the Heinz Journal

Policy. Research. Practice.

23 May 2016 Volume 13, Issue 1 • Summer 2016 journal.heinz.cmu.edu

Critical Examination of the Societal Impact of "Big Data"

Amit Tzur

David Collingridge argues that, "Regulators having to regulate emerging technologies face a double-bind problem: the effects of new technology cannot be easily predicted until the technology is extensively deployed. Yet once deployed they become entrenched and are then difficult to change." In light of this assertion, new game-changing technologies and their applications, generally labelled as "Big Data," have altered the way information is gathered and channelled in our society. Today, more than ever before, personal data is being gathered, aggregated, and manipulated for use by various government entities and private companies. However, discussions of the implications of Big Data often center on a utopian or dystopian future, or alternatively focus solely on privacy concerns. This article, in contrast, will take a more structured approach, focusing on selected societal impacts of Big Data in a coherent manner, by intertwining theoretical concepts with the limited empirical evidence. Specifically, this article will discuss Big Data's impact on democratic values, inequality, free will, and racial discrimination. Moreover, the article will shed light on the underlying concepts that are prevalent in these four societal issues. Despite inconclusive empirical findings and the fact that no one can fully foresee the impacts of Big Data, I argue that given its rapid adoption by private firms and governments worldwide, it should be tracked closely, lest Collingridge's warning about technology's potentially irreversible effects be ignored.

> "Regulators having to regulate emerging technologies face a double-bind problem: the effects of new technology cannot be easily predicted until the technology is extensively deployed. Yet once deployed they become entrenched and are then difficult to change.
>
> *—David Collingridge, 1980*

The introduction of new game-changing technologies and their applications, generally labelled as "Big Data", has altered the way information is gathered and channelled in our society. Today, more than ever before, personal data is being

gathered, aggregated, and manipulated for use by various government entities and private companies. These rapid changes seem to have created a new equilibrium in the markets, in which those who fail to use Big Data lose an important competitive edge.[12] The combination of bottom-up adoption of new technologies and ever-increasing capabilities driven by the unique nature of Big Data,[3] means that our society is struggling to address the current impacts of Big Data, and those that are likely to follow in the future.

When discussions regarding the implications of Big Data have arisen, they have tended to trigger general claims about Big Data, often framed within utopian or dystopian worldviews. Such discussions often make airy, inexplicit claims and place disproportionate emphasis on certain aspects of Big Data. This narrow focus of many of the discussions misses the more nuanced effects of Big Data.[4] When Big Data is examined more closely, however, the discussion often drills down to privacy issues; indeed regulatory efforts to intervene in the realm of Big Data on the whole relate to privacy concerns.[5] Moreover, issues of data protection and privacy habitually pay little attention to the cumulative effect of other aspects.[6] A different kind of literature focuses on the modifications and remedies that would solve the perceived problems that Big Data raises. In that context, an oft-repeated argument calls for greater transparency and explicability that will tackle the "one-way mirror" problem,[7] and will grant greater powers to citizens and marginalized groups.[8]

Despite the importance of privacy in our contemporary society, social scientists should not overlook the overarching societal impacts of Big Data. Such

1 Scott Peppet, "Unraveling Privacy: The Personal Prospectus and the Threat of a Full-Disclosure Future," *Norwestern Unversity Law Review* 105(2015): 1153-1156.

2 Joseph Turow, *The Daily You: How the New Advertising Industry is Defining Your Identity and Your Worth* (New Haven: Yale University Press, 2011), 65-69.

3 Peppet, "Unraveling Privacy", 1163-1164.

4 Danah Boyd and Kate Crawford, "Critical Questions for Big Data," Information Communication & Society 15, no. 5 (2011): 663-664.

5 Boyd and Crawford, "Critical Questions for Big Data," 664; Cynthia Dwork and Deirdre Mulligan, "It's Not Privacy and It's Not Fair," *Stanford Law Review* 66, no. 35 (2013). 1-10.

6 Jean-Francois Blanchette and Deborah Johnson, "Data Retention and the Panoptic Society: The Social Benefits of Forgetfulness," *The Information Society* 18 (2002): 34.

7 "One-way mirror" refers to information and power asymmetry between those who possess Big Data information and the capability to analyse it, and those who do not. The former holds vast information about the latter, while the latter is not even aware of the extent of the former's information. See Frank Pasquale, The Black Box Society: The Secret Algorithms That Control Money and Information (City: Harvard University Press, 2015), 10-11.

8 See "Event Summary: The Social, Cultural, & Ethical Dimensions of Big Data," *Data & Society Research Institute*, last modified March 17, 2014, http://www.datasociety.net/pubs/2014-0317/BigDataConferenceSummary.pdf. 1-2; Frank Pasquale, *The Black Box Society*, 10-11, 14-18.

effects might eventually hold substantive consequences for our society. Moreover, as they are often less tangible than privacy intrusions, and perhaps less immediately relevant for individuals, they do not benefit from the same exposure and urgency. For that, I will argue that social scientists should place more emphasis on the societal impacts of Big Data. This essay represents an attempt to shed light on this issue, and to present Big Data's main societal impacts: on the democratic values in society, on inequality, on free will and one's discretion to determine the course of her life, and on racial discrimination.[9]

Some critics argue that because we cannot yet establish a clear theory of immediate, tangible harm to society regarding Big Data, the discussion about its adverse societal impacts is premature. According to this line of argument, any debate is indefinite and unwarranted, since there is no immediate tangible harm to the society caused by Big Data tools, a topic I will discuss in later sections. However, I will argue that the very same characteristics of this new technology—rapid changes, uncertainty, and a variety of possible future trajectories—are precisely why this discussion is so important. That is simply because under the current circumstances, present choices will greatly affect future consequences.[10] As Big Data technologies are likely to continue to develop in the future and to have decisive influence over our society, I posit that it should be tracked closely, before, as Collingridge warns, the technology becomes too entrenched to change.

Part 1: What is Big Data, What is New about It, and What Can It Do?

We begin our discussion of Big Data and its implications with a brief explanation of what qualifies as Big Data and how it works. The term "Big Data" is very nebulous and it is often used to mean various things.[11] However, most definitions of Big Data refer to the "growing technological ability to capture, aggregate and process an ever-growing volume, velocity and variety of data."[12] This characterization captures the elusive and context-dependent nature of the term "Big Data." Big Data is therefore distinguished not by a unique technology, but rather by the new possibilities it

9 For example, see "Event Summary," 1-5, or "Big Data: Seizing Opportunities, Preserving Values" (Executive Office of the President, Washington D.C., 2014).
10 Boyd and Crawford, "Critical Questions for Big Data," 664.
11 Ibid., 663.
12 "Big Data: Seizing Opportunities, Preserving Values," 2.

enables,[13] most notably the "Three V's" — volume, variety, and velocity. The Three V's relate to, respectively, the ability to analyse near-ubiquitous data, the ability to gather and integrate data from a range of sources, both from cyberspace and the "real world,"[14] and the ability to manipulate the data automatically in real-time, in a way that immediately affects a person's options according to her previous behavior.[15] Moreover, it should be noted that Big Data is now deployed by most big firms and governments worldwide.[16] Furthermore, the use of Big Data tools will most likely continue to grow in scale, as continuous reduction of data storage costs, gradual improvement of processing power, and greater amount of sensor technologies increase the feasibility of Big Data uses.[17]

We will now briefly describe how Big Data works, in what can be conceptualized as a threefold mechanism.[18] In doing so, it is instructive to pay special attention to how Big Data generates new possibilities for its users, and how these possibilities have changed previous conceptions and social consequences. First, computerized systems gather vast amounts of information from different "touchpoints", such as website clicks, from consumers and citizens.[19] In this way, Big Data distinguishes itself from previous methods of gathering data by its ability to collect, store, and tabulate colossal amounts of data, thanks to multiple computerised touchpoints with end-users, which are supplemented by the low costs of collecting and storing data.[20] Next, Big Data systems try to find patterns in the analyzed data in order to form a profile of each person, which will enable the categorization of individuals into groups.[21] Finally, these groupings allow the data collector, in turn, to reach each customer "individually," according to tailored parameters.[22]

Hence, the gathering and manipulating of large databases usually allows

13 Ibid., 3.
14 Ibid., 50. The integration of physical objects with the cyber-world is often referred as "the internet of things"- see, for example, Neil Richards "The Dangers of Surveillance," Harvard Law Review 126(2013): 1940.
15 "Big Data: Seizing Opportunities, Preserving Values," 4-5.
16 Ibid., 1-3; Eric Siegel, *Predictive Analytics: The Power to Predict Who Will Click, Buy, Lie or Die* (Wiley, 2013), 12.
17 "Big Data: Seizing Opportunities, Preserving Values," 1-2.
18 In practice, it is usually not feasible to distinguish between the different stages. The artificial division is only meant to provide a theoretical framework to discuss the different functions of Big Data.
19 Anthony Danna and Oscar Gandy, "All That Glitters is Not Gold: Digging Beneath the Surface of Data Mining," Journal of Business Ethics 58 (2002): 374.
20 Blanchette and Johnson, "Data Retention and the Panoptic Society," 34.
21 Danna and Gandy, "All That Glitters is Not Gold," 376-378.
22 "Big Data: Seizing Opportunities, Preserving Values," 7-8; Joseph Turow, *The Daily You*, 5-12.

for social sorting and profiling,[23] which in turn gives the collector the ability to target those who should receive "special" treatment.[24] Before Big Data, social sorting and profiling were accomplished using less precise data, which often led to delivery of a generic message to large groups, identified primarily by location or known demographic variables.[25] With the advent of Big Data, however, what was previously impossible has become a reality for many organizations due to recent advances in processing and storage technologies.[26] The data-mining ability therefore enables data collectors to realize the old desire to address consumers and citizens individually.[27] Additionally, real-time analysis capabilities, coupled with the ability to design the architecture of the user's surrounding, has enabled even more precise sorting and profiling.[28]

Before we can discuss the societal impacts of Big Data, we must first describe its three primary applications. One application Big Data technologies offer is the ability to use multiple variables, gathered by constant surveillance of individuals' behaviour, and to allow differentiated access to vast services for different consumers or citizens. The increased ability to collect ever larger databases of consumer observations, and to manipulate them with greater precision, enable firms and governments to deploy individual sorting mechanisms with more efficiency, and to do so more frequently.[29]

Second, Big Data is used for making predictions about end-user behaviour, by using Predictive Analytics,[30] a "technology that learns from data to predict the future behaviour of individuals in order to drive better decisions," and tailor these decisions to each person.[31] To construct these predictions, samples of data are gathered and analyzed to search both for patterns of specific users and for typical behaviour of some groups. These patterns of behaviour are used to predict what

23 Lyon, "Surveillance as Social Sorting," 20.
24 Ibid., 20.
25 Rob Kitchin, *The Data Revolution*, 176.
26 Blanchette and Johnson, "Data Retention and the Panoptic Society," 34.
27 Danna and Gandy, "All That Glitters is Not Gold," 373.
28 "Big Data: Seizing Opportunities, Preserving Values," 4-5.
29 Stephen Graham, "Software-sorted geography," Progress in Human Geography 29, no. 5 (2005), 9-10; "Big Data: Seizing Opportunities, Preserving Values," 7-8.
30 Also referred to as "machine learning"- see Eric Siegel, *Predictive Analytics*, 11, or "actuarial methods"- "The mechanical combining of information for classification purposes, and the resultant probability figure which is an empirically determined relative frequency"- see Bernard Harcourt, *Against Prediction: Profiling, Policing and Punishing in an Actuarial Age* (Chicago: The University of Chicago Press, 2007), 16-18.
31 Eric Siegel, *Predictive Analytics*, 11-12.

users are likely to do in future situations.[32] In that sense, Predictive Analytics can be regarded as part of Big Data technology, since Big Data both gathers the large databases required to perform predictions, and forms the predictions by using high-level computing powers to conduct comprehensive analyses. Predictive Analytics are widely used, for example, by financial services companies to check credit scores of potential borrowers, regarding their probability to successfully pay back the loan,[33] and by police forces in order to predict future crime-prone locations.[34] I will further explore how Predictive Analytics is used, as well as its implications, in subsequent sections.

Big Data's third application involves price discrimination, which is accomplished by combining the ability to sort and segment individuals with the ability to make predictions regarding their willingness to consume different products,[3536] for instance by selling the same good or service to different consumers at different prices.[37] Similar methods of discrimination can be used to offer different services to individuals, according to their perceived profile and price elasticity. Personalised price discrimination is the manifestation of the long-held desire of firms and sellers to extract the maximum price from each customer, according to her willingness to pay. Despite the fact that each consumer has different characteristics, economic means, and preferences, firms usually lack the required information and capabilities to differentiate the price they offer to different consumers. However, using this application of Big Data, firms can gather individual information such as geographical location, age, working status, and hobbies.[38]

Building on this data, firms use computerised software that predicts how much the consumer would be willing to pay for the product or service, or at the

32 Ibid., 14-15.
33 Danna and Gandy, "All That Glitters is Not Gold,"374-375.
34 Eric Siegel, *Predictive Analytics*, 51-52.
35 Dwork and Mulligan (2013), para. 14.
36 Although price discrimination can be the result of various market forces, for the sake of this paper we will discuss only personalized price discrimination that stems from client-side characteristics, associated with each individual's interaction with the website. For example, price discrimination can result from members-only prices, and individualized price discrimination can result from the different servers that direct data differently. In contrast, *personalized* price discrimination, as defined above, is the relevant method for the sake of this essay, as it is mostly based on the use of Big Data. For more on this subject, see Aniko Hannak, Gary Soeller, David Lazer, Alan Mislove, and Christo Wilson, "Measuring Price Discrimination and Steering on E-Commerce Web Sites" (paper presented at 14th ACM/USENIC Internet Measurement Conference (IMC'14), 2009). 2-3.
37 See Danna and Gandy, "All That Glitters is Not Gold," 379.
38 "Facebook Using Offline Purchase History to Target Ads," RT, last modified March 27, 2013, http://rt.com/usa/offline-facebook-ads-history-900.

very least what her financial situation is, and to offer her a price accordingly. We can therefore see how Big Data supports sophisticated price discrimination.[39] Recent studies have confirmed the use of price discrimination by most major e-commerce websites.[40] For example, "guest" users might be required to pay hundreds of dollars more than users with accounts for hotel accommodation.[41] It has also been shown that search results are sensitive to parameters such as history of clicked and purchased products, and even to factors such as the platform and operating system of the user's device.[42]

From a more theoretical viewpoint, Big Data is a game-changing technology from at least four different perspectives. First is the quantity of data collected, which is exponentially greater than ever before. Second is the granularity of the data collected, which contains increased capacity to analyse great details, in order to extract business value. Third is the ability to identify cross-correlation between different sources of data, which amplify the importance of the data and provide a much clearer picture of the person behind previously unrelated digital footprints. The fourth is arguably the most important factor, and stems from the previous three aspects. It is the predictive power that is gained by deploying Big Data methods, and enables entities to "discover" information that does not yet exist. Combining these four capabilities, firms can make sense of data that would otherwise remain fragmented.[43]

However, after discussing the basic concepts and uses of Big Data, what becomes apparent is that Big Data is neither a single new technology, nor does it generate new governmental or business objectives.[44] Rather, it equips old desires with new set of possibilities, in ways that can potentially alter the social equilibrium.[45] Therefore, to argue that Big Data's prevalence yields social results that

39 Danna and Gandy, "All That Glitters is Not Gold," 379-381.
40 Aniko Hannak, Sapiezynski Piotr, Arash Molavi Kakhki, Balachander Krishnamurthy, David Lazer, Alan Mislove, and Christo Wilson, "Measuring Personalization of Web Content" (paper presented at International World Wide Web Conference Committee, 2013) 6-7; Jennifer Valentino-Devries, Jeremy Singer-Vine, and Ashkan Soltani, Websites Vary Prices, Deals Based on Users' Information, The Wall Street Journal, December 24, 2012, http://www.wsj.com/articles/SB10001424127887323777204578189391813881534.
41 Aniko Hannak et al., "Measuring Personalization of Web Content," 6-10.
42 For example, mobile users were offered lower prices, but users of the Android operating system are likely to be shown a higher price. See Aniko Hannak et al., "Measuring Personalization of Web Content," 10-13.
43 Blanchette and Johnson, "Data Retention and the Panoptic Society," 38-39.
44 Ibid., 38-39.
45 Dwork and Mulligan, "It's Not Privacy," 18.

demand further examination, it is necessary to understand why current laws and regulations are ill-suited to handle new realities brought about by the achievement of long-held desires. In other words, it will be necessary to reason why a "change of scale leads to a change of state."[46] I will discuss the extent to which these new possibilities necessitate different treatment from contemporary society in the next four sections. These effects are not meant to be exhaustive, but rather are meant to establish a unifying list of some of the most pressing societal impacts.

Before moving on to discuss the social impacts of Big Data, there are three caveats that frame the limits of this discussion. First, although Big Data usually raises complex questions regarding privacy issues, this is beyond the scope of this paper. As noted earlier, despite the influence of Big Data in a variety of areas, there are many discussions of Big Data's implications on privacy concerns.[47] At the same time, as the use of Big Data analysis is becoming more and more common, it affects the society as a whole, as well as the individuals living in it. Therefore, in this paper, I will not address privacy issues and concerns, as they are already subject to widespread public scrutiny, opting instead to discuss only the societal aspects of the use of Big Data technologies that have yet to be considered adequately.[48]

Secondly, I will not discuss the various socially-beneficial uses of Big Data, despite their obvious existence and undeniable contribution to society.[49] The new options that Big Data offers are being used by a variety of governments, businesses, and academic researchers, and encompass various beneficial implications for society and individuals[50] Some benign consequences can be regarded as beneficial for the operation of effective and competitive markets, such as better flow of information and reduced transaction costs.[51] Some Big Data functions enable better medical research or credited with greater governmental efficiency.[52] However, due to the fact that the use of Big Data is encouraged by strong market forces and is becoming ever more prevalent,[53] this paper aims to encourage a more serious debate regarding

46 Viktor Mayer-Schonberger and Kenneth Cukier, *Big Data: A Revolution that Will Transform How We Live, Work, and Think* (Boston: Mariner Books, 2014). 151.
47 Dwork and Mulligan, "It's Not Privacy," 2-3; Rob Kitchin, *The Data Revolution*, 163-174.
48 Dwork and Mulligan, "It's Not Privacy," 1-7.
49 "Big Data: Seizing Opportunities, Preserving Values," 64-65.
50 Neil Richards, "The Dangers of Surveillance," 1939.
51 Rob Kitchin, *The Data Revolution*, 72; "Big Data: Seizing Opportunities, Preserving Values," 64-65.
52 Rob Kitchin, *The Data Revolution*, 73.
53 Mayer-Schonberger and Cukier, *Big Data*, 145.

its social consequences, which would balance Big Data's growing popularity.[54] Considering and measuring the societal impacts of Big Data should therefore only be the first step toward a more sensible and reasoned debate regarding the Big Data phenomenon. Future discussions, nevertheless, should aim to weigh the costs of using Big Data in different contexts, in comparison to its benefits. Such efforts, however, fall beyond the scope of this article.

The third caveat relates to the lack of empirical evidence to support various claims about Big Data. To date, most research regarding Big Data has focused on the normative and theoretical implications of this recent technology, rather than on empirical case studies.[55] Given the relatively early point of the present data revolution, vast empirical research has recently been undertaken and has yet to be published. Moreover, it is not at all certain how this sea-change will unfold, and this casts doubt on the current feasibility of measuring Big Data's long-term implications. The lack of a sufficient body of empirical research, in addition, prevents a more informed evaluation of the social costs and benefits of Big Data. That lack of information limits the ability to establish informed policy. Nevertheless, the lack of empirical evidence should not stop researchers from examining this present data revolution.[56] On the contrary, it might emphasize the importance of developing a theoretical framework of the contested topics, in order to direct future empirical research in these areas.

For the remainder of this paper, each section will discuss a different social impact: the interplay between Big Data and democratic values, Big Data's effect on inequality, Big Data's effect on free will and the ability to determine one's future life direction, and the relationship between Big Data and racial biases. The final section will briefly discuss the theoretical approach to unique aspects of Big Data which underlie the aforementioned social impacts, namely accountability, transparency, complexity, and secrecy. I will conclude by voicing the need to examine Big Data from a social perspective, considering that such examination yields a startlingly different perception of Big Data than the common knowledge.

54 Rob Kitchin, *The Data Revolution*, 175-176.
55 Aniko Hannak et al., "Measuring Personalization of Web Content," 1; Rob Kitchin, *The Data Revolution*, 183.
56 Rob Kitchin, *The Data Revolution*, 17-18.

Part 2: Big Data, Personalized Content, and Democratic Values

In 1995, futurist Nicholas Negroponte predicted that in the future, people will be able to adjust newspapers to suit their own interests.[57] As frequently occurs with the rapid advance of technology, this prophecy seemed outdated when only twelve years later, when Cass Sunstein examined the way electronic content publishers offered readers a "do-it-yourself" mechanism to choose the content that will be displayed for them. This mechanism allowed users to filter the content that they are exposed to, and thereby narrow the scope of the internet to what appeals to them.

In 2016, even Sunstein's model of personalized content seems archaic. Take, for example, the automated content recommendation services that Outbrain[58] offers, which are now used by most online content publishers, including *BBC*, the *New York Times* and others.[5960] Outbrain collects and analyses various data regarding web users, based on elements such as previously viewed sites and search words, geographical location, time spent viewing different articles, and more, and turns this data into a user profile. Outbrain then uses these profiles to match tailored content recommendation to each user according to pre-defined parameters, in a process called "behavioural targeting."[61] Content recommendation is attractive to many content publishers, both in order to lure consumers away from other sites by presenting relevant content, according to the user's profile, and to increase existing users' engagement within the website, in order to extract higher value from advertising slots.[62] Consequently, this advertising method commonly subsidises end-users' free or discounted use of the internet.[63] The users, in turn, often willingly choose from the recommendations available to them, especially when the recommended content is similar to their previous preferences, and this will often strengthen their affiliation with the content tailored to them. Furthermore,

57 Nicholas Negronpontre, *Being Digital* (New York: Vintage Books, 1995), 153.
58 "About Us", Outbrain website, accessed July 25, 2015, http://www.outbrain.com/uk/about/company.
59 Erin Griffith, "How Taboola and Outbrain Are Battling a Bad Reputation and Each Other," Fortune Magazine, August 18 2014, 6; Joseph Turow, The Daily You, 65-69.
60 "Case Studies", Outbrain website, accessed July 25, 2015, http://www.outbrain.com/blog/2015/03/future-of-native-advertising-outbrian-at-sxsw.html.
61 Jianging Chen and Jan Stallaert, "An Economic Analysis of Online Advertising Using Behavioral Targeting," MIS Quarterly 38, no. 2 (2014): 429-431.
62 "Who Uses Outbrain", Outbrain website, accessed July 25, 2015, http://help.outbrain.com/customer/portal/articles/1447212-who-uses-outbrain-amplify.
63 Joseph Turow, *The Daily You*, 8-11.

it should be noted that the behavioural targeting process is completely automated. As Outbrain's CEO puts it, "You use a search engine to reach the content you know you look for; you use a content-discovery engine, like Outbrain, to reach content you did not even know you were looking for."[64] What he failed to mention, however, is that the user will be exposed to recommendations whether he wishes to or not.

Put differently, it is both the efficiency of the system and the lack of intentional involvement of the end-users in the filtering process that is unique to the Big Data age. First, the system of tailoring content using Big Data is becoming more and more accurate and efficient, as it accumulates data from wide sources[65] and becomes even better at individualized targeting. As individualization and segmentation is done more efficiently than ever before, it further reduces users' will to search for new content, and limits the possibility that they will be exposed to information that will challenge their views.[66] Second, the means of collecting data is becoming more and more unavoidable from the end-user perspective. As virtually all major content providers are using these methods as an intrinsic part of their business models, the consumers are left deprived of any substantial opt-out possibility, nor do they have any real alternative to acquire similar services without being exposed to the same methods.[67] Internet users are therefore inevitably exposed to content similar to that which they have previously consumed, based on Big Data profiling and segmentation. Finally, it is no longer the end-user who controls the content he sees online, but rather strong market forces that aim to best match content to the perceived profile of each user.[68] In other words, in contrast to Sunstein's view, Big Data has made the system that isolates individuals not only significantly better, but inevitable and inconspicuous.[69]

What is still relevant in Sunstein's view, and even more so today, is the fear of the segmentation and fragmentation resulting from this individualized design of the web. Sunstein argued that this increasing "personalization" of electronic

64 Yaron Galai, "Our Mission", Outbrain website, Accessed July 25, 2015, http://www.outbrain.com/about/company, Video: 0:14-0:21.

65 For example, health-related data is taken into account in credit and lending related systems.

66 "Big Data: Seizing Opportunities, Preserving Values," 8.

