

Rosenfield, Daniel. 2009. "Rethinking Cyber War." *Critical Review.* 21(1): 77-90.

Rustici, Ross. 2011. "Cyberweapons: Leveling the International Playing Field." *Parameters.* 32-42.

Sanger, David. 2012. "Obama Ordered Sped Up Wave of Cyber Attacks Against Iran." *The New York Times*. 1-5.

Schaap, Arie. 2009. "Cyber Warfare Operations: Development and Use Under International Law." *The Air Force Law Review.* 64: 121-173.

Schmitt, Michael. 2010. "Cyber Operations in International Law: The Use of Force, Collective Security, Self-Defence, and Armed Conflict." *National Academy of Sciences; Workshop on Deterring Cyber Attacks.* 151-178.

Schmitt, Michael *et al.* 2013. *Tallinn Manual on the International Law Applicable to Cyber Warfare.* Cambridge University Press.

Stevens, Tim. 2012. "A Cyberwar of Ideas? Deterrence and Norms in Cyberspace." *Contemporary Security Policy.* 33(1): 148-170.

Sugrue, Matt. 2010. "Virus May be Targeting Iran's Nuclear Program." *Arms Control Today.* 40(9): 7.

Swanson, Lesley. 2010. "The Era of Cyber Warfare: Applying International Humanitarian Law to the 2008 Russian-Georgian Cyber Conflict." *L.A. International & Computer Law Review.* 32: 303-333.

Talbot, Brent. 2011. "Stuxnet and After." *Journal of International Security Affairs.* 21: 69-78.

Vatis, Michael. 2006. "The Next Battlefield: The Reality of Virtual Threats." *Harvard International Review.* 28(3): 56-61.

Waxman, Matthew. 2011. “Cyber Attacks and the Use of Force: Back to the Future of Article 2(4).” *Yale Journal of International Law.* 36: 421-459.