67 Joseph Turow, *The Daily You*, 6-14.

68 Dwork and Mulligan, "It's Not Privacy," 1-7.

69 "With television, people can limit their exposure to dissenting opinions simply by flipping a channel…and, of course, viewers are aware they're actively choosing shows. The concern with personalization algorithms is that many consumers don't understand, or may not even be aware of, the filtering methodology"- Natasha Singer, "The Trouble with the Echo Chamber Online," The New York Times, May 2011, http://www.nytimes.com/2011/05/29/technology/29stream.html?_r=0,

content will benefit the consumers in the short term, but might eventually have dire consequences for democratic society and its values. The growing ability to filter unwanted content might harm two aspects essential to free speech: exposure to unplanned and unchosen material, and the existence of a variety of common experiences within a society.[70] These are the building blocks of a pluralist, cohesive society. In contrast, in a society where one is exposed to the same material over and over again, where people mostly read and see mere echoes of their own voices, citizens are not exposed to opinions that challenge their own, and the society as a whole lacks important common ground.[71]

For example, if one web-user shows interest in conspiracy theories, it is likely that the automated content-recommendation service will offer him even more conspiracy theories, and his belief in the prevalence of such theories will increase, at the same time that his likelihood of reading contradicting opinions will be reduced. Accordingly, I argue that the growing use of personalized content, and its increasing sophistication, exposes an inherent flaw in society's pluralism, in a way that sacrifices democratic values for the sake of market power. The growing use of personalized content, mediated by Big Data technology, brings together "filter bubble"[72] groups of likeminded people and leads to a serious risk of social fragmentation, which supports polarization.[73] Under this view, predictive analytics is a self-fulfilling prophecy[74] that strengthens the previous tendencies and beliefs of different groups.[75] Such a society will have limited public deliberation and few common meeting points, both of which impose greater risk of extremism and a decline of robust free speech than what Sunstein imagined only few years ago.

How do these tendencies affect the role of major websites, and perhaps regulators' approach to these websites? Legal scholar Emily Laidlow claimed that the use of the internet is channelled through different types of gatekeepers, who enable use by choosing what content shall, or shall not, pass through their gates.[76] The gatekeepers, which can be Internet Service Providers, websites or search engines, are important due to their control over the flow, content, and accessibility

70 Cass Sunstein, *Republic.com 2.0* (Princeton, NJ: Princeton University Press, 2007), 4-6.
71 Sunstein, *Republic.com 2.0*, 6-7.
72 A term coined by Eli Pariser, The Filter Bubble: What the Internet is Hiding From You (London: Penguine Press, 2011), 1-12.
73 Sunstein, *Republic.com 2.0*, 46-57.
74 Jay Stanley, "Eight Problems with 'Big Data'," ACLU Blog, 2012. topic 5.
75 Lokke Moerel, *Big Data Protection* (Tilburg, Netherlands: Tilburg University, 2014), 42-43.
76 Emily Laidlow, "A Framework for Identifying Internet Information Gatekeepers," International Review of Law, Computer & Technology 24, no. 3 (2010). 264.

of information, even if they usually do not actively dictate the content that is shown to their users.[77] Among the gatekeepers, Laidlow distinguishded a special group of Internet Information Gatekeepers (IIGs), who as a result of their control over data, affect participation and deliberation in democratic societies.[78] IIGs, claims Laidlow, should hold "Human Rights Responsibilities" when they affect democratic deliberation, depending on their level of exposure and importance in the democratic society. As already discussed, personalization of content using Big Data capabilities has changed the model in which the previously "passive" internet gatekeepers interact with their end-users[79] more and more.[80] Consequently, it can be expected that IIGs now hold even greater social responsibilities. However, we have seen that in practice, IIGs these days tend to increase their control over the flow of data in search for greater revenues, while sometimes overlooking their social role of widening public debate and common ground.

Therefore, what is needed at this point is an examination of the extent to which personalized content is a common practice in today's cyber-world, and its overall effect. Not unlike other potential Big-Data-related research topics, this question has had only limited quantitative investigation.[81] However, one study found that on average, 11.7% of Google search results are altered due to personalization.[82] More specific searches for topics concerned with politics and news yield a higher personalised content rate,[83] which may imply that websites acknowledge the importance of tailored content even more so in news-related searches. However, some online recommendation firms argue that they intentionally incorporate a wide variety of perspectives in their recommendations.[84] Moreover, a recent paper that examined an online service for music-related recommendations found that recommendations usually lead to consumption of a greater variety of content, both due to an increased volume of consumption and to a larger mixture of interconnected, popular products.[85] Such scant empirical evidence for the existence and effect of

77 Laidlow, "A Framework for Identifying Internet Information Gatekeepers," 263.
78 Ibid., 266-267.
79 Ibid.,264-266.
80 Sunstein, *Republic.com 2.0*, 3-6; Joseph Turow, *The Daily You*, 1.
81 Aniko Hannak et al., "Measuring Personalization of Web Content," 1, 10; Kartik Hosanagar et al., "Will the Global Village Fracture into Tribes?" 4-5.
82 Aniko Hannak et al., "Measuring Personalization of Web Content," 1.
83 Ibid., 4-5, 9-10.
84 That is, for example, Google's claim in regard to Pariser's book and his "filter bubble" argument. See Singer, Natasha, "The Trouble with the Echo Chamber Online," last accessed May 10, 2015, http://www.nytimes.com/2011/05/29/technology/29stream.html.
85 Kartik Hosanagar et al., "Will the Global Village Fracture into Tribes?" 29-30.

content personalization suggests that it does not yet hold any chief prevalence in the cyber-sphere, and its effect over social fragmentation is still in its infancy.

In conjunction with the fact that the internet[86] is only one platform of content among many, it is likely that the effect of personalization is very limited in practice. However, we should remember that there are certain ethical, social, technical, and legal limitations that hamper the quantification of Big Data drawbacks. For example, privacy laws limit the ability of researchers to collect data, and technical difficulties in identifying and quantifying harms reduce the feasibility of measuring concrete impacts.[87] Therefore, we can assume that current empirical findings underrepresent Big Data's societal impacts.[88] Moreover, the increasing use of personalization by websites[89] and the use of the internet as a major source of information, suggests that the adverse effects of the "filter bubble" should not be offhandedly rejected. Furthermore, it should be watched closely not only by society and regulators, but also by IIGs, who have ever-increasing social roles and responsibilities.

Part 3: Big Data and Inequality:

> "Individuals viewed through statistics no longer need to be classified as either 'in' or 'out' of the market. Armed with a gradated sliding scale, people all along a spectrum of risk can be offered specially designed products at alternative terms and prices.
>
> *—Poon, Martha (2008), From New Deal Institutions to Capital Markets*

Information allocation techniques, such as data profiling and sorting, can be perceived as invitations. Businesses use profiling and sorting to withhold certain information from customers in an attempt to disinvite them from certain promotions or practices, forcing them to "leave quietly". This mechanism of red-lining, or "weblining", ensures that such individuals will never be invited

86 The internet is one of several platforms that can be personalized, in contrast to mass-media means of communication, such as television and newspapers.

87 Solon Barocas, Danah Bodyd, and Pena Gandadharan Seeta, "Re:Project No. P145406, Big Data: A Tool for Inclusion or Exclusion?" Open Tehnology Institute, August 15, 2014, https://www.ftc.gov/system/files/documents/public_comments/2014/08/00023-92391.pdf. 1-2.

88 Barocas et al., "Re:Project No. P145406," 1-3.

89 Aniko Hannak et al., "Measuring Personalization of Web Content," 1-2.

to certain activities, and thus their options will be limited.[90] People in turn will choose from the options available to them, and will strengthen their place within socio-economic groups. Predictive analysis is thus a self-fulfilling prophecy[91], which tends to strengthen previous tendencies of different groups.[92] The software and code within computerised systems, therefore, is an important element that determines the inclusion, or otherwise exclusion, to many social domains.[93] These computerised systems are increasingly orchestrated using consumerist criteria, which favours privileged users over those deemed unprofitable, risky or deviant.[94]

The sophisticated capabilities of Big Data give rise to increasing prevalence of social sorting and amplify existing inequality. Interestingly, it is exactly the democratization of markets and the minimal scope for discretion, enabled by Big Data, which draws new distinction between individuals and thus further widens social gaps. Big Data thrives on the economic rationales, measure people individually, and then separate and recombine them according to businesses' profit-maximizing purposes.[95] This section focuses on aspects of social sorting and the advantages it yields to those "better-off", among them are fortunate individuals, larger firms and tech-savvy governments. Following general explanations, we will explore examples for these societal processes.

The complexity of Big Data strengthens existing inequality among individuals in several ways. For example, well-off individuals and social groups are in better position to engage with Big Data than marginalized individuals and communities. Marginalized groups often lack the required resources to manipulate Big Data to their own benefit, thus deepening to existing inequality.[96] This disparity is worsened by the fact that many of the marginalised population are often closely monitored and lack awareness of the extent of such surveillance and its implications.[97] Furthermore, gaps in access to information are troublesome as it may limit certain consumers'

90 Danna and Gandy, "All That Glitters is Not Gold," 379, 381.
91 Stanley, "Eight Problems with 'Big Data'," topic 5.
92 Moerel, *Big Data Protection*, 42-43.
93 Graham, "Software-sorted geography," 10.
94 Ibid., 8-9.
95 Marion Fourcade and Kieran Healy, "Classification situations: Life-chances in the neoliberal era," Accounting, Organization and Society 38 (2013): 560.
96 Graham, "Software-sorted geography," 24-25.
97 "Workshop Primer: Inequalities and Asymmetries," Data & Society Research Institute, last modified March 17, 2014, http://www.datasociety.net/pubs/2014-0317/InequalitiesAsymmetriesPrimer.pdf. 1-3; Fourcade and Healy, "Classification situations," 560-563; Joseph Jerome, "Buying and Selling Data: Big Data's Different Burdens and Benefits," Stanford Law Review Online (2013). part 3.

ability to make informed choices or to participate effectively in a marketplace.[98] Finally, people in vulnerable positions, such as prisoners or recipients of national security benefits, are often compelled to share data by different institutions, and have no real "opt-out" option due to their disadvantageous position.[99]

The tendency to "favour the favoured", or to allocate discounts or subsidies to the better-off customers, is common practice for businesses today, as Poon's above quote suggests.[100] This tendency is common in the credit scoring and other "classificatory" industries, for purposes of loans, mortgages, health-care, insurance or others.[101] On the supply side, providers of such services adopted the use of Big Data to systematically assess individuals and segment them according to desired fine-grained criteria such as employment, real-estate and even dating history.[102] On the demand side, greater personalization of different services and products, positions individuals in different segments which are consequential for one's life-chances.[103] A person with better credit-scoring "profile" will be offered lower interest rates, competitive insurance prices and more comprehensive health-care, than an individual who took previous loans, was involved in previous car accident, and so on. The sorting ability enables lending companies, for instance, to reach high-risk segments of the market and to gain considerable profits by offering low-income individuals short-term loans with extremely high interest rate. Consequently, pay-day loans based on Big Data credit-scoring rose by an order of magnitude in recent years, but they offer such high interest rates that they trap the recipients into cycle of rising debts and higher risk of bankruptcy.[104] Well-off consumers are also better situated to manage their own credit score, in order to keep their premium fee as low as possible. For example, according to the US National Financial Capability Study, 56% of those who earn more than $75,000-a-year obtained a credit report[105], three times more than the population who earn below $25,000.[106] In turn, the new

98 Danna and Gandy, "All That Glitters is Not Gold," 381-382.
99 "Workshop Primer," 3-4.
100 Edwin Baker, "Advertising and a Democratic Press," University of Pennsylvania Law Review 140 (1992): 2162-2164.
101 "Big Data: A Tool for Inclusion or Exclusion," Federal Trade Commission, last modified September 15, 2014, https://www.ftc.gov/system/files/documents/public_events/313371/bigdata-transcript-9_15_14.pdf. 8-10.
102 Fourcade and Healy, "Classification situations," 561-562, 569; Blanchette and Johnson, "Data Retention and the Panoptic Society," 37-38.
103 Fourcade and Healy, "Classification situations," 560.
104 Ibid., 566-567.
105 "Credit report" is a report that is used for improving one's credit score.
106 Ibid., 565.

credit-scoring features increase the existing inequality in the markets, as businesses utilise scoring tools that never existed previously.

Additional preferential services are offered to well-off individuals. One recorded example is a tactic deployed by the Royal Bank of Canada used a consumer-analytic approach to target its preferred customers.[107] Individuals that were identified as high-value customers were 'nudged' to advantageous flat-fee packages. These same packages were not offered to the remaining less-profitable consumers in what can be conceived as a "fire the customer tactic", a strategy often deployed on low-value customers. Differentiation of services is also apparent in call centers.[108] Call centers collect and use information regarding their callers based on their telephone number. This information often includes various economic, demographic and social factors from which the centers determine a real time "value judgment" of the caller. Customers are then ranked according to their perceived value. Ranking systems are used to prioritise certain customers and to offer them special services, such as shorter queuing time and favorable service from customer service employees.[109]

Big Data not only supports functions that increase inequality among individuals, but also denies equal access among different entities. Certain companies and governments hold vast amount of data and can choose whether and how to allow or prohibit access to this data.[110] In turn, control of this information supports their inherent advantage that led them to get hold of the data. However, the inequality of Big Data refers not only to better accessibility of more "successful" entities, but also to their better skills and means, as Big Data requires sophisticated capabilities and tools to make sense of the data. Such abilities are not only hard to acquire, but they also tend to strengthen by easy access to large data, in a way to widen the gap between those with access, and those deprived from access.[111] As the importance of Big Data rises in the business and political world alike, it is probable that the 'insiders' of the Big Data world will have clear advantage over the 'outsiders', in a way that is likely to increase social gaps.[112]

Similarly, there are increased concerns regarding the use of Big Data

107 Danna and Gandy, "All That Glitters is Not Gold," 381.
108 Graham, "Software-sorted geography," 18-19.
109 Ibid., 19.
110 Boyd and Crawford, "Critical Questions for Big Data," 673-674.
111 Ibid., 674.
112 Ibid., 674-675.

by governments as a tool to widen the gaps between those who are favoured by governments and those who are not. Certain government entities, including homeland security agencies, attempt to limit the availability and ease of access to information for some the populations.[113] Such agencies have deprived access to information from certain ethnic or other groups, based on characterization of users.[114] Furthermore, governments' usage of Big Data might be limited to tackling the consequences of the problems, and not with the root causes, partially as the former is easier to measure by Big Data.[115] For example, smart city technologies are used to predict future crime areas and to automatically send police-forces to minimize this specific type of risk. However, it will not solve the root-causes of crimes and its relation to poverty.[116]

Finally, scholars claim that Big Data supports seemingly technocratic governance, that de-facto will serve a neo-liberal political economy.[117] The use of code-based infrastructure, and Big Data especially, is not only incomprehensible to most users, but also unrecognizable, to most users.[118] The lack of transparency in the use of Big Data [119] is due to the important role of the code, which is usually developed by corporates and large hardware companies.[120] The role of codes can be used to shift the control from governments to large corporations. For example, many cities deploy police forces to specific locations through an automatic algorithm without public scrutiny or conscious discussion of its wider implications.[121] The power-shifting mechanism can be reasoned by rational justifications of greater efficiency.[122] In practice, however, the mechanism first shifts responsibilities from governments to private bodies, and then produces dependency of governments and public services in these service-providers.[123] Many scholars claim that in order for regulation and democratic scrutiny to be feasible and effective, the configuration and implications of the software-sorting process should be noted and explained clearly.[124] In other words, they claim that without explicability, there can be no

113 Danna and Gandy, "All That Glitters is Not Gold," 383.
114 Ibid., 383-384.
115 "Workshop Primer," 6-8.
116 Rob Kitchin, *The Data Revolution*, 179-181.
117 Ibid., 180-182.
118 Graham, "Software-sorted geography," 10.
119 Rob Kitchin, *The Data Revolution*, 180.
120 Ibid.
121 Eric Siegel, *Predictive Analytics*, 51-52.
122 Rob Kitchin, *The Data Revolution*, 181-182.
123 Ibid., 179-182.
124 Lucas Introna and David Wood, "Picturing algorithmic surveillance: The politics of facial

effective regulation of Big Data and other technological means. However, since there is little to no internal motive to expose the way the software is coded, and in any case such explanation is highly-complex to convey, it does not seem to be the case that transparency is feasible without any external intervention. This seems to be, thus, a paradox, that will leave Big Data's lack of transparency intact.[125] Ultimately, that outcome serves neo-liberal forces that increase the inequality within modern societies.

Part 4: Big Data and Free Will:

> By mandate of the District of Columbia Precrime Division, I am placing you under arrest for the future murder of Sarah Marks.
>
> —*Tom Cruise, from the movie* Minority Report

The idea of "starting over" is crucial to many societies for psychological, social and moral reasons, and inherently involves the elimination of forgetting the past and forging a new future.[126] For example, the importance of removal of previous juvenile court history is important and statute in many jurisdictions, in order to permit full rehabilitation and to assure social mobility.[127] This is not only due to the individual's right to full accomplishment of their lives, but also due to the importance of providing opportunities to "transform" individuals into normative citizens, and thus to benefit the society.[128]

However, there is an inherent tension between individuals' right to change the course of their lives, and the will of companies' and governments' to evaluate and predict future behaviour based on previous characteristics, in order to extract competitive advantage.[129] The gathering and storage of vast resources of data, combined with the ability to integrate several distant resources to one database, enables new possibilities for evaluation and remembrance of data. For example,

recognition systems," *Surveillance and Society* 2 (2004): 195-196

125 Graham, "Software-sorted geography," 28-30.

126 Gary Marx, *Undercover: Police Surveillance in America* (Berkeley: University of California, 1988), 222-223; Blanchette and Johnson, "Data Retention and the Panoptic Society," 34-36.

127 Blanchette and Johnson, "Data Retention and the Panoptic Society," 37.

128 Ibid.

129 Ibid., 35; Mayer-Schonberger and Cukier, *Big Data*, 151.

a minor criminal record can be a decisive factor in setting the proposed interest rate by loan-firms, even long after the person has adopted normative behaviour. Therefore, in light of the growing use of Big Data to offer different opportunities to individuals, past behaviour in various contexts poses increasing significance to future possibilities. Big Data's increased capabilities, therefore, might have dire social consequences in regards to the ability to change the course of one's life, as it hampers individuals' range of choices and opportunities.[130] Even when firms are pursuing legitimate, rational business endeavors, certain social costs are imposed on the society when data mining activities are performed.[131]

Predictions such as these, however, reverse the usual order of judgment, as we judge an individual according to his predicted act before it had ever occurred.[132] Such prejudices not only undermine the assumption of innocence, but limit the ability of the individuals to change their life course. This concept, based on the growing use of Big Data to make predictions, contradicts western legal-systems, as well as our basic moral conception.[133] It should be stressed, however, that Big Data does not reveal much about causality, but rather offers merely statistical correlation. Therefore, it is an ill-suited tool to assign culpability based on statistical findings.[134] Additionally, complete data simply provides an historical snap-shot of a person and does not take into account that humans can change their behaviours in an unpredictable way.[135]

However, it is not at all certain that tech-savvy entities allow individuals the required leeway to change their future behaviour. For example, judges and parole boards in the State of Oregon use a predictive model that evaluates prisoners' likelihood of recidivism before deciding about a prisoner's incarceration or release from jail. These types of predictive models operate under the assumption that past actions are a good indication of future behaviour.[136] Oregon's predictive model is based on 350,000 offender records, and has successfully reduced the probabilities of reoccurred felonies by current prisoners.[137] This tool only serves as a recommendation, or as a supplemental element, by the hands of authorised

130 Dwork and Mulligan, "It's Not Privacy," 10.
131 Danna and Gandy, "All That Glitters Is Not Gold," 379.
132 Mayer-Schonberger and Cukier, *Big Data*, 160-162.
133 Ibid., 162.
134 Ibid., 163.
135 Danna and Gandy, "All That Glitters is Not Gold," 379.
136 lanchette and Johnson, "Data Retention and the Panoptic Society," 38.
137 Eric Siegel, *Predictive Analytics*, 59-60.

personals. However, it draws its authority from wide database and empirical evidences, which contributes to the high credibility of the system.[138] Under such circumstances, the possibility of a false positive conviction is a frightening one.[139][140] This kind of judgement is in contrast to our basic conceptions of justice, because when future probabilities determine current consequences, people are deprived of the opportunity to change the course of their lives.[141] The opportunity to exploit Big Data's capabilities in order to make predictions and to act accordingly in a determinist way, will limit the available options of the individual, and thus the very idea of justice can be undermined.[142]

Part 5: Big Data and Equality Before the Law

An important component of modern democracy is the alleged equality before the law.[143] Clearly, this principle is not fully practiced in reality, especially when encountering human law-enforcers, or judges, that carry their biases into their workplaces, as many studies show.[144] To investigate and uncover these hidden human biases, the legal system and democratic society have developed certain mechanisms and procedures to scrutinise the behaviour of law-enforcement officers.[145] However, technology is readily assumed to be a neutral and value-free mechanism, when in fact, the code that operates it is both dependent upon its human programmers and imbedded into a socio-technical network that may have been shaped by human biases. Therefore, it is highly likely that racial, gender or social biases will be implicitly reflected in the coded sorting systems.[146] These concerns are worsened by the underrepresentation of minority groups in the high-tech community- for example, only 2 percent of Google employees are African-Americans.[147] Nevertheless, we tend not to question the validity and impartiality of automated machines with the same level of scrutiny as we do with human agents.[148] Furthermore, even as doubts do arise regarding the impartiality of certain

138 Ibid., 60-62.
139 Ibid., 59-61.
140 Mayer-Schonberger and Cukier, *Big Data*, 175-176.
141 Eric Siegel, *Predictive Analytics*, 61.
142 Mayer-Schonberger and Cukier, *Big Data*, 176.
143 Introna and Wood, "Picturing algorithmic surveillance," 195.
144 Ibid.
145 Ibid.
146 Graham, "Software-sorted geography," 29.
147 Frank Pasquale, *The Black Box Society*, 39-40.
148 Introna and Wood, "Picturing algorithmic surveillance," 195.

computerized systems, it is often unfeasible to unpack and trace the causes for such forms of discrimination, since computerized results depend on complex algorithms consisting of multiple variables and decision processes.[149]

Big Data's abilities can also be used in "digitally redlining" and categorizing unwanted groups using sophisticated and almost-untraceable means, in order to offer them customized service options that are different from those offered to more attractive groups.[150] This may affect people's accessibility and quality of services in crucial sectors such as health, education, employment and credit.[151]

Nonetheless, the biases and discrimination are not necessarily products of deliberate intention. One cause for such discrimination could be implicit bias in the existing database, which Big Data is drawn from and built upon. For example, if police forces focus their efforts on minority communities, Big Data analysis can consequently imply that the crime rates among these communities are higher, further reinforcing previous racial biases.[152] However, it is unlikely that such existing biases can be easily recognized due to the complexity of Big Data systems.

Discrimination can take even more subtle forms. A research that examined ethnic-related biases of search results in Google found that searching racially-associated names yielded different results, which consequently triggers unproportioned targeting of minorities by certain on-line services such as InstantCheckmate.com.[153] The research observed that names associated with African-Americans individuals are 25% more likely to receive search-results that include suggestions of an arrest record.[154] Not surprisingly, Google and InstantCheckmate.com have denied the existence of any racial elements in their codes.[155] However, other elements that can be directly correlated to ethnical-background, such as geographical location, might affect Google search results, in a way that will further reinforce racial discrimination with no explicit intentions.

On the other hand, some scholars argue the contrary and praise the plausible positive effects that Big Data functions might play in reducing discrimination and racial biases enforcement. Traditional law-making and enforcing processes, it is

149 "Big Data: Seizing Opportunities, Preserving Values," 7-8.
150 Ibid., 52-53.
151 Ibid., 64-65.
152 Frank Pasquale, *The Black Box Society*, 38-42.
153 A website that offers "quality background checks", which include criminal records and other personal details.
154 Latanya Sweeney, *Discrimination in Online Ad Delivery* (Cambridge: Harvard University Press, 2013), 20-23.
155 Frank Pasquale, The Black Box Society, 38-39.

argued, are inherently discretionary, and monitoring and enforcement inevitably result-in the disproportionate targeting of already marginalised groups.[156] In contrast, technology-based enforcement that rely on Big Data methods can possibly overlook factors such as race, sex, appearance and others, which are used to profile individuals and to segment groups. In that manner, such systems might be programmed to base their judgement solely on factors that are directly-related to the topic in question, and not on proxy factors such as race.[157] However, this argument assumes at least two premises: first, that the system is programmed to judge according to relevant factors only; second, that everyone is equally subjected to the same surveillance regime, which demands a universal database. It is unlikely that these two premises will hold true in reality for various reasons.[158] For example, the first street-based facial recognition system operated in Britain was installed in one of the poorest constituencies in the country for the purpose of tracking down offenders.[159] Indeed, in that case, the bias was not caused by the application of the automated system, but rather by its deployment by human policy-makers. In any case, it is plausible to argue that further empirical research is needed in the context of Big Data and discrimination, similarly to many of the abovementioned topics.

Part 6: Underlying Elements, Discussion and Conclusion

Looking through a more theoretical lens, we can see that a few elements prevailed in the background of most of the topics discussed above. These elements, which will be further elaborated below, characterize the use, abilities or implications of Big Data and are common constituents in the literature on Big Data. This list contains the elements of accountability, transparency and explicability, complexity and secrecy. Thus, I will now turn to briefly examine them and their relations to Big Data and to the above societal impacts.

The first element is the clear distortion in *accountability*, which occurs when meaningful societal processes are based on computerized algorithms that are behind the control or understanding of most of the lay public.[160] The blurred lines of accountability are clearly shown, for example, in the case of Google's ethnically-

156 Claive Norris, "From Personal to Digital: CCTV, The Panopticon, and the Technological Mediation of Suspicion and Social Control," in *Surveillance as Social Sorting: Privacy, Risk, and Digital Discrimination*, ed. David Lyon (London: Routledge, 2002), 276.
157 Norris, "From Personal to Digital," 276-277.
158 Ibid.
159 Ibid., 277.
160 Eric Siegel, *Predictive Analytics*, 61.

biased results. It is not at all certain who should be held accountable- Google as the corporate entity, the programmers, or simply the cultural settings. Similarly, it is not clear to whom they should be accountable to, and how they should be held accountable.

Closely related is the issue of *transparency* and *explicability.*[161] A common argument in that context is that Big Data should never become a "black box" that offers no explicability, transparency and traceability, in order to ensure that our society as a whole will be able to play a more central role in shaping Big Data progress.[162] Another important element is the complexity of Big Data, which is related to the rapid changes of Big Data. The multi-dimensional and complex nature of Big Data makes it difficult to give it a unified definition, resulting in a conceptual confusion among popular and academic debates.

Furthermore, the complexity of Big Data systems places constraints on transparency and accountability in Big Data applications and also reduces the capacity to empirically examine Big Data and its influences. Last is the element of algorithmic and databases *secrecy*, whether deployed by the hands of government and security forces, or by private firms who wish to retain their possession over secret algorithms.[163] Again, the element of secrecy is clearly shown in the aforementioned Google case, when accusation of racially-biased search results can only be examined by the targets of these claims. Consequently, the chief extent of the secrecy element strengthens the lack of transparency and accountability, as it prevents researchers from collecting data about the operation of Big Data systems. Similarly, it shackles the ability to obtain empirical data regarding the impact of Big Data.[164]

Furthermore, what is clear after this discussion is that market efficiency and private actors' desires appear to be in clash with socially-valued norms and values. We have seen that the great progress in Big Data applications might yield adverse effects on socially-desired values such as equality and pluralism. Consequently, the questions and doubts that the common uses of Big Data trigger should not be limited to privacy issues but rather expand to encompass societal concerns. Specifically,

161 Mayer-Schonberger and Cukier, *Big Data*, 176-179. For a more comprehensive discussion about transparency in the age of Big Data, see Frank Pasquale, *The Black Box Society*, 176.
162 Mayer-Schonberger and Cukier, *Big Data*, 178-179; Frank Pasquale, *The Black Box Society*, 9-14.
163 Frank Pasquale, *The Black Box Society*, 39.
164 Barocas et al., "Re:Project No. P145406," 1-2.

we should consider how to best manage the risks imposed onto the social values at stake, and how to strike the balance between private-actors' freedom versus acceptable social equilibrium.[165]

To conclude, this essay does not mean to suggest that Big Data will inevitably harm democracy, nor that it will have adverse effect on equality, the existence of free-will or on racial discrimination. Alternatively, its purpose is to highlight urgent societal topics, which are sensitive and most vulnerable to recent technological change. A coherent framework of discussion regarding the possible adverse societal effects of Big Data is absent, and this essay reckoned to strengthen novel efforts to encompass such discussion. Furthermore, I aspired to suggest direction for future research, and to emphasise the importance of such empirical research.

That is not to say that such research can be easily done, given the aforementioned constraints, or that any change in the progress of Big Data is certainly needed or desired. However, I did try to emphasize that the course of the cyber-content market should be tracked closely, in order to tackle the narrowing of the public sphere and the greater isolation of individuals, the growing segmentation and inequality, the limiting of one's ability to change the course of his life, and the extent of racial discrimination. That is important, as suggested by the Collingridge dilemma mentioned at the beginning of our discussion, because once technology yields considerable affects over our society, it is often irreversible after the technology has become entrenched in our society.

165 Dwork and Mulligan, "It's Not Privacy," 13.

Pre-Accession vs. Post-Accession – EU Impact on Democratization in Poland and Hungary

Kyra Bachmakova

This paper seeks to determine whether potential membership in the European Union (EU) has an impact on the democratization of a potential member state. Poland, as a current role model for democratic development in the EU, is contrasted with Hungary, a country that is experiencing a democratic backslide. After a literature review of the impact of EU accession on a new member state, a case study of Hungary and Poland follows. This case study begins with an overview of the democratic history of the two countries, continues with an analysis of their pre-accession periods and an evaluation of public opinion about accession in both countries, and presents and evaluates their democratic situation between 2003 and 2014. In a further section, I examine whether membership in the EU would have (had) the means to put an end to the deteriorating democratic situation in Hungary.

Introduction

There is no consensus amongst political scientists on whether EU accession has a positive impact on democratization. Due to the requirement that the Copenhagen Criteria be fulfilled if a country is to join the EU, some scholars argue that potential membership in the EU does positively influence democracy in that potential member state. [1]

The case of Hungary, however, does not seem fit this line of argument. While Hungary was a role model for transition towards democracy during its pre-accession period, the country has shown a significant decline in democratic standards over the past years. By contrast, the fundaments of democracy in Poland have improved

1 Kaiser, Therese Avila. "Carrots and Sticks? Democratic Quality in Post-Communist Europe after Accession to the European Union." *European Consortium for Political Research*, 2012. http://www.ecpr.eu/Filestore/PaperProposal/087caf66-6599-48a0-b677-c6e935e8a1ef.pdf.

considerably since it ascended into the EU in 2004.

Based on this divergence, this study seeks to answer the question of whether affiliation with and accession into the EU impacts democratization in a new or potential member state, in both the pre-accession and post-accession periods. In the final section, I look at potential instruments the EU could use to increase its influence on the democratic standards in a member state in a positive way.

EU Impact on Democracy

There are several explanations for why countries like Poland and Hungary experienced a relatively smooth transition from communist autocracies to liberal democracies within a decade after the fall of the Soviet Union. First, their political systems were relatively developed and stable by the time the Soviet Union dissolved, which meant that the pro-democracy forces within both countries benefited from a greater deal of freedom and liberty than was the case elsewhere. This allowed for a more fluid economic transition away from communism, and as both countries opened to trade, economic growth flourished. Second, both Poland and Hungary have in common that even during times of communism, there existed active oppositional forces. This oppositional pressure forced communist leaders to adopt more pragmatic ways to shape the policies of the country, and allowed for the relatively smooth transition detailed in the first argument. Third, they typically began to establish relationships with Western countries during their last years of communism, and were therefore beneficiaries of Western foreign aid, allowing them the opportunity to acquire Western expertise and skills. After the collapse of the USSR, then, key figures in the new governments of the respective countries were able to shape the transitional path of their countries by applying that knowledge. This was only possible as the citizens of these countries voted

the communist parties out of office in their first democratic elections, in favor of parties who sought to modernize and democratize the states.[2]

The impact of EU accession on democratization in a potential member state is difficult to measure. While Kaldor & Wilke (1997) use an approach based on six levels of impact to analyze the development of democracy[3], Kubicek (2003) suggests a framework of four categories to think about the impact of international actors on the spread of democracy within a country.[4] These categories are control, contagion, convergence, and conditionality. According to his view, the EU exercises control, at least to a certain degree, over its member states, and thereby facilitates democratization. He notes, however, that in order to become a member, the EU requires that the accession candidate fulfill each of the Copenhagen Criteria. This entails that member states are already democracies when they join the EU, and therefore, that the democratic process in a member state does not begin at the time of its accession. His second category, democratic contagion, refers to events that, as they appear desirable, spill over into neighboring countries. This was the case with the EU and Central and Eastern European Countries (CEEC) after the collapse of the Soviet Union. Kubicek argues that the contagion theory does not explain the underlying causality of this effect, but only focuses on specific correlations without addressing the root of the problem: neither local conditions and national differences, nor the actors involved, are taken into account. Moreover, it makes assumptions that prove to be wrong — for example, that the EU has a mainly passive role and does not take action with regard to democracy. This is why Kubicek suggests a

2 Ekiert, Grzegorz. "149. Why Some Succeed and Others Fail: Eight Years of Transition In Eastern Europe." Wilson Center. July 07, 2011. http://www.wilsoncenter.org/publication/149-why-some-succeed-and-others-fail-eight-years-transition-eastern-europe.

3 Kaldor, Mary, and Peter Wilke. "Final Report - Evaluation of the PHARE and TACIS Democracy Programme." 1997. http://ec.europa.eu/europeaid/how/evaluation/evaluation_reports/reports/cards/951432_en.pdf.

4 Kubicek, Paul J. *The European Union and Democratization*. London: Routledge, 2003.

third idea – convergence – that advances the concept of contagion by explaining the causes of the change towards democracy. He distinguishes between two forms of convergence: the first one is convergence through a rational calculation of domestic elites; the second is constructivist and argues that convergence is the result of a socialization process within the country. Both of these ideas can be applied in the case of the European Union: first, the EU supported regimes in transition and second, particularly through NGOs, fostered the idea of democracy within the non-member states (CEECs). A final concept, conditionality, includes a "carrots" and "sticks" policy that is used to facilitate democracy in another state. This policy rewards countries that fulfill certain criteria or programs, with the Copenhagen Criteria being an example of such a policy.

Schimmelfennig & Sedelmeier (2004) employ the concept of conditionality in their paper on EU rule transfer as well. They find that the external incentives model is best suited to explain EU rule transfer that works as follows: the EU, with superior bargaining power, can dictate the rules in the accession process and incentivize CEECs to comply with them by offering rewards in form of financial assistance, agreements, and eventually full membership. This conditionality seeks to convince potential member states to adopt certain rules and behaviors, but does not actively punish them for non-compliance. The chances of a positive outcome increase with the clarity and formality of rules (determinacy of conditions), the size and speed of rewards, and the credibility of conditional threats and promises.[5] In addition, two other conditions must be met to allow for a successful EU rule transfer: democratic conditionality and acquis conditionality. In order for external governance to be effective, the potential member states must already show a certain

5 Schimmelfennig, Frank, and Ulrich Sedelmeier. "Governance by Conditionality: EU Rule Transfer to the Candidate Countries of Central and Eastern Europe." *Journal of European Public Policy* 11, no. 4 (2004): 661-79. doi:10.1080/1350176042000248089.

level of democratization and have been – credibly – promised potential membership with the adoption of the EU acquis as the basic condition.

In 2007, Schimmelfennig and Scholtz published a paper on EU democracy promotion in which they try to generalize Schimmelfennig's and Sedelmeier's findings from 2004. The authors present three mechanisms of democratization: conditionality, modernization, and linkage. The results of their analysis confirm the earlier assumption that a credible membership outlook offer is required if the EU wants to impact the democratization of a potential member state. In addition, modernization theory —which states that democracy is dependent on the level of social and economic development in a country — proved to be another important factor, while linkage in this study could not explain the enhancement of democracy.[6]

Raik's argument is that the EU pre-accession phase is highly undemocratic, and therefore is itself a paradox. Ideals such as inevitability, speed, efficiency, and expertise are used in the official discourse to describe the accession process. Raik points out that this automatically results in a power construct among elites, leaving no time for public debate. A democratic mandate is imposed by the EU as efficiently and quickly as possible in order to prevent the "window of opportunity" from closing before accession has been realized. Although the European integration necessarily became a driving factor for reforms, the quality of the democratic system remains questionable, as expectations were too high and enforced in only a short period of time.[7]

In general, there is no EU democratization model that would be universally

6 Schimmelfennig, Frank, and Hanno Scholtz. "EU Democracy Promotion in the European Neighbourhood: Political Conditionality, Economic Development and Transnational Exchange." *European Union Politics* 9, no. 2 (2008): 187-215. doi:10.1177/1465116508089085.

7 Raik, Kristi. "EU Accession of Central and Eastern European Countries: Democracy and Integration as Conflicting Logics." *East European Politics and Societies* 18, no. 4 (2004): 567-94. doi:10.1177/0888325404269719.

applicable to all post-Soviet countries. Mitropolitski (2009) suggests that we distinguish between four main groups which influence the level of democratization in a country: first, its social, cultural, political, and economic heritage; second, the institutional choices after the end of communism; third, the importance of political ideology among the elite in power; and fourth, external factors, in particular the impact of European integration on the democratization process.[8] This leads back to the original question of what the impact of European integration on democratization in a country actually is. As Mitropolitski proposes, the democratization of a country is not primarily dependent on external influences, but on domestic development and circumstances. For this reason, I start by analyzing both Hungary and Poland with respect to their history, combining the first of his three categories.

First, I look at the democratic histories of Hungary and Poland before 1989, in order to answer the question of whether the two nations had a chance to make their first steps towards democracy before they finally opened up after the collapse of the Soviet Union. An analysis of each nation's accession process follows. This section provides insight into the transition period and how the EU supported the countries' democratic and economic development prior to becoming a member state. Third, I consider public opinion on EU accession in Hungary and Poland in the pre-accession period compared to the post-accession period. By doing so, I examine how EU integration has affected people in both countries. Their responses are an indication of the success or failure of integration, including the democratization efforts on the part of the EU. The fourth section concerns how one can measure democracy, and how this interpreted level of democracy in Hungary and Poland has changed over recent years. To explain these developments, I address domestic political

8 Mitropolitski, Simeon. *The European Integration and the Democratization in Eastern Europe*. Ottowa, 2009.

circumstances since EU accession in both countries with a focus on the politically problematic Hungary. In a fifth section, I try to answer the central question of whether it would have been possible for the EU to prevent democratic backsliding in member countries, particularly in Hungary. I then come to the final conclusion that the democratization process during the pre-accession period is accelerated by the political efforts within the candidate country. After accession has successfully taken place, however, democratization slows down, as the goal of becoming a EU member state has been reached: thus, there is a lack of incentive and punishment to make post-Soviet countries continue to work on democratization.

Historical Democratic Development

Democratic History of Hungary Before 1989

Between 1867 and 1919, Hungary was part of the Austro-Hungarian Empire under the Habsburg monarchy. In the Compromise of 1867, Hungary obtained a status equal to Austria's within the empire, that of a constitutional monarchy. Although suffrage was limited, the foundation for Hungarian parliamentarianism was laid. When Austria was defeated in WWI, Hungary lost major parts of its territory as it broke away from the empire. After the Aster Revolution had led to the formation of a democratic coalition government on November 16, 1918, the Hungarian People's Republic was proclaimed by Mihály Károlyi. On January 11, 1919, Károlyi was appointed head of state, but was forced to abdicate only two months later when the triple entente claimed further Hungarian territory. After a short period of interruption when Hungary became a Soviet republic under Belá Kun, the Hungarian People's Republic regained its power on August 1, 1919 for a few days until the royal Romanian army occupied Budapest. [9]

9 Demokratiezentrum Wien. "Ungarn Im 20. Jahrhundert." 2015. http://www.demokratiezentrum.org/wissen/timelines/ungarn-im-20-jahrhundert.html.

Between 1919 and 1939, monarchy was formally reintroduced as the state form in Hungary. In practice, "Reichsverweser"[10] Horthy managed to gradually expand his power. He consolidated the nation and introduced an authoritarian regime in 1920.[11]

Hungary fought on the side of the Germans during WWII from 1941 to 1945, initially by choice and then continued only when the Horthy government was coercively replaced by the Nazis. On August 20, 1949, Hungary became a Socialist People's Republic based on the Stalinist model and led by Mátyás Rákosi. Imre Nagy followed Rákosi when Stalin died in 1953 and the tensions in the country increased. Nagy liberalized the economy and adopted political reforms, but was overthrown in 1955. In the same year, Hungary co-founded and joined the Warsaw Pact.

Then, in 1956, the Hungarian workers started a revolution, asking for democratic freedom and Hungarian independence, and seeking support from the United States. Nagy formed a government and tried to end the oppression of the Hungarian people by the Soviet Union. When he withdrew the country from the Warsaw Pact, Soviet troops stamped out the political opposition in a bloody offensive that lasted from November 4 until November 11. Consequently, Hungary remained under communist control until 1989.[12]

Janós Kádár, General Secretary of the Hungarian Socialist Worker's Party, implemented the "New Economic Mechanism", an economic program that raised the standard of living under communist rule and granted Hungarians relatively more freedom. By doing so, he placated the Hungarian public, which depoliticized as the need for political reform had decreased. The Hungarians' "adaptational character"

10 "His Serene Highness the Regent of the Kingdom of Hungary"
11 Ibid.
12 Ibid.

was reinforced and opposition partly lost its legitimacy. As a consequence, massive riots or other forms of organized protest ceased.[13] Moreover, the Hungarian opposition was mainly comprised of intellectuals rather than workers, and was not necessarily anti-communist.[14]

Democratic History of Poland before 1989

According to Pula, the beginnings of Poland's democratic history can be traced back to the late sixteenth century.[15] However, as the first democratic constitution according to modern political standards was adopted during the Second Polish Republic, I start the historical analysis of democracy in Poland in 1918.

After the end of WWI, Jozef Pilsudski proclaimed Polish independence on November 14, 1918. From then on, as per the promise of the Provisional People's Government of the Polish Republic, the new parliamentary democracy would always be the "Polish People's Republic". The Poles for their part were very receptive to this political reorientation of their nation. They admired the victorious Western Allies, in particular the United States and France, and perceived the outcome of war as the triumph of democracy over other forms of government like monarchy or military rule. Pilsudski, who strongly supported equal rights for all people living in Poland regardless of their religious affiliation or social and ethnic origin, was appointed provisional head of state. He tried to integrate every political party into the state-building process and addressed the most urgent issues of the new Polish republic by adopting more than two hundred decrees before the Polish parliament,

13 Prohnitchi, Elena. "Comparative Analysis of the Modes of Transition in Hungary and Poland and Their Impact on the Electoral Systems of These States." *CEU Political Science Journal*, 2006, 5-10.

14 Kamm, Henry. "Hungary Is Far From Democracy, and Even From Poland." The New York Times. July 29, 1989. http://www.nytimes.com/1989/07/30/weekinreview/the-world-hungary-is-far-from-democracy-and-even-from-poland.html.

15 Biskupski, Mieczysław B., James S. Pula, and Piotr J. Wróbel. The Origins of Modern Polish Democracy. Athens: Ohio University Press, 2010.

Sejm, was elected. The parliamentary elections took place on January 26, 1919 and were open to every Polish citizen over the age of 21 (with the exception of members of the army), including women. Thus, Poland became the first state in Europe to grant women the right to vote. One month later, on February 20, the Polish Sejm was established and Pilsudski formally transferred his power to parliament. The "March Constitution", which replaced the "Little Constitution", a transitional constitution that had been adopted in 1919, mirrored those of Western democracies, particularly the French Constitution of 1875. Back then, the Polish regarded their new constitution as "one of the most democratic constitutions in the world".[16] The year of 1921 saw the culmination of Poland's democratic history. With the passing of the constitutional amendment which is known as the "August novella" on August 2, 1926, the Second Polish Republic took on authoritarian characteristics, after its first democratic steps had not been able to unite the politically divided nation.[17]

With its defeat in the Second World War, Poland came under communist control, and so remained until the Soviet Union collapsed in 1989. Still, in the early 1970s, the Polish people showed that they were well able to organize themselves in opposition to the imposed regime, and political dissent persisted. A severe economifc crisis encouraged a number of workers' strikes and resulted in a slight liberalization of economic and social policies, which paved the way for future opposition movements. This mobilization against a common enemy, the Soviet regime, united the Polish people and eventually led to the Solidarity independent trade union. In addition, the opposition movement was strongly supported by the Catholic Church in Poland, which acted as a liaison between the communist regime and Solidarity,

16 Biskupski, Mieczysław B., James S. Pula, and Piotr J. Wróbel. The Origins of Modern Polish Democracy. Athens: Ohio University Press, 2010.
17 Ibid.

and facilitated the Roundtable negotiations in 1989.[18]

In comparison, Poland had the opportunity to develop democratically for a longer period of time than Hungary did. In addition, the opposition in Poland during communist leadership was stronger, as there was no political figure like Kádar who alleviated the financial and psychological side effects of the autocratic state form by launching an economic program and by granting relatively more freedom.

Hungary's and Poland's Path to EU Accession

The Impact of PHARE

In December 1989, the Council of Ministers of the EU decided to launch the "Poland and Hungary: Assistance for Restructuring their Economies (PHARE)" program, put into effect the following year.[19] Originally, the program only supported Poland and Hungary, but it was quickly extended to a total of thirteen CEECs.[20] The amount given to a country was dependent on its population, GDP, and various qualitative criteria.[21] Between 1990 and 1993, Poland received ECU 822 million, and Hungary ECU 416. Along with Romania, the two countries were the main recipients of PHARE aid. The program was designed to foster democracy during the transition period by making the commitment to democratic values and the establishment of the rule of law a condition for financial support. In addition, each country had to pursue the long-term goal of becoming a market economy. [22]

18 Prohnitchi, Elena. "Comparative Analysis of the Modes of Transition in Hungary and Poland and Their Impact on the Electoral Systems of These States." *CEU Political Science Journal*, 2006, 5-10.

19 *What Is Phare?: A European Union Initiative for Economic Integration with Central and Eastern European Countries*. Brussels: European Commission, 1994.

20 Kaldor, Mary, and Peter Wilke. "Final Report - Evaluation of the PHARE and TACIS Democracy Programme." 1997. http://ec.europa.eu/europeaid/how/evaluation/evaluation_reports/reports/cards/951432_en.pdf.

21 *What Is Phare?: A European Union Initiative for Economic Integration with Central and Eastern European Countries*. Brussels: European Commission, 1994.

22 Ibid.

The democratic impact of the PHARE program that can be considered a first step towards EU accession for Poland and Hungary is difficult to measure in quantitative terms. The PTDP evaluation report (Kaldor & Wilke, 1997) mentions four main problems that arise when trying to analyze the outcome of specific projects within the PHARE framework. First, the democratic situation of a country without the benefits — that is, a counterfactual analysis of what might have happened in the country if the EU had not offered incentives for democratization — of the project is unknown. Second, the investment in technical assistance does improve the skill level of people working in institutions, but this outcome is not quantifiable. Third, it is impossible to clearly distinguish between the impact of one democratic project over another. Finally, if a change in the behavior of institutions and people does not translate into corresponding local policies, the outcome of the project might not be appropriately reflected.[23] There are still, however, ways to evaluate the level of democracy after the implementation of programs such as PHARE. Based on the overall progress of (1) democracy, (2) specific policy areas, (3) increase in the number of NGOs, (4) single project outcomes, (5) pro-democratic local policies, and (6) transfer of know-how, the authors of the evaluation report created the following "development of democracy" table in 1997:

Table 1: Development of Democracy Table (Kaldor & Wilke, 1997)

	Direction of Development	Comments
Poland	↑	Stable development towards democratic society
Hungary	↑	Stable development towards democratic society

On the basis of this analysis, it is reasonable to conclude that Poland and

23 Kaldor, Mary, and Peter Wilke. "Final Report - Evaluation of the PHARE and TACIS Democracy Programme." 1997. http://ec.europa.eu/europeaid/how/evaluation/evaluation_reports/reports/cards/951432_en.pdf.

Hungary were steadily developing into democracies before EU accession. That is, enough of the criteria upon which the authors based their evaluation, listed above, were met in each country.

Association Agreements and Accession Agreements

The Association Agreement between the European Community and Hungary and Poland was signed December 16, 1991, and came into effect on February 1, 1994.[24] About two months later, Hungary and Poland formally submitted their EU-membership application. After having responded to a questionnaire designed to evaluate the current state of affairs in the CEECs who intended to become part of the EU in 1996, the Commission invited Hungary and Poland along with four other CEECs to accession talks. After referenda in both Poland and Hungary with a respective outcome of 77.45% and 83.76% in favor of EU accession, the Treaty of Accession was signed in Athens on April 16, 2003 and entered into force on May 1, 2004[25]. [26]

Before a CEEC country was able to apply for EU membership, it had to be recognized as a European State according to Article 49 of the EU Treaty and commit itself to freedom, democracy, human rights and fundamental freedoms, and the rule of law according to Article 6 of the EU Treaty. Furthermore, accession candidates had to fulfill the Copenhagen Criteria which separated liberal countries from authoritarian or communist states.[27]

Public Opinion about the European Union

24 "The History of Hungarian EU Membership." The EU Policy Website of the Hungarian Govenrment. 2015. http://eu.kormany.hu/the-history-of-hungarian-eu-membership.
25 "EU Statement on the Accession Referendum in Poland." European Union Delegation to the United Nations. June 10, 2013. http://eu-un.europa.eu/articles/en/article_2408_en.htm.
26 "The 2004 Enlargement: The Challenge of a 25-member EU." Europa - Summaries of EU Legislation. 2007. http://europa.eu/legislation_summaries/enlargement/2004_and_2007_enlargement/e50017_en.htm.
27 Ibid.

An important aspect in the analysis of the discussion about EU accession and how it affected democracy in Hungary and Poland is public opinion in these countries regarding their potential membership in the EU. The following table demonstrates how Poles and Hungarians thought about EU accession in 1996 and 2001 (Pickel, 2003).

Table 2: How Poles and Hungarians thought about EU accession (Pickel, 2003)

	Who profits the most from EU accession? (in %, 1996)		**In case of a referendum about EU accession, I would vote (in %, 2001 (1996))**	
	Nation	**EU**	**Yes**	**No**
Poland	24	24	54 (77)	26 (8)
Hungary	25	29	70 (54)	10 (18)

In both nations, the percentage of those who expected accession to the EU to be beneficial to their own country versus to the EU was more or less the same in 1996. Neither in Poland nor in Hungary did most of the people expect EU accession to be beneficial to their nation or to the EU as a whole. At the same time, a majority would have voted in favor of EU accession in a potential referendum. Five years later, in 2001, the picture had slightly changed. While in both countries, still more than 50% would have supported EU accession, the percentage of "yes" voters had fallen from 77% to 54% in Poland; at the same time, 26% versus previously 8% would even have voted against joining the EU. The case in Hungary is reversed: here, the number of those in favor had increased from 54% to 70%, while those who rejected EU accession only made up 10% in comparison to 18% in 1996.

Overall, the population in Hungary and Poland supported EU accession prior to joining the EU. The question remains how this picture might have changed during the first years of EU membership. A survey conducted by the Policy

Association for Open Society (PASOS) found the following results in 2009.[28] Both Poles and Hungarians stated that their country needed a political change prior to 1989. Striking, however, are the answers to the remaining three questions: 66% of Hungarians considered the way democracy had been established in their country a failure, while 62% of Poles saw it as a success.

The picture is repeated with regard to the perception of the advantages and disadvantages of the current period compared to the time before 1989. Fifty percent of Hungarians thought that the current period had more disadvantages. By contrast, 59% of Poles said the current period had more advantages. Finally, 46% of Hungarians were convinced that their democracy had been built mostly with the help of other countries, while only 25% of Poles shared this opinion in their country. A quote presented in the study demonstrates the fact that these answers are mainly based on economic factors and not necessarily political ideology: "Although we cannot remember the pre-1989 period well, I am convinced that during the communist regime there was a certain living standard achievable for every citizen, whereas nowadays we face economic and unemployment risks, and uncertainty in life."[29]

28 Bútorová, Zora, and Olga Gyarfášová. "Return to Europe: New Freedoms Embraced, but Weak Public Support for Assisting Democracy Further Afield." *Policy Association for an Open Society*, 2009. http://cps.ceu.edu/sites/default/files/publications/pasos-policy-brief-return-to-europe-2009.pdf. [see Table 3]

29 Bútorová, Zora, and Olga Gyarfášová. "Return to Europe: New Freedoms Embraced, but Weak Public Support for Assisting Democracy Further Afield." *Policy Association for an Open Society*, 2009. http://cps.ceu.edu/sites/default/files/publications/pasos-policy-brief-return-to-europe-2009.pdf.

Table 3: Results of survey about democracy conducted by the Policy Association for Open Society (PASOS) in 2009 (Butorova & Gyarfasova, 2009)

	From the perspective of 20 years, the building of democracy in our country was:		In comparison with the pre-1989 period, the current period has:		Did the pre-1989 political system in our country require changes?		We have established and built our democracy:	
	Success	Failure	More advantages	More disadvantages	Substantial changes	No changes	Mostly with help of other countries	Mostly through our own efforts
Poland	62	29	59	10	56	6	25	62
Hungary	28	66	28	50	45	8	46	35
Source (p.)	3		3		4		9	

Measuring Democracy – the democratic situation in both countries from 2003 to 2014

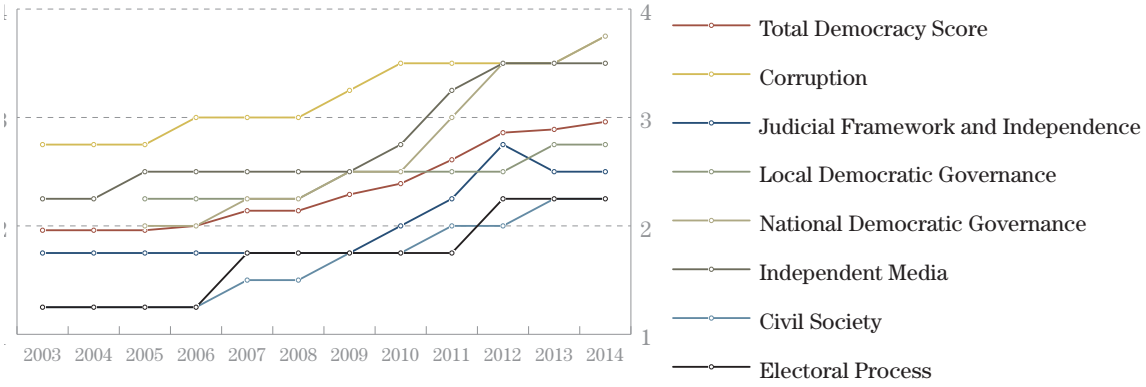
There exist several indices that measure democracy, each differing in methodology, transparency, and fundamental assumptions. I have decided to use the Nations in Transit Rating by Freedom House (FH) and the democracy report by The Economist Intelligence Unit (EIU) for the purpose of this paper, as these indices provide a detailed analysis for both Hungary and Poland.

The Nations in Transit Rating is comprised of various sub-categories that seek to measure the level of political rights in the country of interest. On a scale of 1 = best and 7 = worst, and in increments of one quarter, a country's democratic situation is assessed. Another frequently cited index created by FH is the Freedom in the World Index. Countries are analyzed in two categories: political rights (i.e. electoral processes, political pluralism, functioning of government), and civil liberties (i.e. freedom of speech and association, rule of law, and personal rights).[30] The

30 Norris, Pippa. "Measuring Governance." *Harvard Kennedy School of Governance*, May 15, 2011. http://www.hks.harvard.edu/fs/pnorris/Acrobat/Measuring%20Governance.pdf.

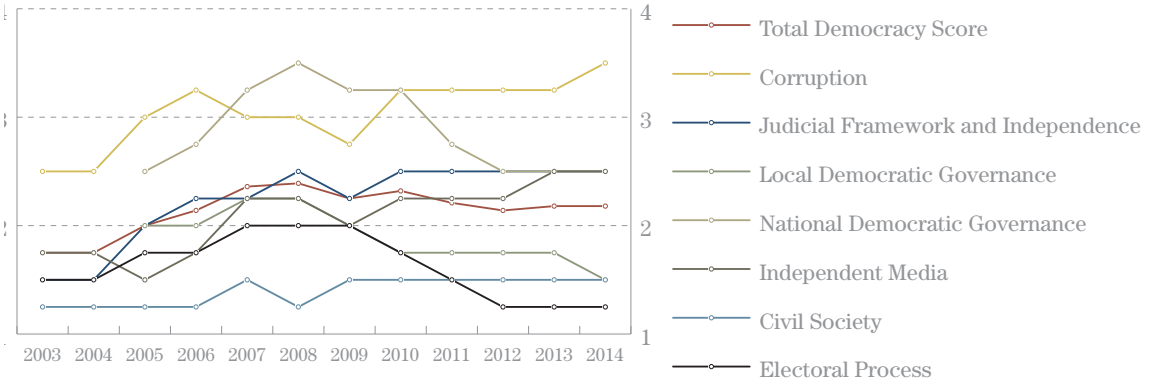
current indices for Poland and Hungary are 1/1 and 2/2 respectively, with an overall Freedom Rating of 1 for Poland and 2 for Hungary.[31] For an in-depth analysis of the democratic situation in Hungary and Poland, however, I looked at the Nations in Transit Rating for both countries from 2003 to 2014, the most recent data available. This allowed me to track the evolution of democracy from before accession to the EU until today. Interestingly, both Poland and Hungary show overall democracy scores in 2014 that are above their scores from the years before and after accession. While the absolute score rose from 1.75 in 2003/2004 to 2.18 in 2014 for Poland, it increased by a whole point, from 1.96 in 2003/2004 to 2.96 in 2014 in the case of Hungary. The general trend for both cases already indicates that joining the EU eventually led to an overall decrease in the quality of democracy. This observation is particularly pronounced with regards to Hungary: for the period beginning in 2011 until today, the score exceeds 2.5. The timing of this observation coincides with Viktor Orbán's assumption of office as Prime Minister of Hungary in May 2010.

Figure 1: Nations in Transit Ratings and Averaged Scores for Hungary (Freedom House, 2015)



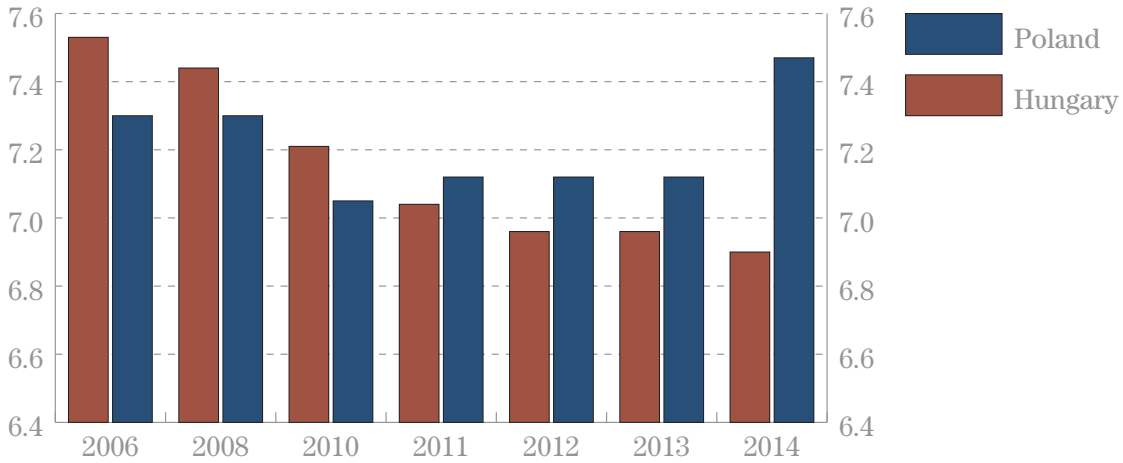
31 "Freedom in the World." Freedom House. 2015. https://freedomhouse.org/report-types/freedom-world#.VTW8B1VViko.

Figure 2: Nations in Transit Ratings and Averaged Scores for Poland (Freedom House, 2015)



The EIU index shows a similar picture. It measures the level of democracy in five different categories: electoral process and pluralism, civil liberties, the functioning of government, political participation, and political culture. The resulting overall score is then used to classify a country as one of the four following types: full democracy, flawed democracy, hybrid regime, authoritarian regime. The EIU report includes 167 countries, which are ranked from 1 = highest score to 167 = lowest democracy score. Poland was ranked 40th, and Hungary 51st in 2014.[32]

Figure 3: Democracy Indices for Hungary and Poland, 2006 – 2014 (The Economist Intelligence Unit, 2015)



32 "Democracy Index 2014." The Economist Intelligence Unit. 2015. http://www.eiu.com/public/topical_report.aspx?campaignid=Democracy0115.

When looking at the development of the overall democracy index beginning in 2006, which was the first year the index was produced, the downward trend for Hungary becomes instantly visible. For Poland, by contrast, the outlook according to EIU is promising, as the index increased by 0.35 points from 2013 to 2014. The current indices are 6.9 and 7.47 for Hungary and Poland respectively. In the running report, EIU mentions Hungary as the negative example with respect to the development of its democracy.[33]

In April 2010, Viktor Orbán's party, Fidesz, won the elections with a two-thirds parliamentary majority. Orbán, now centre-right, started his political career as a student in the late eighties when he co-founded the "Alliance of Young Democrats". Then, in 1994, he began to gradually convert the originally liberal youth organization into a "Führer" Party. The reason for this change was simply Orbán's ambition for power and personal glory. He realized that, in order to be successful, his party would have to adopt conservative, nationalist policies. Following this strategy, he accused the Social-Liberal government of not truly representing Hungarians. Instead, he claimed, it complied with rules coming from international financial institutions that were not in the interest of the people. Thus, the government was "alien". When a corruption scandal among government officials was called to public attention, Orbán's Fidesz party reacted quickly and made electoral promises that they would put an end to scandal and corruption. His strategy turned out to be effective: Orbán became Prime Minister in July 1998.[34]

During his first term in office, there were several corruption scandals in his government. Although some of these incidents were significant, Orbán was able

33 "Democracy Index 2014." The Economist Intelligence Unit. 2015. http://www.eiu.com/public/topical_report.aspx?campaignid=Democracy0115.

34 Lendvai, Paul. *Hungary: Between Democracy and Authoritarianism*. London: Hurst & Company, 2012.

to stay in power and did not resign. In order to win back the sympathy from the population, he launched various policies that directly benefitted them. Nevertheless, voters decided not to support Orbán to the same extent as they did in the previous election, and was voted out of office in 2002.[35]

Debreczeni, who wrote the biography "Image" about Orbán, predicted in 2009 that Orbán would try to regain the power he had to give up in 2002. As soon as Orbán had the opportunity, Debreczeni asserted, he would put all his efforts into regaining his office and assuring that he not fall from power again.[36] Debreczeni's prophecy turned out to be right. After Orbán had assumed office in 2010, he appointed his friends to key positions, such that formerly independent offices like that of the presidency, the state audit office, the media council, and the head of Magyar Nemzeti Bank, Hungary's central bank, were controlled by his cronies.[37]

Moreover, in 2012, Hungary adopted a new constitution, the Fundamental Law, which has since been amended several times. As of now, many political decisions require a supermajority, which makes it very difficult for future governments to enact legislation, as they a majority of two-thirds of the seats in parliament in order to do so. [38]Orbán was reelected in 2014 and is likely to win the elections again in 2018.[39]

In the case of Poland, there has been no fundamental change in the democratic situation of the country for the past three years, with both EIU and the Nations in Transit Rating showing this trend. EIU, however, indicates a positive development

35 Ibid.
36 Ibid.
37 "Democracy Index 2014." The Economist Intelligence Unit. 2015. http://www.eiu.com/public/topical_report.aspx?campaignid=Democracy0115.
38 Kovács, Balázs Áron. "Nations in Transit: Hungary." Freedom House. 2014. https://freedomhouse.org/report/nations-transit/2014/hungary#.VTUlYVVVikp.
39 "Democracy Index 2014." The Economist Intelligence Unit. 2015. http://www.eiu.com/public/topical_report.aspx?campaignid=Democracy0115.

for democracy for 2014, as the score for "political participation" and "political culture" increased significantly (from 6.11 and 4.38 to 6.67 and 6.25 respectively) .[4041] In the FH report, the corruption score – by far the highest score of all subcategories – increased from 3.25 to 3.5, while the local government index improved from 1.75 down to 1.5. The increased number of referenda in Poland might also explain the improvement in the two EIU categories. [42]

From 2007 to 2014, Donald Tusk was the country's prime minister. He was followed by Ewa Kopacz, the current incumbent.

EU – Missed Opportunity to Prevent Hungary's Democratic Backsliding?

According to Gyarfasova (2013), a general problem with the viability of democracy in Eastern Europe persists: the scope of discretion conferred on the authorities is too large.[43] Through arbitrary decision making, democracy loses its credibility in the eyes of the people in these countries. This problem then can only be solved through public policies and governance capacities.

Ungváry argues that the Orbán regime was able to emerge as a result of "internal cultural and political traditions" of Hungarian society. It could gain power during times that posed novel problems, like the situation of Hungary after the collapse of the Soviet Union and the lost confidence in liberal democracy when this newly

40 Cześnik, Mikołaj. "Nations in Transition: Poland." Freedom House. 2014. https://freedomhouse.org/report/nations-transit/2014/poland#.VTU8T1VViko.
41 Jasiewicz, Krzysztof. "Nations in Transit - Poland." Freedom House. 2012. https://www.freedomhouse.org/sites/default/files/NIT2012Poland_final.pdf.
42 Cześnik, Mikołaj. "Nations in Transition: Poland." Freedom House. 2014. https://freedomhouse.org/report/nations-transit/2014/poland#.VTU8T1VViko.
43 Gyarfasova, Olga. "Eastern Europe's Third Decade of Democracy." EurActiv. February 18, 2013. http://www.euractiv.com/future-eu/eastern-europe-third-decade-demo-analysis-517876. Gyarfasova, Olga. "Eastern Europe's Third Decade of Democracy." EurActiv. February 18, 2013. http://www.euractiv.com/future-eu/eastern-europe-third-decade-demo-analysis-517876.

implemented system showed its flaws and negative implications for society. Orbán was the one political figure who could fill these vacuums and give the nation new hope and self-confidence. In a country that had been on the losing side in both World Wars, and that had no tradition of free public discourse, Orbán quickly realized that fascism would not be capable of openly disrupting and eventually destroying democracy. Instead, he incorporated democracy into his politics as a way to legitimate his actions and rhetoric, while simultaneously undermining democratic institutions. His party skillfully made use of all the failures of these new structures. By propagating the belief that everything and everybody outside of Hungary was an enemy, he successfully united a majority of Hungarians, poor laborers and rich beneficiaries of his politics alike. Orbán made himself not only the political, but also the cultural leader of the country. A mixture of Christian spirituality — as when he refers to Hungary as "God's Country" — and nationalist thought seem to work for Orbán's purposes, whose final goal can be stated as absolute political power.[44]

An EU strategy that focuses on sanctions, therefore, would only sustain Orbán's power. He will exploit every opportunity to convince Hungarians that Western institutions do harm to their nation in order to vindicate his political actions. This is why the opposite approach would be a more effective instrument.

To prevent further democratic backsliding of the country, assuring that the Hungarian media can maintain its independence in a hostile environment, and investing in its democratic civil organizations will be essential. First, this method guarantees the independence of at least part of the media. Currently, only media companies that support the Fidesz government get funding, making it nearly

44 Ungváry, Rudolf. "Hungary: Ruling in the Guise of Democracy." OpenDemocracy. November 8, 2014. https://www.opendemocracy.net/can-europe-make-it/rudolf-ungv%C3%A1ry/hungary-ruling-in-guise-of-democracy.

impossible for those that are not loyal to the regime to survive. Second, a strong civil society – informed by an independent media – is likely the only way back to liberal democracy. Strengthening NGOs in the country would countervail Orbán's efforts to entirely infiltrate democracy and its institutions.[45] As Rose-Ackerman argues public participation in shaping a country's policy is important to ensure government accountability.[46] But only if the public is informed and educated about the political situation in the country will it be able to raise its voice and demand more transparency and the right to political participation from its government. This would create a domino effect: an educated society re-evaluates its current political situation and pushes for more political participation, thereby improving the accountability of the government.

The general problem of Hungary and its people's attitude towards Europe is economic in nature. Although, overall, the country has benefitted from EU accession, many Hungarians did not; often, their individual economic situations even deteriorated. Indeed, while multinational corporations reap the benefits, small-scale farming and the food industry are facing insolvency. Hungarians' hopes for what might come with EU membership turned out to be illusive. The current transition phase therefore is perceived as just another period that produces poverty and uncertainty. This is why Orbán's popularity is so high – he seems to understand the deception of the country and offers a path that leads to independence from other countries' political wills.[47]

45 Bitó, László. "How Hungary Can Be Led Back to the Path of Liberal Democracy." OpenDemocracy. September 23, 2014. https://www.opendemocracy.net/can-europe-make-it/l%C3%A1szl%C3%B3-bit%C3%B3/how-hungary-can-be-led-back-to-path-of-liberal-democracy.

46 Rose-Ackerman, Susan. "From Elections to Democracy in Central Europe: Public Participation and the Role of Civil Society." *East European Politics & Societies* 21, no. 1 (2007): 31-47. doi:10.1177/0888325406297132.

47 Verseck, Keno. "Ungarn: Feldzug Gegen Die EU." Bundeszentrale Für Politische Bildung. February 27, 2014. http://www.bpb.de/politik/wahlen/europawahl/179664/ungarn-feldzug-gegen-die-eu.

Orbán's strategy has worked out well for him so far. The central question in this context is this: why has the EU not reacted to his undemocratic rhetoric and actions until now? At this point, it is not predictable if and when his balancing act between upholding Hungary's role as a democratic member state of the EU who respects the union's values, and his nationalist rhetoric and policies to strengthen the ruling party's political power, will start to tilt irreversibly to the wrong side?[48] Organizations like Human Rights Watch show their concern about the lack of action on behalf of the EU with regard to Hungary. The European Commission had introduced a "rule of law" measure in 2014 to counteract human rights abuses in EU member states, but this instrument has not been applied to Hungary so far.[49]

The EU has responded to the shifting political situation in Hungary, but did not address the underlying and fundamental problem of a democratic backsliding; rather, they dealt with symptoms rather than consequences of this problem. First, there was an ECJ ruling against Hungary when judges were sent to early retirement. Second, the Commission took enforcement action against Hungary's controversial constitutional changes. Third, two commissioners, Kroes and Reding, publicly stated that they are in support of applying Article 7 of the EU Treaty that would suspend Hungary's voting rights.[50]

By contrast, the EP has not been able to agree on any action so far, as Orbán's Fidesz party is a member of the European People's Party, while the liberal parties support Kroes' and Reding's call for Article 7.[51] In July 2013, Green MEP Tavares

48 Orenstein, Mitchell A., Péter Krekó, and Attila Juhász. "The Hungarian Putin? - Viktor Orban and the Kremlin's Playbook." Foreign Affairs. February 8, 2015. http://www.foreignaffairs.com/articles/143014/mitchell-a-orenstein-peter-kreko-and-attila-juhasz/the-hungarian-putin.

49 "Hungary: Little EU Action on Rights Concerns." Human Rights Watch. February 18, 2015. http://www.hrw.org/news/2015/02/18/hungary-little-eu-action-rights-concerns.

50 Gall, Lydia. "Response to Hungary Is Test for EU." EU Observer. May 16, 2013. https://euobserver.com/justice/120145.

51 Ibid.

presented a resolution that declared Hungary's political actions incompatible with the democratic values of the EU, referring to Article 2 of the Treaty on European Union.[52]

There has neither been any form of response on part of the European Council.[53]

The Council of Europe responded to the constitutional draft in 2011 by expressing its concerns that the process had not involved oppositional forces. Then, in April 2013, Hungary nearly became the first member state to be monitored by the Monitoring Committee of the Council of Europe's Parliamentary Assembly, as Hungary had not been able to meet democratic standards defined by the EU. The Parliamentary Assembly, however, did not adopt this radical measure and only repeated its concerns.[54]

From the action and inaction of the EU, it becomes obvious that there would have been means and opportunities for the EU to counteract Orbán's anti-democratic policies, had there been more of a consensus in Brussels on the definition and priority of democratic standards. It is important that the EU takes the situation in Hungary seriously and responds accordingly such that it does not lose its credibility for protecting the values upon which it is based.

I contend that EU sanctions against Hungary as an instrument to stop its democratic backsliding would be detrimental. Instead, the leverage of the EU's diplomatic and political authority with regard to its member states' compliance

52 Sarlo, Alexandra Wiktorek, and Maia Otarashvili. "Can the EU Rescue Democracy in Hungary?" Foreign Policy Research Institute. July 2013. http://www.fpri.org/articles/2013/07/can-eu-rescue-democracy-hungary.

53 Gall, Lydia. "Response to Hungary Is Test for EU." EU Observer. May 16, 2013. https://euobserver.com/justice/120145.

54 Sarlo, Alexandra Wiktorek, and Maia Otarashvili. "Can the EU Rescue Democracy in Hungary?" Foreign Policy Research Institute. July 2013. http://www.fpri.org/articles/2013/07/can-eu-rescue-democracy-hungary.

with democratic standards could be increased by strengthening the media sector and NGOs in the country. In addition, the EU should apply Article 7 in the EU Treaty to emphasize the importance of its democratic values. By not doing so, the EU loses credibility in the eyes of current member states and accession candidates. It also demonstrates the EU's incapability of dealing with its member states due to the apparently unfeasible application of articles in the EU Treaty.

Conclusion

From the literature review we can conclude that there does not exist a single framework that can explain the impact of the EU on democratization in a member state during both the pre- and the post-accession period. Most studies examine EU impact on democracy for the time before the accession to the EU, but there are few scholars who try to deal with the question for current member states. This might have to do with the fact that most scholars predicted that democratic institutions and values, once established, would be stable enough in the future if a potential member state were able to fulfill the Copenhagen Criteria in advance. The case of Hungary proves this argumentation wrong. Instead, the democratic development of a country is accelerated and intensified during the pre-accession period, when the EU imposes top-down policies that accession candidates are eager to implement to evidence their desire to become a member state.

After accession, however, the picture changes. Even in the case of Poland, it is clear that the pre-accession period with high democracy scores was followed by a decline of the country's democratic standards. Although not as pronounced as in Hungary, this observation shows that, as soon as conditionality is not in place anymore after a country has joined the EU, the incentives to live up to the

democratic standards — which were themselves hastily implemented — decrease.

The further democratic development of the country is then dependent on its democratic history, the economic situation of its people, and, very much tied to that, the people's opinion of the EU. Also, it does not seem to be correlated to pre-accession success, although this hypothesis would have to be examined in detail in an additional study. Ultimately, there is no single, unified framework in which to assess the effect of EU accession. Each potential and current member state of the EU is foremost its own sovereign territory with unique cultural, economic, and social identities. As such, the affect of EU accession on democratization will inevitably differ between states, as will the extent to which its democratic institutions will ultimately develop.

Sectarian Conflict in the Middle East and the Rise of ISIS: An Analysis of Saudi and Iranian Roles and Influences

Muhammed Hasnain Haider

Following the realist and neorealist traditions, this paper addresses how Iran's power ambitions and Saudi determination to maintain Sunni hegemony have factored directly into the strife in Iraq, Syria and Yemen. The analysis is further deepened by viewing the ongoing power competition in the Middle East through the prism of larger geopolitical concerns, specifically the desire of the United States to sustain its hegemonic status in the region by supporting both Saudi Arabia and Israel. The paper also elaborates upon the proposition that both Saudi Arabia and Iran have persistently attempted to leverage Salafi extremism while fundamentally failing to realize the mutual threat presented by ISIS and the opportunities inherent in a joint anti-jihadist strategy.

The paper opens with an account of the processes by which both the Saudi monarchy and Iran's theocracy have evolved into state champions of their respective fundamentalisms. The cases of present-day Iraq, Syria and Yemen are then considered in detail with special focus on the underlying commonalities and significant differences. The rise of Salafi extremism in the context of both fundamentalisms is analyzed through the paper. Other recurring themes are the role and shifting priorities of the United States in the region, the U.S-Saudi relationship, and the goals of the Iranian regime. The paper concludes with specific policy recommendations.

Introduction

In 632 AD, the Prophet Mohammed died and the majority of people in the small Arabian city-state of Medina recognized the Prophet's close aide and childhood friend, Abu Bakr, as the new leader. Abu Bakr thus became the first Caliph, or successor to Muhammed: a revered figure for the Sunnis, a usurper to the Shias. Many of the rivalries in the Middle East today are defined to a great extent by this succession controversy some 1,400 years ago in Medina. The maelstrom of Shia-Sunni conflict in the contemporary Middle East represents a struggle for dominance over this Islamic narrative. To a great extent, however, Saudi and Persian religio-

political identities have interacted to spark fires of sectarian strife that are currently aflame across the Middle East.

The internal ethnic and sectarian fault-lines of the countries discussed in this paper, coupled with the struggle between Iran and Saudi Arabia over ideology and regional hegemony, have enabled Takfiri jihadism, which strives to impose an extreme version of Islam by militant force, to greatly increase its power, territorial reach, and capacities for spreading death and destruction. It appears clear things will get much worse in terms of violence and bloody conflict before they get any better.

This paper will explore the processes by which both the Saudi monarchy and Iran's theocracy have evolved into the foremost state champions of their respective fundamentalisms. After establishing how religion, regional politics, and global powers factor into the historically fraught relations between Saudi Arabia and Iran, the paper will examine the religious-political lines in Iraq after the U.S. invasion and how those lines have shaped the rise of ISIS. Finally, this paper will examine the war in Syria through the lenses of Iraqi, Iranian, and Saudi influence. The remainder of the paper proposes strategies, which, if adopted by the regional and international players, can hope to bear favorable results in the long-term.

In this context, two world events hold special significance: the Iranian Revolution of 1979 and the terrorist attacks of September 11th, 2001. The former ushered in a Shia theocracy in Iran, determined to stake out a more assertive role in the Middle East, and unique in the region in its hatred for the United States. The latter resulted in the United States' wars in Afghanistan and Iraq, which strengthened the extremist narrative within Sunni Islam and intensified the virulence of jihadist terrorism as an unintended consequence. The invasion of Iraq freed the country's Shia majority to serve as the first real testing ground for hands-on Iranian influence. This Iranian opportunity deepened the animus between Saudi Arabia and Iran, and used the age-old differences between Shia and Sunni as a catalyst for a full-blown struggle for regional influence. Presently, as Shias, mostly sidelined minorities in Sunni-majority states, coalesce around Iranian leadership, and Iran jockeys for increasing control in the Shia Crescent, pushback from the Sunni world has resulted in many Muslim nations' eruption into seemingly endless violence.[1]

Following the realist and neorealist traditions, this paper addresses how Iran's

1 V. Nasr, *The Shia revival: How conflicts within Islam will shape the future* (New York: Norton, 2006), 184.

ambitions for carving out a regional power bloc, and Saudi determination to maintain Sunni hegemony, have factored directly into the strife in Iraq and Syria. The rise of Salafi extremism in the context of both the aforementioned fundamentalisms remains a consistent theme through every section of this paper. In addition, the role and shifting priorities of the United States in the region is a recurrent theme, given the U.S.'s extensive part in all ongoing Middle Eastern conflicts, Saudi Arabia's status as a long-standing U.S. ally and client, and the Iranian regime's avowed opposition to U.S. policies in the region.

The Shia-Sunni Split in Islam

A handful of the Prophet's companions felt that, during his lifetime, Mohammed had designated his cousin, son-in-law and protégé, Ali ibn Abi Talib, as his successor. These minority dissenters came to be known as the Shia, the partisans of Ali. Ali eventually became the fourth "rightly-guided" caliph of an Islamic empire that had been greatly expanded by his predecessors. By the time of his assassination, however, he had been completely politically outmaneuvered by the Umayyad clan, ancient Meccan rivals of the Hashemite clan of Mohammed and Ali.[2] The Umayyad army's massacre of the Prophet's grandson, Hussain ibn Ali, and a small band of companions and blood relatives at Karbala, Iraq, in 680 AD, definitively cemented Shi'ism as the political and dogmatic alternative to the mainstream Sunni Islam of the caliphal empires. The Shias suffered tremendous oppression under the Umayyad and Abbasid caliphates, augmenting their sense of exceptionalism.[3] Over the centuries, however, the exigencies of empire, tribalism, and shared living space taught the Shias and the Sunnis to peacefully coexist across the vast reaches of the Islamic faith despite spasmodic episodes of violence.

A political fault-line in the Middle East that predates the Shia-Sunni schism is the ancient civilizational rivalry between the Arab and Persian peoples. In Persian history, the fall of the Sasanian Empire to the Arabic armies of the Caliph Umar marks a time of great humiliation and suffering. Therefore, throughout Islamic history, greater Persia consistently hosted rival dynasties to the caliphates. Furthermore, in the 15th century, Persian national identity became irretrievably fused with Shi'ism.

2 L. Hazelton, *After the prophet: The epic story of the Shia-Sunni split in Islam* (New York: Doubleday, 2009).
3 Ibid.

Between the 18th and 20th centuries, the regions comprising present-day Saudi Arabia, drifted towards a new interpretation of Sunni Islam that called for a return to the ways of the earliest Muslims and, most disturbingly, considered Shi'ism a sinful aberration against the faith that must be dealt with most harshly. In the late 20th century, this Saudi Wahhabism would face off against Persian Shi'ism with disastrous consequences.

Saudi Arabia: A Brief History

Contemporary Saudi-Iranian relations are largely defined by the Shia-Sunni doctrinal dichotomy in the Islamic narrative, which continues to inform the sociopolitical identities of both nations. Prior to the Iranian revolution of 1979, Saudi Arabia imagined itself the nominal leader of the Muslim world, owing to the existence of Islam's holiest shrines in Mecca and Medina. After the revolution, as Iran's assertive Shia theocracy ambitiously strove to provide alternate leadership to the Muslim world's historically downtrodden Shias, Saudi Arabia assumed more aggressive leadership of Sunni fundamentalism. This standoff between Saudi Arabia and Iran's Shia theocracy has engendered a new cold war in the Middle East.[4] Furthermore, since modern-day Islamic extremism and Saudi Wahhabism share the same basic ideological strain, it is imperative that the rise of the Al-Saud family in peninsular Arabia be examined in proper religious and political context.

Beginnings in Saudi-Wahhabi Alliance

In the mid-eighteenth century, Mohammed ibn Al-Saud, the progenitor of the present Saudi dynasty and a tribal elder in the central Arabian region of Nejd, formed an alliance with Mohammed bin Abdul Wahhab, a religious leader who professed a puritanical and fundamentalist version of Islam. In the Wahhabi tradition, Sufi Islam, reverence of saints, shrines, and other syncretic elements of the Islamic culture, are considered corruption of the true monotheistic faith. All groups who espouse such practices are liable to be declared apostates under the concept of "takfir" and "should be killed, their wives and daughters violated, and their possessions

4 F. Gregory Gause III "Beyond Sectarianism: The New Middle East Cold War," *Brookings Doha Center* (2014): Accessed May 20, 2015. http://www.brookings.edu/~/media/research/files/papers/2014/07/22-beyond-sectarianism-cold-war-gause/english-pdf.pdf

confiscated."[5,6] The Wahhabis reserve special hatred for the Shia, considering them apostates and referring to them by the derogatory term "rafidha," or those who reject the legitimacy of the initial successors to the Prophet Mohammed in favor of Ali, the Prophet's son-in-law.[7, 8] Mohammed ibn Al-Saud fully embraced Wahhabi ideology in the hope of exploiting their religious fervor for greater political and territorial gain. The followers of Ibn e Abdul Wahhab, in turn, wanted to leverage the alliance to stamp out the heretic ways of the Ottomans and the Hashemite Sharifs of Mecca and impose their own religious doctrine in the Arab heartland.

For the entire nineteenth century, the fortune of this alliance waxed and waned. Shias got their first taste of Wahhabi zealotry in the bloody 1802 sack of Karbala, Iraq, by Saudi forces.[9] A conquest of Mecca and Medina proved short-lived in the face of effective Ottoman retaliation. In 1891, the Al-Saud were ousted from their own homeland of Nejd by the rival Rashidi tribe, but they returned in the early 20th century to form a small tribal kingdom around present-day Riyadh.

Sykes-Picot: Al-Saud's opportunity

During the First World War, the British enlisted the aid of Sharif Hussein of Mecca, the venerated Hashemite ruler of the holy cities of Mecca and Medina, against the Ottoman Empire in return for the promise to install Hussein as the ruler of a unified Arab kingdom after the war.[10, 11] The Sharif's help proved instrumental in weakening Ottoman resistance. The Saudis did not participate in this Hashemite-led effort, choosing rather to consolidate themselves in the Nejd against the pro-Ottoman Rashidis. Upon the conclusion of World War I, it was revealed that the British and the French had secretly entered into the Sykes-Picot Agreement,

5 Shaykh ul-Islam Ibn Abdul Wahab, "Shaykh ul-Islam Ibn Abdul Wahab on Those Whom Takfir is made of," *Salafipublications.com*, Accessed May 20, 2015. http://www.spubs.com/sps/downloads/pdf/MNJ090005.pdf

6 Alastair Crooke, "You Can't Understand ISIS If You Don't Know the History of Wahhabism in Saudi Arabia," *The World Post* (2014), Accessed May 20, 2015. http://www.huffingtonpost.com/alastair-crooke/isis-wahhabism-saudi-arabia_b_5717157.html.

7 Fanar Haddad, "The Language of Anti-Shiism," *Foreign Policy* (2013), Accessed November 20, 2015. http://foreignpolicy.com/2013/08/09/the-language-of-anti-shiism/.

8 Tom Rogan, "Al-Baghdadi's Global Jihad," *National Review* (2014), Accessed May 20, 2015, http://www.nationalreview.com/article/392662/al-baghdadis-global-jihad-tom-rogan.

9 Helen Chapin Metz, *A Country Study: Saudi Arabia*, (Washington, D.C.: Library of Congress, 1993), Accessed May 20, 2015, http://cdn.loc.gov/master/frd/frdcstdy/sa/saudiarabiacount00metz_0/saudiarabiacount00metz_0.pdf.

10 "Husayn-McMahon Correspondence | British-Palestinian History," *Encyclopedia Britannica*. Accessed November 20, 2015. http://www.britannica.com/topic/Husayn-McMahon-correspondence.

11 Peter Shambrook, "Contradictory Promises," *The Balfour Project* (2014), Accessed May 20, 2015, http://www.balfourproject.org/contradictory-promises/.

which carved Arab lands formerly held by the Ottomans into European spheres of influence. While no pan-Arab state came into being, the British did recognize Sharif Hussein as the king of Hejaz while installing his sons as rulers in the protectorates of Jordan and Iraq.

In religious terms, the Wahhabi inclinations of the Al-Saud placed them at odds with the moderate Sunnism of the Sharif of Mecca. Detecting a souring of relations between the Sharif and Great Britain over the Sykes-Picot division of Arab territories, Abdul Aziz Al-Saud launched his campaign of conquest, completely ousting the Sharif from the Hejaz by 1926. The Sharif's request to the British for aid against the onslaught from Nejd was turned down on the pretext that the British Empire did not intervene in religious disputes. Sharif Hussein fled to Jordan while the Wahhabis, as first order of business, took to destroying shrines venerated by Shias and moderate Sunnis alike in the vast necropolises of Medina and Mecca.

Consolidation of Power by Al-Saud

By 1932, Abdul Aziz Al-Saud was able to consolidate all his territorial gains in the Arabian Peninsula into the present-day Kingdom of Saudi Arabia. A final challenge, however, emerged from Al-Saud's own ranks as the hardcore Wahhabi Ikhwan clamored to spread their creed to the British protectorates of Jordan and Iraq. Unwilling to wager his newfound kingdom in conflict against the British Empire, King Abdul Aziz refused the Ikhwan's expansionary zeal. Civil war ensued, in which Al-Saud's tribal armies effectively liquidated the Ikhwan ranks and leadership between 1929 and 1930.[12] This established a trend that persists to the present-day, whereby the Al-Saud, while upholding and projecting Wahhabi doctrine across the Muslim world, refuses to risk their dynasty or their self-professed leadership of Islam. Thus, where in the beginning they battled the Ikhwan, in 2015 they must oppose ISIS and Al-Qaeda although they share the same ideological core. Within the borders of the Kingdom, at least, Wahhabism has been transformed "from a movement of revolutionary jihad and theological takfiri purification, to a movement of conservative social, political, theological, and religious da'wa (Islamic call) and to justifying the institution that upholds loyalty to the royal Saudi family and the King's absolute power."[13] The use of diplomatic realpolitik and the discovery of

12 Hassan Abedin, "Abdul Aziz Al-Saud and the Great Game in Arabia, 1896-1946," King's College London (2002), Accessed November 20, 2015. https://kclpure.kcl.ac.uk/portal/files/2925835/397151.pdf.

13 Alastair Crooke, "You Can't Understand ISIS If You Don't Know the History of Wahhabism in Saudi Arabia," *The World Post* (2014), Accessed May 20, 2015. http://www.huffingtonpost.com/

oil in the Kingdom's east in 1938 enabled Abdul Aziz's Saudi Arabia to become an important player in international politics.[14]

Saudi Arabia: Exporter of Oil and Extremism

In the twentieth century, Saudi Arabia's prominence on the global stage and its unique relationship with the West, and the United States in particular, rested both on its status as the top producer and exporter of oil in the world and on its readiness to manipulate Sunni Islam to further American geopolitical interests. Partly in service of the aforesaid interests and partly in a protracted effort to establish its own exclusive hegemony over the Muslim world, Saudi Arabia set about to "'Wahhabise' Islam, thereby reducing the 'multitude of voices within the religion' to a 'single creed.'"[15] Conservative estimates place the investment of an approximate 100 billion USD of Saudi Arabia's petroleum wealth since the start of the Afghan War into promoting Wahhabism and Salafi Jihad,[16] a modern-day nom de guerre espoused by the Wahhabis to denote their aspirations of the pious and glorious ways of the first two caliphs.

Saudi largesse has had disastrous consequences for nations that were eager to receive it. Pakistan's military dictatorship in the 1980's, prosecuting the Afghan Jihad with support from the United States, allowed millions of dollars to be funneled into the establishment of Wahhabi seminaries across Pakistan to prepare impressionable youth born into poverty for holy war. The current disequilibrium is such that, in a country where only a minority professes Wahhabi (Deobandi) Islam, a vast majority of the seminaries promote that strain.[17] Holy warriors returning from the Afghan Jihad wreaked bloody havoc on the minority Shias of Pakistan. In Afghanistan, the Wahhabi theocracy, in the form of the Taliban, dutifully hosted the perpetrators of 9/11. Much of present-day Islamic terrorism traces its roots to that fateful decade in Afghanistan where modern Salafi Jihad attained maturation with Saudi money, American equipment, and Pakistani management.[18]

---

alastair-crooke/isis-wahhabism-saudi-arabia_b_5717157.html.

14 "March 3, 1938: Oil in Saudi Arabia," *CNN* (2003), Accessed May 20, 2015, http://www.cnn.com/2003/US/03/10/sprj.80.1938.oil/.

15 Crooke, "You Can't Understand ISIS," *The World Post*.

16 Yousaf Butt, "How Saudi Wahhabism Is the Fountainhead of Islamist Terrorism," *The World Post* (2015), Accessed May 20, 2015, http://www.huffingtonpost.com/dr-yousaf-butt-/saudi-wahhabism-islam-terrorism_b_6501916.html.

17 Tariq Rahman, "Madrassas: The Potential for Violence in Pakistan," *Criterion Quarterly* (2013), Accessed November 20, 2015. http://www.criterion-quarterly.com/madrassas-the-potential-for-violence-in-pakistan/.

18 John Moore, "The Evolution of Islamic Terrorism: An Overview," *PBS*, Accessed October 30,

Even the current standard bearer of Islamic extremism, ISIS, can attribute its strength and influence to misplaced efforts by the Saudi and like-minded gulf monarchies to check ascendant Iranian influence and Shia power after the U.S. invasion of Iraq in 2003. Petrodollars blindly funneled to topple Shi'ite-aligned Assad in Syria and prevent the stabilization of the Shia-dominated democratic governments in post-Saddam Iraq kept ending up in the wrong hands until the world was confronted with the scourge of ISIS.[19]

Iran: Since the Revolution

Over the past decade, partially as a consequence of the U.S. invasion of Iraq, the Shia Islamic Republic of Iran has rapidly emerged as an alternative power-center in the Middle East vis-à-vis Sunni/Wahhabi Saudi Arabia. Apart from unsettling the Al-Saud dynasty's political and regional ambitions, Iran's theocracy has also repeatedly challenged the nerves of the United States regarding long-standing U.S. geostrategic interests in the region, the interests of U.S.-aligned Arab states, and the security of Israel. It is almost too fantastic, in the present-day context, to conceive of a time not long ago when Iran was the West's most visible partner in the Middle East.

Pre-Revolution Iran: Brief Overview

Iran holds unique status in the Muslim world in that it is deeply wedded to the millennia-old Persian language and culture that predates the Islamic conquest of Persia in 651 AD by thousands of years. The historical rivalry between Arab and Ajam (Persian), before and after Islam, was a major contributing factor of the Persian Empire gradually espousing the alternative creed in the Islamic faith: Shi'ism.[20] From the fifteenth century up until 1979, Iran was ruled by various Shia dynasties with largely secular patterns of government and imperial hegemony.[21] In 1952, Iran's fledgling attempt at constitutionalism and economic self-determination was jettisoned via a CIA-engineered coup d'état that overthrew the democratically elected Prime Minister Mossadegh and handed absolute power to the Shah. This

2015. http://www.pbs.org/wgbh/pages/frontline/shows/target/etc/modern.html

19 O. Jones, "To really combat terror, end support for Saudi Arabia," *The Guardian* (2014), Accessed May 20, 2015. http://www.theguardian.com/commentisfree/2014/aug/31/combat-terror-end-support-saudi-arabia-dictatorships-fundamentalism

20 F. Haddad, "The language of anti-Shiism," *Foreign Policy* (2013), Accessed May 29, 2015. http://foreignpolicy.com/2013/08/09/the-language-of-anti-shiism/

21 M. Shuster, "The Origins Of The Shiite-Sunni Split," *NPR* (2007), Accessed May 29, 2015. http://www.npr.org/sections/parallels/2007/02/12/7332087/the-origins-of-the-shiite-sunni-split

move left lingering feelings of outrage and resentment among the general public, which would eventually unite such diverse elements as the Shia clergy, leftist students and Marxist intellectuals, the urban middle classes, and the rural poor in an anti-Shah, and anti-U.S., revolution.[22] The Shah, meanwhile, became increasingly heavy-handed towards his subjects while his intelligence agencies, the SAVAK, became the embodiment of brutal repression and state terror.

Iran's relations with Saudi Arabia during this time remained cordial. In a letter in the 1960's, the Shah advised Saudi King Faisal bin Abdulaziz Al Saud to "modernize" his country by adopting western culture and attitudes and thus strengthen the House of Saud. King Faisal's reply was to prove prophetic: "Your population is 90 percent Muslim. Please do not forget that."[23] In a short span of time, the Shah's brazenly western and callously luxurious lifestyle had completely alienated the Iranian masses.

Revolution

By the 1970's, an exiled firebrand Shia cleric, Ayatollah Roohullah Khomeini, had captured the imagination of the average Iranian Shia as the true voice of dissent against the Shah. The mysterious deaths of Khomeini's son and revolutionary intellectual Ali Shariati in 1977 sparked a cycle of nationwide protests and violence that culminated in an entirely new political order by early 1979. When the Shah fled in January 1979, the interim government under Prime Minister Shahpour Bakhtiar invited Khomeini back from exile in the hopes of establishing a democracy under the clergy's spiritual blessing. Khomeini, on the other hand, had dedicated much of his life as a jurist to deriving the notion of "Velayat e Faqih" from Shia Islamic law.[24] Under this philosophy, during the continued occultation of the 12th Shia Imam, the Faqih, i.e. the senior-most Shia jurist/lawgiver, is the Imam's vicegerent in the world and has complete authority over the polity in both spiritual and temporal matters. Pursuantly, challenging the authority of the Faqih is akin to disobedience to Allah.[25] The worldly punishment for any opposition to Khomeini's interpretation

22 "Iran and the Left: Why They Supported Islamic Reaction," *Workers Vanguard* No. 229 (1979), Accessed May 29, 2015. http://www.internationalist.org/iranandleft7904.htm

23 E. Sciolino, "U.S. Pondering Saudis' Vulnerability," *New York Times* (2001), Accessed May 29, 2015. http://www.nytimes.com/2001/11/04/world/a-nation-challenged-ally-s-future-us-pondering-saudis-vulnerability.html

24 Hamid Hosseini, "Theocracy versus Constitutionalism: Is Velayat e Faghigh Compatible with Democracy?" *Journal of Iranian Research and Analysis*, Vol. 15, No. 2 (1999), Accessed May 29, 2015. http://www.cira-jira.com/Vol%20%2015.2.8%20%20Hosseini%20November%201999.pdf

25 R. Khomeini, "Governance of the Jurist," *Iran Chamber Society*, Accessed May 29, 2015.

of scripture has often been nothing short of death.

Riding a massive wave of popularity, Khomeini acted quickly to assert his divine authority.[26] With a demoralized, mutinous army refusing to stand by Prime Minister Bakhtiar, Khomeini proclaimed his own interim government under moderate Islamist Mehdi Bazargan. By the end of 1979, the constitution of the new-fangled Islamic Republic of Iran had come into force, vesting supreme legal and executive authority in the person of the Vali e Faqih. In effect, the revolution merely oversaw the transition from monarchic to clerical absolutism.[27] Khomeini's ambitions for unopposed theocracy, however, chafed against the democratic and socialist aspirations of the thousands of political activists and intellectuals who had made the revolution possible. Within the clergy itself, there was high-level opposition to Khomeini's fusion of religion and politics. The Iran-Iraq War was to give Khomeini ample opportunity to remove these thorns from his side, consolidate his hold over the country, and tweak the rules of his own doctrine to designate a successor of his choice to the Supreme Leadership.

Iran-Iraq War: 1980-1988

Ostensibly, Iraq's ill-timed and ill-advised invasion of Iran in September 1980 was to settle longstanding border disputes with its easterly neighbor. The glaringly Shia essence of the Iranian Revolution unsettled Iraq's Baathists vis-à-vis their own suppressed Shia majority. Khomeini's blatant pan-Islamism, calling for all Muslims of the world to unite against despotism in the name of God, challenged Saudi Arabia's leadership of the Islamic world and threatened the Saudi dynasty.[28] The bile that Khomeini's Revolution reserved for Israel and the U.S. created concerns regarding U.S. interests in the Middle East. After the 1982 revolutionary takeover of the U.S. embassy in Tehran, U.S. aid to Iraq would greatly increase while Saudi Arabia reportedly provided 30.9 billion USD to Saddam over the course of the war.[29]

Internationally isolated and materially challenged, Iran fought back tooth and nail by the sheer force of nationalism and the martyrdom-centric Shia faith.[30] The

http://www.iranchamber.com/history/rkhomeini/books/velayat_faqeeh.pdf

26 V. Nasr, (2006). "The Shia revival: How conflicts within Islam will shape the future" (p. 131). New York: Norton.

27 Laura Secor, "From Shah to Supreme Leader," *Foreign Affairs* (2014), Accessed May 30, 2015. https://www.foreignaffairs.com/reviews/review-essay/shah-supreme-leader

28 Nasr, The Shia revival, 137-8.

29 "Iran-Iraq War," (n.d.), Accessed May 30, 2015. http://www.saylor.org/site/wp-content/uploads/2011/08/HIST351-11.1.4-Iran-Iraq-War.pdf

30 Lisa Farhamy, "Iranian Nationalism," The Public Purpose Vol. 5, Accessed May 30, 2015.

war also greatly empowered Khomeini, as the nation, reeling from the turmoil of the revolution, coalesced around his person. The fabled Revolutionary Guards emerged as Iran's elite fighting unit, owing loyalty to no one but the Supreme Leader. By mid-1981, Iran's first democratically elected President, Abol Hassan Banisadr, was hounded out of both the Presidency and the country for coming into conflict with one of Khomeini's clerical underlings. Clerical opposition to Khomeini was effectively—sometimes brutally—suppressed.[31] As Iranian forces reversed all Iraqi territorial gains, Khomeini effectively outmaneuvered domestic political opposition, banning and persecuting all secular, liberal, and Marxist parties who held different aspirations for post-imperial Iran. Upon ceasefire in 1988, Khomeini issued an infamous fatwa that sanctioned the executions of thousands of leftists held in Iranian prisons.[32] Interestingly, in condemning these prisoners, Khomeini's fatwa used the same language that is all too familiar in today's war-torn Middle East, including condemnations of enemies of Allah and Islam, apostates, rejecters of the true faith, and hypocrites.[33] Towards the close of his life, in order to ensure the continuation of his legacy, Khomeini altered the dynamics of Velayat e Faqih and elevated Ali Khamenei, a minor cleric but a Khomeini loyalist, as his successor and the next Supreme Leader.

Iran: Isolated but Rising

Since the Revolution, Iran has struggled to maintain a functioning, oil-reliant economy in the face of grueling economic sanctions imposed by the West. These sanctions are punishment for Iran's presumed nuclear program and its support for Hezbollah, Hamas, and other organizations fighting Israel. Prior to the U.S. invasion of Iraq, Iran was hemmed in on all sides with mostly unfriendly nations.[34] Domestically, Iran has witnessed a perpetual tug-of-war between the hardliners and the reformists. The Iranian youth's overwhelming desire for social freedoms, openness, and overall change is manifest in the 2009 protests against election fraud

https://www.american.edu/spa/publicpurpose/upload/Iranian-Nationalism.pdf

31 Said Amir Arjomand, "Consolidation of Islamic Theocracy," in *The Turban for the Crown: The Islamic Revolution in Iran* (New York: Oxford University Press, 1988), 147-163.

32 "Deadly Fatwa: Iran's 1988 Prison Massacre," *Iran Human Rights Documentation Center* (2014), Accessed May 30, 2015. http://www.iranhrdc.org/english/publications/reports/3158-deadly-fatwa-iran-s-1988-prison-massacre.html

33 Struan Stevenson, "The Forgotten Mass Execution of Prisoners in Iran in 1988," *The Diplomat* (2013), Accessed May 30, 2015. http://thediplomat.com/2013/07/the-forgotten-mass-execution-of-prisoners-in-iran-in-1988/

34 William Beeman, "Examining Iran's ties to Hezbollah," *International News*, Accessed May 30, 2015. http://www.political-analysis.org/intnews/id3.html

which kept hardliner Ahmadinejad in power, the 2013 election of moderate Hassan Rouhani, and the recent jubilation witnessed upon the signing of the nuclear accord with the U.S.

The game-changing event for Iranian fortunes in the Middle East was the American invasion of Iraq, which freed the Iraqi Shia majority to find its own footing in a nascent democracy and to take the leading role in state formation. The development of new linkages with Iran was inevitable, as much of the returning Shia leadership, clerical and otherwise, had at one time or another been given asylum by the Islamic Republic. Furthermore, innate distrust of Americans within the Iraqi Shia also enabled Iran to quickly develop its networks and auxiliaries of influence. Iran has played its hand in Iraq in a very calculated and pragmatic manner. As violence erupted between various Shia factions in 2004-06, Iran chose not to play favorites.[35] Iran has also generally recognized and respected the unifying stature for the Iraqi Shias of Grand Ayatollah Ali Sistani of Iraq, who is clearly opposed to the doctrine of Velayat e Faqih and has supported democracy in Iraq.[36] The opening up of Iraq has formed the continuous land-bridge between Iran and Lebanon, famously termed "the Shia Crescent" by Jordan's King Abdullah, which has provided an entirely new channel for Iranian ambition and influence.[37]

Iranian meddling in post-Saddam Iraq is often blamed by the West and Saudi Arabia for creating conditions whereby Iraqi Sunnis feel alienated and marginalized, feeding directly into the Sunni insurgency in various forms over the past decade.[38] This is an oversimplification of matters, as a host of factors contribute to the present-day horrors in Syria and Iraq, which I will discuss at length in this paper. Regarding the mass support for insurgency in the Sunni heartland, history is yet to decide whether it represents a case of extreme marginalization or the loss of disproportionate power and centuries' old Sunni privilege in Iraq's new electoral democracy. In either case, Iran, at present, is fully invested in the fight against ISIS.

35 Selig Harrison, "Iran, Iraq, and the United States: The View from Tehran," *Center for International Policy* (2014), Accessed May 30, 2015. http://www.ciponline.org/research/entry/iran-iraq-and-the-united-states-view-from-tehran

36 Mehdi Khalaji, "The Last Marja: Sistani and the End of Traditional Religious Authority in Shiism," *The Washington Institute* (2006), Accessed May 30, 2015. https://www.washingtoninstitute.org/uploads/Documents/pubs/PolicyFocus59final.pdf

37 Ali Mamouri, "Is the Shiite revival here?" *Al-Monitor* (2015), Accessed May 30, 3015. http://www.al-monitor.com/pulse/originals/2015/03/iran-shiite-sunni-middle-east.html#

38 Mark Mazzetti, "Shiite Radicalism Could Fuel Wider Violence, Official Warns," *New York Times* (2007), Accessed May 30, 2015. http://www.nytimes.com/2007/01/12/washington/12intel.html

Iranian Major General Qassem Soleimani boasted that, "in the fight against this dangerous phenomenon, nobody is present except Iran."[39] The Iranian commitment to the fight against ISIS, the global upsurge in Sunni extremism, and the recent thaw in U.S.-Iranian relations all stand to redefine Iran's role and image on the world stage.

The War in Iraq and Syria

The seemingly unending bloody conflict in post-Saddam Iraq and post-Arab Spring Syria is arguably the ugliest chapter of the Saudi-Iran rivalry. During this period, both regional powers jockeyed for influence in the Middle East. This section aims to shed light on how this rivalry continues to shape the main present day conflicts in the Middle East.

Iraq: Aftermath of the U.S. Invasion

The U.S. invasion of Iraq in March 2003 and the subsequent disintegration of Iraqi defense and Saddam's Baathist regime changed Iraq's status, at least in American estimations, from yet another Middle-Eastern mischief-maker and regional flashpoint to a client state that must be rebuilt and brought into the global political economy on American terms. What likely eluded American decision-makers at the point of attack were the intricacies of the Iraqi polity that rendered holistic control over the entire country almost impossible. By the time of the U.S. withdrawal in 2011, it seemed that no amount of U.S. military presence could reverse the internal conflicts in Iraq.[40, 41] Critics, however, believe that the military vacuum left by the 2011 U.S. withdrawal was eventually filled by ISIS in 2014.[42]

The toppling of Saddam Hussein yeilded the immediate return of many exiled political figures, most of whom were Shia, maneuvering to stake their claim in the new political system. While many of these returned exiles were secular politicians

39 Sam Wilkin and Parisa Hafezi, "Only Iran is confronting Islamic State, paramilitary chief says," *Reuters* (2015), Accessed May 29, 2015. http://www.reuters.com/article/2015/05/25/mideast-crisis-iraq-iran-idUSL5N0YG0MK20150525

40 James F. Jeffrey, "Behind the U.S. Withdrawal From Iraq," *Wall Street Journal* (2014), Accessed June 9, 2015. http://www.wsj.com/articles/james-franklin-jeffrey-behind-the-u-s-withdrawal-from-iraq-1414972705

41 Jason Brownlee, "Was Obama Wrong to Withdraw Troops from Iraq?" *Washington Post* (2014), Accessed November 20, 2015. https://www.washingtonpost.com/news/monkey-cage/wp/2014/06/26/was-obama-wrong-to-withdraw-troops-from-iraq/

42 Shadee Ashtari, "If You're Blaming The Iraq Crisis On Obama's Troop Withdrawal, Answer These 4 Questions." *The Huffington Post* (2014), Accessed November 20, 2015. http://www.huffingtonpost.com/2014/08/12/obama-iraq-criticism_n_5669444.html

who gained initial favor with the U.S. administration, the real power brokers would prove to be the clerics and religious leaders returning from Iran whose tribulations under Saddam truly registered with the long-oppressed Shia majority of Iraq.[43] The lifting of the Baathist ban on ancient Shia rituals around the shrines in Karbala, Najaf, and Baghdad and the spontaneous outpouring of religious fervor added to the influence and prestige of the clerical establishment—both past exiles and local Ayatollahs who had quietly suffered Saddam's excesses.[44] The wounds of Saddam's brutal suppression of the Shia uprising of 1991 and life as disempowered, second-class citizens appeared fresh in the popular Shia psyche.

On the other hand, the U.S. administration of Iraq under L. Paul Bremer proceeded to disband the Iraqi army and pursue the de-Baathification of the civil bureaucracy. Since the Baathist state was disproportionately staffed with the minority Sunnis of Iraq, these steps amounted to a sudden loss of privilege for Sunnis. This created a large population of disenfranchised, disaffected, and militarily-trained Sunni men with a grudge to nurse.[45] Already weaned on perpetual Baathist propaganda of the Iranian threat to the Sunnis of Iraq and portrayals of the Iraqi Shias as Iranian proxies, the inclusion of Shias and Kurds in the upper echelons of power by the U.S. administration did not sit well with the Sunnis. The stage was thus set for armed insurgency.

Insurgency in Iraq: The Sectarian Dimension

The violence in post-2003 Iraq has generally had two distinct faces: guerilla warfare against the U.S., and later, bloody sectarian violence between Sunni and Shia coupled with the presence of Iraqi regime forces in Sunni northwestern Iraq. In the initial years after the invasion, violence was largely directed against the Shias by a loose alliance of former Baathists and Wahhabi/Salafis. The most pro-Iran faction among the Shias in post-invasion Iraq was the Supreme Council for Islamic Revolution in Iraq (SCIRI) led by Ayatollah Baqir Al-Hakim, who was killed along with 125 others in a massive car bombing in 2003. Bombings targeting civilians in Shia neighborhoods across the breadth of Iraq have become the norm with varying

43 "Iraq's Shias: Return of the exile," *The Economist* (2003), Accessed June 9, 2015. http://www.economist.com/node/1781366

44 Johanna McGeary, "Iraq's Shadow Ruler," *Time* (2004). Accessed June 9, 2015. http://content.time.com/time/magazine/article/0,9171,995500,00.html

45 Robert Weiler, "Eliminating Success During Eclipse II: An Examination of the Decision to Disband the Iraqi Military," *Marine Corps University* (2009), Accessed June 9, 2015. http://www.dtic.mil/dtic/tr/fulltext/u2/a511061.pdf

frequency. Shia reprisals for gratuitous sectarian attacks began in earnest in 2006 after the shrine in Samarra, wherein two Shia Imams are entombed, was blown up by Salafi extremists.[46] Such reprisals have resulted in the deaths of hundreds of civilian Sunnis.

A major contributing factor towards the escalating sectarian flavor of the conflict in Iraq was the emergence of Wahhabi (Salafi) extremists at the forefront of Sunni resistance to first the U.S. and then the Shia-dominated government in Baghdad. Sensing opportunity in the post-invasion chaos and widespread Sunni disaffection in Iraq, the Al-Qaeda leadership gave the go-ahead to Jordanian militant and veteran of the Afghan Jihad, Abu Musab Al-Zarqawi, to set up the local chapter of the international terrorist network, Al Qaeda in Iraq (AQI), in 2004. Al-Zarqawi proved adept at forging alliances with Sunni tribes and ex-Baathist military officers to make the infamous "Sunni triangle" a living nightmare for U.S. forces.[47] In his virulent hatred towards the Shia, Al-Zarqawi was even more extreme than his bosses; his independent streak would eventually be inherited by ISIS, the successor organization to AQI. The killing of Al-Zarqawi in a U.S. airstrike in June 2006 was a huge setback to the insurgency in Iraq. However, the many Salafi outfits fighting in Iraq did unite under the banner of the Islamic State of Iraq (ISI) in late 2006 to ensure that wide swathes of the country remained lawless territory.

Iraqi Problems: Representative Government

While constant unrest brewed in the Sunni northwest, Shia southern Iraq was beset with its own particular set of problems. Shia political parties vacillated between considering America the foremost enemy and some willingness to work with U.S. authorities towards rebuilding the state. Furthermore, many armed Shia militias openly vied for influence with the Shia populace. Most notable among these were the Al-Badr brigades associated with SCIRI and Moqtada Al-Sadr's Mahdi Army. [48] Shia militias, especially the Mahdi Army, have also taken the lead in terrorizing the Sunnis in Baghdad and elsewhere.[49] The Mukhtar Army, notorious for its openly

46 Robert Worth, "Blast Destroys Shrine in Iraq, Sets off Sectarian Fury," *New York Times* (2006), Accessed June 9, 2015. http://www.nytimes.com/2006/02/22/international/middleeast/22cnd-iraq.html

47 M. Kirdar, "Al-Qaeda in Iraq," *Center for Strategic and International Studies* (2011), Accessed June 9, 2015. http://csis.org/files/publication/110614_Kirdar_AlQaedaIraq_Web.pdf

48 Juan Cole, "It Takes a Following to Make an Ayatollah," *The Washington Post*, Accessed June 9, 2015. http://www.washingtonpost.com/wp-dyn/articles/A64131-2004Aug13.html

49 Joshua Partlow, "Mahdi Army, Not Al-Qaeda, is Enemy No. 1 in Western Baghdad," *The Washington Post* (2007), Accessed June 9, 2015. http://www.washingtonpost.com/wp-dyn/

anti-Sunni agenda in Iraq, pledges direct allegiance to Iran's Supreme Leader, Ali Khamenei.

Iraq's electoral domain has been equally chaotic over the past decade. In the parliamentary elections of December 2005, an electoral coalition of major Shia parties carried the most seats, with SCIRI winning the major chunk. However, in order to form a government, a parliamentary coalition was cobbled together with Kurdish parties, with Nouri Al-Maliki, of a smaller Shia faction, as the compromise Prime Minister. A non-cleric but with close ties to Iran, Al-Maliki was beholden to the larger Shia factions within the United Iraqi Alliance. His policies contributed to alienation felt by Sunnis, which he managed through heavy-handed crushing of demonstrations and victimization of senior Sunni political figures.[50] Sunni politicians thus only retained elitist sinecures in parliament and provincial bodies, as initiative on the ground had been lost, for all intents and purposes, to the Salafi Jihadists of ISIS.

The Rise of ISIS

The eruption of Syria into civil war in 2011 gave the ISI ample opportunity to wage holy war against the heretic Alawite regime of Bashar Al-Assad, initially through the Nusra Front. ISIS draws its entire senior leadership from Sunni Iraq, which represents a marriage between former Baathists and Salafi Jihadists. Former Baathist military men heavily populate ISIS's military council responsible for war both on the Iraqi and Syrian fronts.[51] Furthermore, ISIS victories in Mosul and Tikrit in 2014 were achieved on account of strong tactical coordination with Izzat Ibrahim Al-Douri's Naqshbandi Army of Saddam loyalists.[52]

In Iraq, ISIS has successfully played on Sunni tribal insecurities and grievances, and the persistent fear of the Iranian bogey-man. Sunni tribal forces joined ISIS on all fronts in the onslaught of 2014 against the Iraqi government forces, allegedly participating in such atrocities as the Camp Speicher massacre of 1,700 captured

---

content/article/2007/07/15/AR2007071501248.html

50 Juan Cole, "Top 10 Mistakes of former Iraq PM Nouri al-Maliki (That Ruined his Country)," *Informed Comment* (2014), Accessed June 9, 2015. http://www.juancole.com/2014/08/mistakes-maliki-country.html

51 Liz Sly, "The hidden hand behind the Islamic State militants? Saddam Hussein's," *The Washington Post* (2015), Accessed June 9, 2015. http://www.washingtonpost.com/world/middle_east/the-hidden-hand-behind-the-islamic-state-militants-saddam-husseins/2015/04/04/aa97676c-cc32-11e4-8730-4f473416e759_story.html

52 Shane Harris, "The Re-Baathification of Iraq," *Foreign Policy* (2014), Accessed June 9, 2015. http://foreignpolicy.com/2014/08/21/the-re-baathification-of-iraq/

Shia army recruits.[53] Iraq's much-vaunted armed forces, trained at the expense of $26 billion by the Americans, crumbled miserably in the face of the ISIS advance. An overwhelmingly Shia force—thanks to Al-Maliki's flawed policies—the Iraqi army has come to represent to the Sunnis all that they have lost since 2003. In addition, as Iran's Revolutionary Guard assumes key leadership in the fight against ISIS, the Iraqi Army increasingly appears to be a mere tool for the perpetuation of Iranian hegemony. It is the draconian laws and practices imposed by ISIS over the regions under its control that have compelled many Sunni tribes to rethink their stances and consider cooperation with the government in Baghdad.[54] For Iraq's Sunnis, however, there remains a compulsory choice between ISIS and their future in a centralized state, the perception of which remains bleak.

For the Shias of Iraq, the ISIS phenomenon has proved to be both a galvanizing and a unifying force. In 2013, the "quietist" Grand Ayatollah Ali Al-Sistani issued a fatwa condemning and strictly prohibiting sectarian violence against civilian Sunni populations by any Shia organization. In a 2014 fatwa, the Grand Ayatollah made jihad against ISIS incumbent upon all able-bodied Shia men. Spurred to action by these clerical edicts, the various rival Shia militias have combined into the "Hashad Shaabi," the Popular Mobilization Committees at the forefront of the fight against ISIS.[55, 56] While ISIS receives jihadi recruits from all over the world after its spectacular successes in Iraq, Shia men from Iraq and Iran stream to join the Hashad Shaabi after the Ayatollah's fatwa.

Ferment in Iraq: The Role of Saudi Arabia

Saudi leaders had advised the Bush administration against the invasion of Iraq primarily because they foresaw the consequent expansion of Iranian influence in the region. By 2009, the Saudi spy chief, Prince Muqrin bin Abdul Aziz, was complaining to U.S. diplomats that the Shia crescent was "becoming a 'full moon,' encompassing

53 Frederic Wehrey, "An Elusive Courtship: The Struggle for Iraq's Sunni Arab Tribes," *Carnegie Endowment for International Peace* (2014), Accessed June 9, 2015. http://carnegieendowment.org/syriaincrisis/?fa=57168

54 Nour Malas and Ghassan Adnan, "Sunni Tribes in Iraq Divided Over Battle Against Islamic State," *The Washington Post* (2015), Accessed June 9, 2015. http://www.wsj.com/articles/sunni-tribes-in-iraq-divided-over-battle-against-islamic-state-1432251747

55 Ali Mamouri, "Sistani Issues Fatwa Against Sectarian Violence in Iraq," *Al-Monitor* (2013), Accessed June 9, 2015. http://www.al-monitor.com/pulse/originals/2013/10/iraqi-moderates-manage-sectarianism.html#

56 Matt Schiavenza, "Why Ayatollah Al-Sistani's Iraq Fatwa Is So Important," *International Business Times* (2014), Accessed June 9, 2015. http://www.ibtimes.com/why-ayatollah-al-sistanis-iraq-fatwa-so-important-1600926

Lebanon, Syria, Iraq, Bahrain, Kuwait, and Yemen," thus creating problems for the kingdom at home and abroad.[57] Saudi actions in Iraq and Syria have therefore been aimed at breaking the Shia Crescent.

Twelve years since the U.S. invasion of Iraq, Saudi Arabia has yet to establish formal diplomatic relations with the new Iraqi state. Considering the Shia-led government in Baghdad as a mere Iranian stooge, Saudi Arabia has instead attempted to cultivate direct relations with the Sunni tribal, religious, and political leaders of northwestern Iraq.[58] Since the earliest days of the insurgency against the U.S. and the central Iraqi government, millions of dollars of private Saudi religious donations and other aid have persistently made their way to Sunni tribal elders and Wahhabi clerics.[59] Much of this largesse has gone into strengthening the Salafi extremists that are today united under the banner of ISIS as a result of the clerics' shared ideological core with the Salafi jihadists and the fluid nature of the tribes' relations with the Sunni extremists. ISIS takes "Sunni contempt for the Shiites to its logical, and bloody, extreme."[60] This contempt is succinctly captured in the pre-9/11 comments of Prince Bandar bin Sultan, the Saudi Ambassador to the U.S. at that time, to the British Intelligence Chief that the "more than a billion Sunnis have simply had enough of [the Shias]."[61]

Saudi Arabia is the birthplace of the ideology that is the raison d'être of ISIS, and the Saudi clerical establishment shares the notion of takfir for Shias with ISIS. Furthermore, the kingdom has a long history of fanning violent Salafism abroad while laboriously containing it within its own borders.[62] The fact that the status of a Shia in ISIS-held territory is akin to that of a Jew in Nazi-occupied Europe is probably proof of the success of the aforesaid Saudi policy.[63] However, with ISIS, the

57 "SAUDI INTELLIGENCE CHIEF TALKS REGIONAL SECURITY WITH BRENNAN DELEGATION" (2009). Accessed June 9, 2015. https://wikileaks.org/plusd/cables/09RIYADH445_a.html

58 Helene Cooper, "Saudis' Role in Iraq Frustrates U.S. Officials," *New York Times* (2007), Accessed June 9, 2015. http://www.nytimes.com/2007/07/27/world/middleeast/27saudi.html

59 Salah Nasrawi, "Saudis Reportedly Funding Iraqi Sunnis," *The Associated Press* (2006), Accessed June 9, 2015. http://www.washingtonpost.com/wp-dyn/content/article/2006/12/07/AR2006120701070.html

60 Simon Henderson, "The Battle for Iraq Is a Saudi War on Iran," *Foreign Policy* (2014), Accessed June 9, 2015. http://foreignpolicy.com/2014/06/12/the-battle-for-iraq-is-a-saudi-war-on-iran/

61 Patrick Cockburn, "Iraq crisis: How Saudi Arabia helped Isis take over the north of the country," *The Independent* (2014), Accessed June 9, 2015. http://www.independent.co.uk/voices/comment/iraq-crisis-how-saudi-arabia-helped-isis-take-over-the-north-of-the-country-9602312.html

62 Henderson, "The Battle for Iraq."

63 Cockburn, "Iraq crisis."

fire has come too close to home. Not only are the Salafi Jihadists locked in mortal combat with the Iranian-backed Shias of Iraq, they also invoke takfir on the Saudi royal family for being western lackeys and have designs on dislodging it from the heart of the Islamic world.[64] Key ISIS strategy in Saudi Arabia is to push the Saudi Shias towards rebellion in an effort to prove to the Sunni masses that the dynasty has failed its founding ideology.[65] With the kingdom's Sunni populace so radicalized that it has historically provided the most recruits to all Salafi insurrections around the world, perhaps it is time for the House of Saud to reassess its priorities and reorder the kingdom's list of enemies.[66]

Iran's Strategic Depth

After the fall of Saddam, linkages between revolutionary Iran and Shia-majority Iraq were inevitable due to the political, religious, and economic configuration of the two neighbors. Trade picked up almost immediately, and the flow of Shia pilgrims between the two countries provided a boon to both struggling economies. Most importantly, Iran was quick to exploit its strategic advantage. With the majority of Shia political personalities returning to Iraq receiving direct Iranian backing (or having enjoyed Iranian hospitality at one time or the other), Iran's status as the best friend to Iraq's new Shia-dominated state was assured. The Kurds already had strong working relations with Iran from the days of the Iran-Iraq war. Leveraging these new relationships, Iran used Iraqi territory to augment its stakes further west in Syria and Lebanon. In Iraq itself, Iran maintained cordial relations with all warring Shia factions, eschewing partisanship and generally respecting the religious authority of Ayatollah Al-Sistani. All this goodwill was quietly underwritten by the general understanding that in times of crises for the Iraq Shias, Iran would remain steadfast at their back even if it meant war.

As Iraq's Sunni insurgency gained strength, Iran, Iraq's Shias, and the U.S. found themselves battling the same enemy, albeit with no coordinated strategy and with much mutual distrust. U.S. officials believed Iran helped Salafi insurgents travelling

64 Alastair Crooke, "Middle East Time Bomb: The Real Aim of ISIS Is to Replace the Saud Family as the New Emirs of Arabia," *The Huffington Post* (2014), Accessed May 20, 2015. http://www.huffingtonpost.com/alastair-crooke/isis-aim-saudi-arabia_b_5748744.html

65 Aaron Y. Zelin, "The Islamic State's Saudi Chess Match," *The Washington Institute* (2015), Accessed June 9, 2015. http://www.washingtoninstitute.org/policy-analysis/view/the-islamic-states-saudi-chess-match

66 "Saudis most likely to join ISIS and 10% of fighter are women," *Middle East Monitor* (2014), Accessed June 9, 2015. https://www.middleeastmonitor.com/news/middle-east/14758-saudis-most-likely-to-join-isis-10-of-groups-fighters-are-women

from Afghanistan to Iraq to make America "bleed."[67] Iran, on the other hand, still maintains the rhetoric that Salafi insurgency in Iraq, including ISIS, is a grand Saudi-U.S. conspiracy to fracture the Muslim world in the defense of Israel.[68] The vacuum left by U.S. withdrawal in 2011 was filled, at one end, by heightened jihadist activity, and at the other, by Iran's elite Quds Force assuming greater leadership of the beleaguered Iraqi armed forces and the inexperienced Shia militias. Iranian units have taken over the security of Shia holy sites across Iraq, even the greatly-threatened shrine in Samarra deep inside the Sunni triangle.[69] The recent battlefield reverses suffered by ISIS at the hands of the Hashad Shaabi owe in large part to Iranian units joining the battle and the leadership of battle-hardened Iranian commanders. Although Iran has pledged support to all groups fighting ISIS regardless of religious creed, it is improbable that Iraq's Sunnis will ever trust Iran, or be comfortable under overarching Iranian influence. Polarizing as Iran's role in the region may be, its irreversible status as a key player has gained enough recognition for the Obama administration to increase diplomatic engagement with this former enemy, much to the chagrin of the House of Saud and the Salafi Jihadists in both Iraq and Syria.

Syria: The Endless Conflict

The ongoing civil war in Syria has been the most prolonged conflict emerging from the ructions of the Arab Spring in 2011. The tenacity of Bashar Al-Assad, the attitude of the Syrian armed forces, a divided Syrian polity, an irreparably fractured armed opposition, and the interests of regional and international players continue to fuel the fire. While revolts in other Arab countries produced comparatively quick results, there is no end in sight to the bloodletting in Syria, which has produced hundreds of thousands of casualties and millions of refugees.

Assad Regime: 1970—Present-day

Syria has been ruled by the Assad family since 1970, which espouses Baathist Arab Nationalism and belongs to the 12% Alawite minority of Syria, an esoteric strain of Shia Islam.[70] Hafez Al-Assad, a former Air Force officer and Baathist

67 Dexter Filkins, "The Shadow Commander," *The New Yorker* (2013), Accessed June 9, 2015. http://www.newyorker.com/magazine/2013/09/30/the-shadow-commander

68 Aryn Baker, "To Iran, ISIS is one more American plot," *Time Inc.* (2014), Accessed June 9, 2015. http://time.com/2992269/isis-is-an-american-plot-says-iran/

69 Behnam Gholipour, "Deaths in Iraq show two sides of Iran's role in sectarian conflict," *The Guardian* (2014), Accessed June 9, 2015. http://www.theguardian.com/world/iran-blog/2014/dec/30/iran-militia-leaders-killed-iraq-battat-taqavi

70 Tom Heneghan, "Syria's Alawites, a secretive and persecuted sect," *Reuters* (2012),

Defense Minister, led a coup against his own party leadership to establish himself as Syria's dictator in 1970. For thirty years, Hafez Al-Assad ruled with an iron fist, crushing such challenges as the Islamist uprising of the 1980s. He also filled the state's security apparatuses with loyal Alawites to strengthen his regime. However, Hafez Al-Assad maintained a largely secular state, including Sunni and Christian elites in the power circles, championing Arab nationalism against Israel, and keeping the military well-fed and busy in Lebanon. Furthermore, as the nationalistic spirit dissipated in the Arab world, Syria under Hafez cozied up to Iran and Iran-backed Hezbollah in Lebanon during the 1990s. Owing to these factors, Hafez became the only non-monarchic Arab autocrat to date to establish a dynasty and successfully engineer the transfer of power to his son, Bashar Al-Assad, prior to his own death in 2000. Bashar initially appeared a mild reformer and a benign figurehead atop the watertight regime his father had put into place. Since 2011, however, Bashar has fought tooth and nail to cling onto power with scant concern or compassion for the civilian population, turning Syria into a powder-keg primed for conflict.

Arab Spring and Civil War

The Arab Spring sprouted in Syria in quite the same manner as it had in the other countries of the Middle East and North Africa. In February 2011, protests demanding the political rights and personal freedoms that had been suspended for the reign of the Baath party erupted across major Syrian cities, especially Damascus and Aleppo. After failing to placate the masses on the street with promises of reform and threats of crackdown, the regime finally resorted to violence in March and April 2011. Orders to fire on the largely Sunni protestors did not sit well with many in the heavily Sunni armed forces. Early and high-ranking defections from the army led to the formation of the Free Syrian Army (FSA), which spearheaded the insurrection against Assad.[71] Many exiled Syrian politicians and anti-Baathists, organized as the Syrian National Council in Turkey, supported the FSA and it received immediate Western and allied support. The Syrian armed forces, regardless of creed or sectarian identity, in large part remained loyal to Assad, enabling the regime to sustain itself and to retain control of key cities.[72] The armed opposition to Assad remained largely

Accessed June 13, 2015. http://www.reuters.com/article/2012/01/31/us-syria-alawites-sect-idUSTRE80U1HK20120131

71 Jonathan Spyer, "Defying a Dictator: Meet the Free Syrian Army," *World Affairs* (2012), Accessed June 13, 2015. http://www.worldaffairsjournal.org/article/defying-dictator-meet-free-syrian-army

72 Zoltan Barany, "Why Most Syrian Officers Remain Loyal to Assad," *Arab Center for Research*

Sunni, while the sizeable Christian minority chose to bet on secular Assad.[73]

The Salafi extremist element to the Syrian conflict was definitively introduced in January 2012 when the Jabhat Al-Nusra (Victory Front), composed mainly of Syrian and other Levantine and foreign Salafi fighters involved in the Iraqi insurgency under the AQI or ISI banner, burst onto the scene and joined the fight in support of the FSA. The Al-Nusra benefited greatly from the monetary aid of Saudi Arabia and like-minded kingdoms, and from the blind inflow of military aid to all anti-Assad combatants from the U.S. and European allies.[74] As it gained strength and territory, tensions developed with the FSA over the prosecution of the war. Furthermore, Al-Nusra's leader, Abu Mohammed Al-Golani, also ran afoul of ISI's Abu Bakr Al-Baghdadi by asserting too much independence and failing to share the windfall gains from the war. For Al-Baghdadi, who considered Al-Nusra to be an offshoot of the ISI, the final straw was Ayman Al-Zawahiri's ruling that Al-Nusra and ISI were independent organizations working under the global umbrella of Al-Qaeda.[75] Rebranding his organization as the Islamic State of Iraq and Al-Shaam (ISIS), Al-Baghdadi repudiated Al-Qaeda suzerainty and in April 2013 entered the Syrian fray primarily against Al-Nusra. Much of Al-Nusra's foreign fighting strength defected to ISIS. Its eastern territories also fell to ISIS, which established the capital of its so-called Islamic caliphate at Raqa'a. As ISIS gained de facto control of eastern Syria, the civil war quickly became a conflict in which everybody seemed to be fighting everybody else, with an almost mushroom-like growth of factions and belligerent groups. Producing more than an estimated 300,000 people dead and three million refugees, the Syrian Civil War threatens to become the bloodiest and most destructive Middle Eastern conflict in decades.[76]

American Hand, Saudi Glove

& Policy Studies (2013), Accessed June 13, 2015. http://english.dohainstitute.org/release/b8f4f88b-94d3-45a0-b78e-8adad3871daa

73 Majid Rafizadeh, "For Syria's minorities, Assad is security," *Al Jazeera* (2011), Accessed June 13, 2015. http://www.aljazeera.com/indepth/opinion/2011/09/201191213521392719 6.html

74 Ernesto Londono., and Greg Miller, "CIA begins weapons delivery to Syrian rebels," *The Washington Post* (2013), Accessed June 13, 2015. http://www.washingtonpost.com/world/national-security/cia-begins-weapons-delivery-to-syrian-rebels/2013/09/11/9fcf2ed8-1b0c-11e3-a628-7e6dde8f889d_story.html

75 Radwan Mortada, "Al-Qaeda and ISIS: The Renunciation of Abu Bakr al-Baghdadi," *Al-Akhbar* (2014), Accessed June 13, 2015. http://english.al-akhbar.com/content/al-qaeda-and-isis-renunciation-abu-bakr-al-baghdadi

76 "320,000 people killed since the beginning of the Syrian Revolution," Syrian Observatory for Human Rights (2015), Accessed June 13, 2015. http://www.syriahr.com/en/2015/06/320000-people-killed-since-the-beginning-of-the-syrian-revolution/

Unlike post-2003 Iraq, where the Saudi hand was played far more subtly as it acted in opposition to U.S. policy, the Saudi role in Syria has been much more visible and direct. For the purpose of this paper, Saudi policy refers to the joint policy of the Wahhabi-oriented bloc of Arab princely states. At the outset of the conflict in 2011, the United States, Turkey, and the Saudi bloc, each in pursuit of its own particular interests, blindly doled out aid and support to all anti-Assad forces.[77] The U.S. wanted to bolster Israel's security by taking down pro-Iran Assad. Saudi Arabia also wanted to weaken Iran's strategic outreach across the Shia Crescent. Turkey's rightwing Erdogan was concerned about the vast influx of Syrian refugees, the plight of the Sunnis in Syria, and Turkey's shared Kurdish question with Syria. This miscalculation as to the fluidity of the ground situation in Syria, in tandem with considering one type of Salafi jihadist to be different from or better than the other, would later make these powers rue this initial policy. Largesse captured from the FSA, Al-Nusra, and other fighting units provided the momentum that carried ISIS back across all of northwestern Iraq and helped Al-Baghdadi establish his sordid caliphate.[78]

While the United States distanced itself from the Islamist opposition in Syria, declaring Al-Nusra a terrorist organization in late 2012 for being an Al-Qaeda affiliate and going so far in 2014-15 so as to unofficially cooperate with Assad in tackling ISIS, Saudi Arabia continues to play with the Salafi fire.[79] The Saudi youth have been most eager to join Salafi outfits in Syria, and many Saudis consider ISIS members true defenders of the faith rather than terrorists.[80] The Saudi bloc actively funded Al-Nusra until it fell out of favor with the United States. In late 2013, a number of Salafi groups fighting in Syria united under the name of the Islamic Front, eclipsing Al-Nusra as the prime alternative to ISIS in Syria's Islamic Jihad and enjoying complete Saudi approval and support.[81] In 2015, a Turkish and Saudi-

77 Behlül Özkan, "America, Turkey and Saudi Arabia Are Pouring Fuel on the Fire in Syria," *The Huffington Post* (2015), Accessed June 13, 2015. http://www.huffingtonpost.com/behlal-azkan/america-turkey-saudi-arabia-syria_b_7278586.html

78 Michael Stephens, "Islamic State: Where does jihadist group get its support?" *BBC* (2014), Accessed June 13, 2015. http://www.bbc.com/news/world-middle-east-29004253

79 Michael R. Gordon and Anne Barnard, "U.S. Places Militant Syrian Rebel Group on List of Terrorist Organizations," *New York Times* (2012), Accessed June 13, 2015. http://www.nytimes.com/2012/12/11/world/middleeast/us-designates-syrian-al-nusra-front-as-terrorist-group.html

80 Reese Erlich, "With Official Wink And Nod, Young Saudis Join Syria's Rebels," *NPR* (2013), Accessed June 13, 2015. http://www.npr.org/2013/03/13/174156172/with-official-wink-and-nod-young-saudis-join-syrias-rebels

81 Ian Black, "Syria crisis: Saudi Arabia to spend millions to train new rebel force," *The Guardian* (2013), Accessed June 13, 2015. http://www.theguardian.com/world/2013/nov/07/

brokered alliance between the Islamic Front and Al-Nusra rose, wiping out units of the FSA in northwestern Syria as its first order of business.[82] Recently, Al-Nusra has also attempted to curry favor with the U.S. by posturing as anti-regime fighters rather than Salafi terrorists.[83]

In an ultimate analysis, not all American and Saudi efforts have been in vain, despite extremely undesirable consequences. The Shia Crescent as a continuous land bridge between Iran and Lebanon is broken, with the Al-Baghdadi caliphate wedged right in the heart of it. Furthermore, Israel's security stands enhanced as the Syrian state lies in tatters, Iran struggles to maintain its sphere of influence, and Hezbollah fights Assad's war against the Salafi jihadists.

Iran's Extended Fight

Iran and Syria have maintained close relations since the time when both were global pariahs in the 1990s. Iran has remained steadfast behind Assad, in spite of the fact that before the Arab Spring, Syrian intelligence managed their own extremist problem by encouraging jihadists to travel to Iraq to fight in the Sunni insurgency and ultimately undermine Iran's interests in the country.[84] Unlike Iraq, Syria has no significant Twelver Shia population that could be galvanized by Iran's revolutionary Islamism against the forces of Takfirism. The Alawite minority of Syria, albeit a Shia offshoot, is strongly represented in the state, and therefore, it is in no need of Iranian leadership. The Sunnis (secular, fundamentalist, and extremist alike) have no use for Iran's role in the country. As a result, in the early years of the revolution, Iran's support to the Assad regime was limited to weaponry and funds, with very limited Iranian boots on the ground in consultative capacities. Any Iranian functionary met the most gruesome of ends when apprehended by the opposition forces, especially the warriors of Al-Nusra.[85]

In the present, Iran's commitment to the conflict in Syria is only set to increase, Assad's position notwithstanding. ISIS has fought its way through the Syrian land-

syria-crisis-saudi-arabia-spend-millions-new-rebel-force

82 Kim Sengupta, "Turkey and Saudi Arabia alarm the West by backing Islamist extremists the Americans had bombed in Syria," *Independent* (2015), Accessed June 13, 2015. http://www.independent.co.uk/news/world/middle-east/syria-crisis-turkey-and-saudi-arabia-shock-western-countries-by-supporting-antiassad-jihadists-10242747.html

83 Michael Pizzi, "Syria Al-Qaeda leader: Our mission is to defeat regime, not attack West," *Al Jazeera* (2015), Accessed June 13, 2015. http://america.aljazeera.com/articles/2015/5/28/syria-al-qaeda-leader-our-mission-is-to-defeat-regime.html

84 Hayder Al-Khoei, "Syria: The view from Iraq," *European Council on Foreign Relations* (2013), Accessed June 13, 2015. http://www.ecfr.eu/article/commentary_syria_the_view_from_iraq136

85 Dexter Filkins, "The Shadow Commander," *The New Yorker*.

mass to engage in a historic first direct battle with Hezbollah on the Lebanon border.[86] While the ISIS attack was repelled with heavy casualties, the first direct face-off between the respective embodiments of Shia and Sunni fundamentalisms clearly means that Iran cannot leave its most prized pet in the lurch.[87] In the Iranian mind, the ISIS advance on Lebanon is proof of the alliance between the U.S., Zionism, and Salafism. Dictatorship in Syria is Iran's best bet, as a Sunni-led democracy will not be as amenable to Iranian interests. In this perspective, the ISIS horror and the consequent softening of western attitudes towards Assad and coalition airstrikes against jihadist targets is a disguised victory for the Iranian position in the region.

The Future of the Region

In pursuit of the narrow ambitions of their respective political and religious establishments, both Iran and Saudi Arabia seem to have been blinded to the fact that there exists a common enemy: Salafi jihad, especially as embodied by ISIS. Whereas the Shias of the world and the greatest bastion of Shi'ism in Iran remain the Salafists' avowed targets for destruction, the downfall of the House of Saud ranks high up on the jihadist agenda in the course of the establishment of a true Islamic caliphate. This factor alone should have provided adequate rationale for Saudi-Iranian cooperation at some level in order to root out extremism from the region. Rationality invariably fails in the face of a religion-fueled politics; perhaps it is time for both regional powers to reassess their individual strategies in the conflict zones.

In a society as fractured as present-day Iraq, democracy and federalism are the only logical ways forward. The top-down democracy introduced by the U.S. post-Saddam did empower the long-suppressed Shias, but, in the absence of a meaningful federal component, sowed the seeds of Sunni alienation.[88] It is clearly discernible from the course of events since 2003 that the leading role of the Shias in Iraqi politics is an irreversible phenomenon. Saudi Arabia should respect the fact that the Shia-led government in Iraq is here to stay. Furthermore, perpetual instability in Iraq may

86 Jack Moore, "Hezbollah and Isis clash in first-ever battle," *Newsweek* (2015), Accessed June 13, 2015. http://europe.newsweek.com/hezbollah-isis-clash-first-ever-battle-328519

87 Matthew Levitt, "Hezbollah's Syrian Quagmire," *The Washington Institute* (2014), Accessed June 13, 2015. http://www.washingtoninstitute.org/policy-analysis/view/hezbollahs-syrian-quagmire

88 Joost Hiltermann, Sean Kane, and Raad AlKadiri, "Iraq's Federalism Quandary," *International Crisis Group (*2012), Accessed July 9, 2015. http://www.crisisgroup.org/en/regions/middle-east-north-africa/iraq-iran-gulf/iraq/op-eds/hiltermann-iraqs-federalism-quandary.aspx

suit Israeli interests as a means of keeping Iran occupied, but it has become a clear and present danger to American policies and the House of Saud itself.

The Iraqi Shias are not mere Iranian proxies, as demonstrated in their successful resistance to the Iranian model of clerical rule and their willing participation in electoral democracy. On the other hand, Iraqi Shias' desire to have close relations with Iran is natural for obvious reasons. The ISIS scourge has greatly enhanced Iranian influence in Iraq. Iran is the only ally willing to actively fight the Takfiri onslaught as the Iraqi army crumbles, and the U.S. is reluctant to send combat troops against ISIS. The resulting Iraqi reliance on Shia militias to fight off ISIS has further polarized society and propels the Sunni tribes towards cooperation with ISIS. This vicious cycle in Iraq needs to be broken. The Saudis must use their networks of influence with the Sunni tribes to form a Sunni tribal coalition against ISIS. In addition, they should lobby the U.S. to exert pressure on Iraq for a federal structure of government and more inclusive state and military apparatuses. Failing that, Iranian influence in Iraq is only set to increase as it claims to occupy the moral high ground in the fight against ISIS.

In Syria, where the sheer number of actors in the combat theatre prohibits any reasonable analysis of the general direction of the civil war, both Saudi Arabia and Iran are going by their standard playbooks. Hardcore Salafi jihadists of Al-Nusra and the Islamic Front have united in 2015 under Saudi and Turkish aegis to form Jaish Al-Fatah (Conquest Front) against Assad.[89] On the regime's side, Iran's Lebanese proxy Hezbollah has joined in full force with Syria's minorities and seculars, desperately clinging on to Assad as the palatable alternative to Sunni fundamentalism. Meanwhile, the entire Eastern part of Syria has been effectively ceded to ISIS to experiment with its grisly statehood, except for pockets of heroic Kurdish resistance aided by U.S.-led coalition airstrikes.

Whereas the Obama administration seems to have realized the risks inherent in funding and arming the Syrian opposition, the Saudis perceive this as a lack of commitment on the part of the U.S. Saudi Arabia is also agog at the prospect of a U.S.-Iran nuclear deal. Though 53% of Saudis perceive Iran to be its "principal enemy," with only 22% identifying ISIS, the country has experienced an unprecedented thaw in its relations with Israel.[90] In the context of the larger Muslim world, this may cause

89 Derek Davison, "Saudi Arabia and Turkey Rejoin Hands in Syria," *Common Dreams* (2015), Accessed July 9, 2015. http://www.commondreams.org/views/2015/05/09/saudi-arabia-and-turkey-rejoin-hands-syria

90 "The new frenemies," *The Economist* (2015), Accessed July 9, 2015. http://www.economist.

a loss of prestige for the Saudis as Iran and Hezbollah capitalize on their reputation as dogged fighters against the Jewish nation. In the Syrian context, Iran will stick by Assad as its sole toehold of influence in the country. In the current circumstances, however, the fall of Assad will quickly translate into a victory for Islamists, be they the Jaish Al-Fatah or ISIS. The Saudi bloc may at this time feel that they will be able to control their Salafi clients in the future, but the lessons of Afghanistan and Iraq must not be forgotten. In an ideal situation, the U.S., Saudi Arabia, and Iran would cooperate to negotiate Assad's departure and the installation of a national unity government in Syria that then takes on the fight against extremists. In a more pragmatic, lesser-of-all-evils calculation, however, the U.S. should recognize and impress upon its regional allies that for the time being, Assad may be the best bet in ground combat against ISIS and other extremist outfits. Assad is just one party to the atrocities in Syria, not the sole perpetrator, and the U.S. has a long history of necessity-driven cooperation with dictators.[91]

Conclusion

The best-case scenario for the Middle East will materialize if Saudi Arabia and Iran set aside all other concerns to jointly counter Salafi extremism, which is an existential threat to both. However, the deep investment of both powers in the opposing sides of the conflict renders this ideal solution highly unrealistic. It is symptomatic of the malaise of religious extremism that a negotiated settlement between belligerents is not an option. Therefore, since major ground offensives, and not airstrikes alone, are needed to dislodge the pernicious hold of extremist organizations like ISIS over large populations and wide swathes of territory, without such cooperation the Middle East may continue to writhe in fire and blood for the foreseeable future.

---

com/news/middle-east-and-africa/21654070-shared-interests-have-brought-israel-and-arab-world-closer-now-new

91 John Mueller, "To Fight ISIS, Leave Assad in Power," *Time Inc* (2015), Accessed November 20, 2015. http://time.com/4116371/paris-attacks-fighting-isis/

Why Government Organizations Don't Care: Perverse Incentives and an Analysis of the OPM Hack

James Twist, Matthew Hutchison, Blake Rhoades, Ryan Gagnon

Many security experts have addressed the financial and personal security risks involved with the recent data breach at the Office of Personnel Management (OPM). This work supplements previous analyses of the event, and explores how the recently disclosed OPM breach has impacted the national security of the United States. By examining the elements of the breach - within the context of the stolen data and linkages to other data breaches - this work points to a larger offensive cyber campaign as the primary concern for U.S. leaders and policy makers. After thoroughly examining the details of the attack itself and its implications on DoD and national cybersecurity, we argue that government organizations lack appropriate incentives to secure their networks and personal data. The solution to this problem lies with organizational leaders, who must give guidance that incentivizes information security at the "tactical level."

Introduction

After General Benedict Arnold's traitorous maneuver to deliver West Point into the hands of the British in 1780, General George Washington wrote a letter to the post's new commander for the purpose of instilling a sense of urgency in his subordinate. In the letter, Washington's instructions were clear and direct:

> The enemy will have acquired from General Arnold a perfect knowledge of the defenses, and will be able to take their measures with the utmost precision. This makes it essential our vigilance and care should be redoubled for its preservation. You will do everything in your power to gain information of the Enemy's designs and give me intelligence as early as possible of any movement against you.[1]

1 General George Washington's September 1780 correspondence to West Point Commander. Archives. United States Military Academy, West Point, NY.

At the time, Washington considered West Point to be the most strategically significant position in America. Placed at a western point of the Hudson River, this garrison was the only American point of defense between New York City and Canada. The enemy's "perfect knowledge" gained through Benedict Arnold had grave implications for the future success of the continental army. Luckily for Americans, General Washington had the foresight to encourage his subordinate commander to take all provisions necessary to secure this strategic terrain.

Our nation once again finds itself in an equally perilous position. In the wake of the recent Office of Personnel Management (OPM) intrusion and data breach, the forewarnings given in Washington's letter remain prescient. The revelation that digital records associated with over 20 million government employee were stolen from OPM by presumed foreign government affiliated hackers has undermined our nation's national security structure and compromised key digital terrain. Now infamously known as the world's largest known data breach, the OPM breach places national leaders at a critical decision point for how we conduct cyber defense in the future. As Washington implored in 1780, we must now re-double our efforts to mitigate the enemy's ability to exploit its newfound knowledge.

Overview

The stolen OPM data is useful for a variety of purposes to a diverse group of adversaries. For advanced persistent threats, this vast treasure of information and data provide the means to undermine, subvert, or neutralize American national security protections. The files could easily be shared amongst several nation states or, via proxies, with criminal enterprises. Its utility ranges from intelligence applications to identity theft and facilitation of focused computer network operations. Numerous subsets of individuals are vulnerable from the compromise of this data including senior leaders, intelligence personnel, military service-members, government civilians, and family members. The sheer volume of people affected implies the problem is of massive scope which impacts our government as a collective whole. The true value of the stolen data is the authenticity, specialized nature, and years required for its compilation. The only constraints for its application and usage in military and intelligence missions is the creativity of our adversaries who now possess it in its entirety.

In this paper, we examine the OPM breach, the evidence left behind by

the attackers, and examine historical case studies to draw conclusions about the event's impact on the government community and our national security at large. Unfortunately very few political scientists are addressing this issue and policy makers are only now beginning to understand that cyber warfare has become a weapon of choice against the US government.[2] The protracted campaign to degrade or neutralize US national power is becoming more and more evident with attacks like that against OPM.[3] Collectively, these events undermine the government's mandate to secure our nation in cyberspace and to preserve our strategic power abroad. In order to disrupt the ongoing campaign, we argue that policy makers and national leaders must focus on dismantling the lax cybersecurity that plagues the government's networks. This focus starts by holding organizational leaders and commanders responsible for the security of their own networks.

Attack Description

This section of the paper describes the adversary's systematic approach to breaching OPM networks. The attack – which has now been notoriously deemed the world's largest known data breach - likely began as a series of network intrusions occurring as early as 2013 and enduring until the spring of 2015. Over that time period, apparent nation-state hackers took advantage of OPM's poor security posture (and it's poorly monitored relationships with third parties) to steal data that contained a massive amount of information about government employees, family members, affiliated contractors, and prospective government hires (see Annex A).

The public first became aware of the attacks began in July of 2014, when the New York Times publically disclosed that OPM had suffered a systems breach during the spring of that year.[4] According to OPM, the agency had not disclosed the attack to the public because it had completed a security review of its systems – one wherein the agency incorrectly assessed that they had stopped the attacks with appropriate countermeasures – and, more importantly, that no Personally Identifiable Information (PII) had been compromised. As was revealed by the

2 Frates, Chris. "Government Hacks and Security Breaches Skyrocket - CNNPolitics.com." *CNN*. Cable News Network, 19 Dec. 2014. Web. 28 Sept. 2015.

3 Other events include the WikiLeaks scandal, the Snowden Affair, multiple penetrations of our networks by Russian APTs, and directly relevant to this case, the vast pilfering of technology and defense contractor data compromising some our most sensitive military equipment. (See "Why the cyberwar is dangerous for democracies.") http://www.theatlantic.com/international/archive/2015/06/hackers-cyber-china-russia/396812/)

4 Schmidt, Michael, David Sanger, and Nicole Perlroth. "Chinese Hackers Pursue Key Data on U.S. Workers." The New York Times. July 9, 2014. Accessed July 2, 2015.

agency in June 2015, however, the attacks persisted well into the spring of 2015 and were only discovered while OPM was upgrading its security systems. During this discovery period in the spring and summer of 2015, investigators found that multiple attacks had occurred against OPM data servers and that the attackers had gained access to personnel files. While OPM initially suspected four million persons had been affected, they later updated that number to an astounding 22 million.[5]

The hackers likely gained access to OPM systems by exploiting its business relationships with third party contractors. According to security experts and well known cybersecurity firms, the hackers gained access to OPM's networks through carefully crafted phishing attacks against OPM and its partners.[6] Of note, OPM partners USIS and Keypoint were both breached by hackers preceding and during the OPM attacks, thus experts believe the hackers used third-party issued credentials to gain initial access to the systems. In addition to the phishing attacks, security researchers at ThreatConnect identified that the malicious site opm-learning.org was potentially used by the hackers as a secondary means of installing malware and maintaining access to the OPM network.[7] [8]

Multiple sources agree that the attackers then gained persistence on the OPM network by installing an exploit toolkit known as Sakula.[9] Using this sophisticated malware, the attackers were able to ex-filtrate government employee information from the OPM servers through their attack infrastructure, specifically the malicious domain opmsecurity.org. Using the "diamond-model of intrusion analysis,"[10] CrowdStrike and Mandiant have assessed with a high degree of confidence that the attack was perpetrated by Chinese APTs.[11] While the two firms disagree on the attribution of the attack to any specific APT group, they use their proprietary

5 Bisson, David. "The OPM Breach: Timeline of a Hack." The State of Security. June 29, 2015. Accessed July 2, 2015. http://www.tripwire.com/state-of-security/security-data-protection/cyber-security/the-opm-breach-timeline-of-a-hack/.

6 Phishing is an extremely common hacking method where an adversary attempts to gain access to systems through carefully crafted emails that are meant to fool individuals into relaying their usernames and passwords to those systems or by having them install malware, among other strategies.

7 Sakula malware utilizes Dynamic Link Library (DLL) associated with *PlugX* activity to conceal itself from its targets.

8 "OPM Breach Analysis: Update - ThreatConnect | Enterprise Threat Intelligence Platform." ThreatConnect Enterprise Threat Intelligence Platform RSS2. ThreatConnect, 9 June 2015. Web. 21 Aug. 2015. http://www.threatconnect.com/opm-breach-analysis-update/.

9 Ibid

10 Sergio Caltagirone, Christopher Betz, and Andrew Pendergast. "The Diamond Model of Intrusion Analysis." *Dtic.mil*. US Government, 2013. Web. 28 Aug. 2015

11 "Chinese Hackers Violated Systems at the Office of Personnel Management." *Security Affairs*. 11 July 2014. Web. 21 Aug. 2015

network monitoring and data analytics platform to identify several technical characteristics that support their analysis.

The OPM data breach was more than a singular event or a series of unrelated singular events; it was a protracted and thoughtful campaign by an adversary with a deliberate target. Using Lockheed Martin's "cyber Kill-Chain" methodology (see Annex B), we find that OPM's networks were under persistent reconnaissance and penetration for a period of time that spanned years. The individual events that led to the data breach were a part of a collective campaign against OPM and its partner organizations that went unnoticed by OPM Information Technology specialists. While OPM was quick to dismiss early attacks after the onset of the first breach that was revealed to the public in July of 2014, it becomes clear the initial events were a smaller part of a much larger campaign. The OPM IT team – with its small analytical capacity and limited capabilities – did not take a strategic view of what the adversary might be attempting to do during its initial breach.[12] In the face of an advanced persistent threat that is routinely probing our government systems, we cannot afford to take such a lax approach. In today's highly networked world, leaders must place emphasis –in the form of leadership direction and focus, policy, budgets and hiring – on cybersecurity as a priority for their organizations.

Protective Measures and Actions Taken by OPM

As we learn more about OPM's poorly defended networks, it becomes evident that the hackers need not have relied upon *advanced* tactics to infiltrate OPM's network; the security of the networks was lacking to a point the adversary could have relied upon basic methods and elementary tactics to be successful in their campaign. The November 2014 OPM Inspector General Report shows the agency's poor security program left OPM vulnerable to cyber-attacks in many areas and seemed to invite the catastrophe that would be revealed in the summer of 2015. As the data and case studies presented in this paper show, a culture of tolerance for negligent network security was the primary culprit that led to breach.

The intrusions and subsequent data theft were made possible by a

12 As will be demonstrated in subsequent sections of this paper, OPM's small information technology team did not have the resources and personnel that would have been necessary to detect what we now know what a persistent campaign against its networks. Due to its limited budget and small size, the OPM IT team tended to view intrusion events in and around its networks as stove-piped instances that had no connection to one another. Ultimately, this mentality would be proven tragically false and would lead to the world's largest known data breach.

fundamentally flawed approach to cybersecurity at OPM. As early as 2007, the OPM Inspector General (IG) identified agency security practices as a "material weakness" to national security, yet the agency did not hire its first professional IT staff until 2013.[13] By 2014, the agency had hired only seven IT staff members, with only four more in its training pipeline[14]. As of November 2014, the IG noted that OPM had failed to routinely audit its systems and that the agency had no understanding of what machines were or should be connected to its network; they had no list of servers, databases, or network devices.[15]

The apathy of OPM leadership is most obviously displayed in the organization's lack of focus on cybersecurity resources, processes, and a complete lack of a unified effort to defend its networks. OPM failed to adequately monitor its network for even the most benign of security threats and, as the annual IG reports show, the agency's IT staff had no sophisticated methodologies for identifying APT activity. As the agency dismissed earlier instructions from its IG to harden its networks, its adversaries reinvigorated their efforts to penetrate OPM networks and simply found other ways in. Because OPM lacked basic cybersecurity tools and capacity for analysis – such as the "Diamond Model" or the well-known "Kill-Chain" methodology – it had no hope for identifying the presence of an ongoing campaign against its systems.

The 2014 OPM Inspector General Report shows that basic protocols and standards for protecting the information were not followed by government employees. Seven systems out of twenty-five had inadequate documentation of security testing, four of which were directly maintained by OPM's IT department. In 2013, it was confirmed that hackers had stolen the Cold Fusion source code from Adobe, making it susceptible to reverse engineering attacks. Contrary to reasonable security practices, the OPM system administrator continued to use Cold Fusion in conjunction with outdated Operating Systems such as Windows XP. The report also found that many core systems that hadn't been updated since Y2K.[16] Additionally,

13 "OPM 2013 IG Report." *Opm.gov*. US Government. Web. 21 Aug. 2015.

14 Gallagher, Sean. "Why the "biggest Government Hack Ever" Got past the Feds." *Security and Hacktivism*. Arstechnica, 8 June 2015. Web. 21 Aug. 2015. http://arstechnica.com/security/2015/06/why-the-biggest-government-hack-ever-got-past-opm-dhs-and-nsa/.

15 Gallagher, Sean. ""EPIC" Fail—how OPM Hackers Tapped the Mother Lode of Espionage Data." Security and Hacktivism. Arstechnica, 21 June 2015. Web. 17 Aug. 2015. http://arstechnica.com/security/2015/06/epic-fail-how-opm-hackers-tapped-the-mother-lode-of-espionage-data/.

16 Urrico, Roy. "OPM's Weak Security Led to Breach: Report." *OPM's Weak Security Led to Breach: Report*. Credit Union Times, 23 July 2015. Web. 21 Aug. 2015. http://www.cutimes.

due to the lack of realistic threat simulation by red-team tests and penetration attacks, the OPM networks were virtually defenseless when facing a real-life threat.[11] The IG report also showed that OPM failed to maintain accountability of its systems, and lacked procedures to enforce corrective measures for deficient and insecure systems.

As was indicated in the IG report, OPM did not encrypt its databases that contained large amounts of government employee information. OPM attributes the lack of encryption standards to "old" hardware and low budgets, yet federal PII standards require the protection of social security numbers, fingerprints, and other information - all of which were present on OPM servers.[17] Although OPM was in the process of implementing two-factor authentication (Common Access Card (CAC) and Personal Identification Number (PIN)), none of their systems were using this security feature at the time of the attack.[18] In the House Committee on Oversight and Government Reform hearing after the attack, OPM chief information officer Donna Seymour lamented on the difficulties of securing OPM's networks: "A lot of our systems are aged. […] Implementing [security] tools take time, and some of them we cannot implement in our current environment."[19] Seymour's defense is unacceptable and a fundamentally flawed approach towards securing government systems. Her logic shows the agency did not prioritize cybersecurity as a part of the agency's mission, and did not take steps necessary to overcome resource obstacles in order to prevent data breaches compromising US national security.

OPM was successfully attacked despite having DHS "Einstein" network monitoring sensors in place. While some speculate the sensors eventually detected the 2015 attacks, evidence shows that they initially failed to detect intrusions into the network due to Einstein's reactive nature and inability to evolve to dynamic threats.[20] Even if Einstein was more dynamic, most security experts agree that even

com/2015/07/23/opms-weak-security-led-to-breach-report.

17 Perera, David. "Office of Personnel Management Didn't Encrypt Feds' Data Hacked by Chinese." Cybersecurity. Politico, 4 June 2015. Web. 17 Aug. 2015. http://www.politico.com/story/2015/06/personal-data-of-4-million-federal-employees-hacked-118655.html.

18 Norton, Steven, and Clint Boulton. "Years of Tech Mismanagement Led to OPM Breach, Resignation of Chief." The CIO Report RSS. The Wall Street Journal, 10 July 2015. Web. 17 Aug. 2015. http://blogs.wsj.com/cio/2015/07/10/years-of-tech-mismanagement-led-to-opm-breach-resignation-of-chief/.

19 Boyd, Aaron. "OPM Breach a Failure on Encryption, Detection." *Federal Times*. 22 June 2015. Web. 4 Sept. 2015. http://www.federaltimes.com/story/government/omr/opm-cyber-report/2015/06/19/opm-breach-encryption/28985237/.

20 Unfortunately, the current version of Einstein has proven to only be useful for post-attack remediation. This is due to the fact that only known threats are uploaded to Einstein, which

dynamic intrusion prevention systems fail from time to time and must be heavily managed by qualified security personnel. While security technology is helpful in identifying adversarial behavior on networks, it cannot be seen as definitive solution for security networks. Given the advanced and persistent nature of cyber threats, organizations cannot rely solely upon national cybersecurity constructs as a plausible line of defense against cyber intrusions.

While DHS plays a role in protecting and coordinating defensive actions across the many organization's that comprise the government bureaucracy, this paper argues that each organization must have the capability to conducts its own threat analysis. If the government wishes to prevent events such as this from happening again, high speed and high tech security measures coupled with adequately trained IT staff must be implemented at all levels and for all organizations. This will allow leaders to detect and prevent known threats as well as to defend against unknown threats and react with agility upon discovery of new methods or advanced malware signatures. Each organization must be prepared to support its own cybersecurity at the tactical and operational levels while expecting DHS to provide strategic resources and support. Given its apparent reliance upon Einstein as its primary network security mechanism, it appears that OPM was too reliant upon DHS for cybersecurity and did not take ownership of its networks.

Despite the vast technical issues, the main failings of OPM do not lie in its legacy systems or inadequate security tools, but rather in its failure to enforce government IT policy and implement a supportive budget or hire skilled professionals to administer its system. This reflects the priority given to information security and protecting valuable data by OPM leaders. Even the best security tools and technologies are inert without trained and competent personnel. What's more, those personnel must be empowered through policy and leadership to secure networks and implement technological solutions as required. The post-incident response to the event also indicates an absence of effective policy, planning, and leadership throughout the remediation process. As a result, the fallout from the breach may actually increase due to poor post-incident response by the agency. To date – over three months after publically disclosing the breach – the agency has failed to notify the majority of the 22 million individuals who were affected by the breach.[21] In the

then inspects network traffic for all instances of threats that look like any other threat it has "learned" about; the current capability is not self-learning or dynamic enough to adopt to current threats.

21 McAllister, Niel. "Victims of US Gov't Mega-breach Still Haven't Been Notified." • *The*

absence of notification, government employees may get a false sense of security and assume that their data has not been compromised. As a result, the government employees effected may fail to take appropriate mitigation measures which could have limited the overall impact to the collective organization. Once again, such missteps by OPM indicate systemic issues with its security program's management; the lack of a post-incident response plan further detracts from the confidence in the US government's ability to secure its networks.

During the 2015 Black Hat conference, a new cybersecurity mantra, "if you can't protect it, don't collect it," emerged to reinforce norms that sensitive data should not be collected and stored if leaders or organizations are not willing or capable of allocating resources for information security.[22] [23] What's makes OPM's case tragic, is that a simple risk assessment and prioritization of resources to mitigate threats could have overcome their deficiencies; this is the responsibility of a leader in a government organization. In the case of OPM, the agency should not have stored PII unless it had the willingness and resources to protect such data, which – as we now clearly see – compromised national security. As leaders of a government agency with such a critical mission, Seymour – and Director of OPM, Katherine Archuleta - failed as leaders because (1) they did not prioritize cyber defense of its systems, (2) rectify resources deficiencies to support cyber defense, or (3) segregate the data of importance from the network.

Linkages to Other Events

Because of OPM's failure to defend its networks and respond appropriately to the breach, some in the cybersecurity community have downplayed the importance of focusing on the actors behind the attacks and instead called for an emphasis on cybersecurity "lessons learned" that will prevent future failures by the government. This paper argues that consideration of both are equally important. While the failure of OPM to secure its network is a natural point of focus, it is essential that we in the security community examine the strategic implications behind this attack as well. The previous portion of the paper focused on lesson's learned, and this portion focuses on the strategic context of the OPM attack. Initial indications from

Register. 2 Sept. 2015. Web. 4 Sept. 2015. http://www.theregister.co.uk/2015/09/02/opm_data_breach_notices

22 Black Hat is a seminal security and hacking conference that occurs each year in Las Vegas.

23 Bejtlich, Richard. "New Cybersecurity Mantra." *The Brookings Institution*. 3 Sept. 2015. Web. 28 Sept. 2015.

two well-known security firms, Mandiant and CrowdStrike, indicate that the OPM hackers were using Tactics, Techniques, Procedures (TTPs) similar to those of known Advanced Persistent Threats (APT) and have been attributed to previous attacks. The OPM breach is far from unique: over the last 5 years, there have been breaches of organizations that either shared the same TTPs as the OPM hackers, or have had related targets (i.e., the USIS/Keypoint breaches). By analyzing and comparing the data from these previous breaches, patterns can be established that shed light not only on how the hackers accessed these systems but also why. Once again, the Diamond model is a useful model to shape analysis and identify linkages between multiple events (see Annex B and C for ACI TAC interpretation of the data). [24]

The first attack we examine is against a firm with a long standing relationship with the US government. An organization formerly known as the United States Investigative Service, USIS – a contracted associate of OPM, which had been responsible for conducting government security clearance investigations since the late 1990s. Their contract was terminated following the discovery of a recent data breach. The USIS compromise started in April 2013 and was discovered in June 2014. During this period, approximately 25,000 personnel records were stolen. Although this number is large, the most important data that was stolen was not the records but rather the blueprints and information behind the structure of OPM's networks. The breach was linked to China, yet experts cannot pinpoint an exact origin. This intrusion was largely blamed on USIS's lack of network security. The government ironically sued USIS for its network security failures (in addition to its negligence that enabled Edward Snowden and Aaron Alexis to receive security clearances). In September of 2014, OPM cut ties with USIS and switched to another security contractor, Keypoint[25].

The Keypoint breach started prior to its relationship with OPM. While OPM attempted to secure its networks by switching service providers and "cutting off" access to USIS, it was instead contracting with another compromised associate. In total, about 48,000 personnel files were stolen, which is thought to have occurred during the timeframe from December 2013 to September 2014. While few details

24 "Methodology - ThreatConnect | Enterprise Threat Intelligence Platform." *ThreatConnect Enterprise Threat Intelligence Platform*. Web. 18 Oct. 2015.

25 Bisson, David. "The OPM Breach: Timeline of a Hack." The State of Security. Tripwire, 29 June 2015. Web. 17 Aug. 2015. http://www.tripwire.com/state-of-security/security-data-protection/cyber-security/the-opm-breach-timeline-of-a-hack/.

were given to the public about this initial compromise, Keypoint did publically disclose that a second breach occurred; the announcement was made in the aftermath of the 2015 OPM breach disclosure. This second breach included as many as 390,000 stolen files. [26]

A third attack against Anthem – an insurance provider that services government employees – is another significant event that shares some similarity with the OPM attack. This attack started in December 2014 and was discovered January 29th, 2015. The attacks on Anthem targeted information that specifically dealt with government employees and their PII.[27] Overall, 80 million customers were affected. Consistent with the OPM data breach, there is little evidence that the data stolen from Anthem has been used for financial fraud.[28] Also, both the OPM and Anthem breaches used stolen certificates from a Korean software company known as DTOPTOOLZ Co. in order to gain access to the compromised systems.[29] In fact, the methodology in which the attacks were carried out were almost identical, probably, by design rather than coincidence. In both instances the Sakula malware family was used, and in both instances a Command and Control, or C2, node was created with a fake domain name that mimicked actual domain names. Because Anthem was called WellPoint at the time, the breach used the fake domain name "we11point.com" with "1's" - instead of "l's"- in order to disguise itself as regular network traffic, just as the OPM breach used opmsecurity.org and opm-learning.org.[30]

Theses similarities point to an advanced, persistent attack aiming at a clear target, indicating that both OPM and Anthem were victims of calculated focus rather than opportunity.[31] Deliberate efforts to infiltrate government networks and its third party affiliates are indications of an ongoing campaign against the US. Subsequent portions of the paper will focus on trends in those various campaigns and the impact such efforts will have upon the US government and its national security.

The difficulty of attack attribution does not diminish the responsibility of examining the larger picture; as our study will demonstrate, the OPM breach is likely

26 Ibid.
27 "How to Access & Sign Up For Identity Theft Repair & Credit Monitoring Services." Anthem, 8 May 2015. Web. 17 Aug. 2015.
28 Threatconnect Intelligence Research Team. "The Anthem Hack: All Roads Lead to China." ThreatConnect Enterprise Threat Intelligence Platform RSS2. Threatconnect, 27 Feb. 2015. Web. 17 Aug. 2015. http://www.threatconnect.com/the-anthem-hack-all-roads-lead-to-china/.
29 Ibid.
30 Ibid.
31 Ibid.

the next phase of a much larger effort that seeks to undermine the US government's cybersecurity and national power. We expect the data obtained through the OPM breach could be used to shape the environment for future operations. Given this significance, it is important to examine the linkages between the OPM breach and similar attacks.

Usage for Stolen Data

Given the magnitude and comprehensive nature of data ex-filtrated from the OPM servers, there exist two broad categories of malicious usage for the data that affect government employees:

1. ***Illicit Financial Gains and Identity Theft*** - As has been noted above, PII data holds enormous value due to its fixed nature. While credit cards can be deactivated and replaced, social security numbers and biometrics data cannot be changed. Because of such properties, PII is highly valued on various darknet marketplaces; PII data substantiates an underground multi-million dollar criminal industry.[32] Because of the lucrative financial incentives involved, the first obvious use of this information to any common criminal would be to either sell the personal information on the deep web or exploit the personal information for financial gain through credit card fraud. However, if the Chinese government has the information, there are many more possibilities for what could be done with the data. We will elaborate on these possibilities below.

2. ***Espionage and Exploitation by Chinese Government*** - The stolen data is also thought to be of tremendous value for foreign espionage purposes. The Chinese government, for instance, allegedly uses such information and knowledge to support its attempt to recruit and/or blackmail American government workers. By using each piece of PII - as well as "big data" analytics and statistical approaches– the Chinese government can identify potential "weaknesses" or employees that may be susceptible to manipulation due to financial problems, medical problems, or other vulnerabilities to exploitation or subversion. The information could also be used to blackmail employees about embarrassing relationships or other personal information that they would not want exposed. Moreover, the TTPs that link the OPM attacks to its contractors and to Anthem strengthen the argument that the OPM attack was part of a larger campaign against government personnel, not an isolated event. The hypothesis of data being used for intelligence value is supported by fact that the data associated with all of the collective events has the common link of being associated to government individuals

32 From http://searchnetworking.techtarget.com/definition/darknet : "A darknet is a routed allocation of IP address space that is not discoverable by any usual means. The term is used to refer to both a single private network and the collective portion of Internet address space that has been configured in that manner."

An article published in the Los Angeles Times confirms that the stolen OPM data is already being used for espionage purposes:

> Foreign spy services, especially in China and Russia, are aggressively aggregating and cross-indexing hacked U.S. computer databases – including security clearance applications, airline records and medical insurance forms – to identify U.S. intelligence officers and agents.[33]

We assess the most important application of the data will facilitate additional offensive cyberspace operations and support numerous and various intelligence operations. Given the ease with which the data can be reproduced, it is likely the data will be used to achieve multiple ends. It is possible the hackers serve both national and criminal interests, and are willing to resell the data for multiple uses (both espionage and criminal activity). Diverse usage of the data would lend support to the Chinese government's "plausible deniability", as it easily refutes its involvement if the data were to manifest within the dark net. For these reasons, employees should assume their data will be used to support both espionage and fraud. Evidence gathered by the authors indicate that on some level, issues with criminal fraud and ID theft are already being experienced by small numbers of US Government employees.[34]

Perverse Incentives: Why Public Organizations Don't Care About Security

In order to better understand the dynamics behind the government's failing to secure its data, this section explores incentives that motivate data loss protection (DLP) in the private sector and compares them to the incentives towards DLP in the public sector. In both the public and private sector, organizations are responsive to incentives that drive decision making. Because private and public organizations are motivated by different incentives, their behavior is often distinct when it comes to cybersecurity. In the private sector, these incentives consist of market forces that drive firms towards profit, while the public sector incentives occur in various other forms.

In an October 2014, David Chavern, the United States Chamber of Commerce President of the Center for Advanced Technology and Innovation warned of the

33 Bennet, Brian, and AJ Hennigan. "China and Russia Are Using Hacked Data to Target U.S. Spies, Officials Say." Los Angeles Times. Los Angeles Times, 31 Aug. 2015. Web. 2 Sept. 2015.

34 King, James. "Stolen Data On Federal Workers Is Worth $140 Million." *Vocativ*. Web. 18 Oct. 2015.

startling difference between commercial collection of data and government collection of data.[35] Chavern recounts that the government has been quick to scorn companies for aggregating data on individuals at the possible cost of breaching their privacy, but has made no statements about the government's own programs and systems used to maintain similar datasets. Most commercial data collection has some mechanism for "opting out", however, the government has provided no clear guidelines for how to opt-out of its collection programs. More exacerbating is the government may be less motivated to increase data security as threats become increasingly sophisticated.

The 2011 Ponemon study, "The True Cost of Compliance" surveyed a set of organizations to determine how the costs for achieving and maintaining information security compliance compared to the costs of handling a data breach in association with noncompliance. The study found that costs for noncompliance are at least 2.65 more expensive than simply spending the required money to achieve baseline cybersecurity standards.[36] Furthermore, the fact that applicable laws and regulations are the number one motivator for organizations to place importance on compliance efforts is concerning.[37] Sarbanes-Oxley and Payment Card Industry (PCI) standards are in large part responsible for expediting the securing and auditing of security compliance at many organizations in the study. It is unclear whether any of these regulations apply to government organizations, and what punitive measures are possible for failure to comply.

In a common data loss case study involving ChoicePoint Inc., a 2005 data breach of public record aggregation and marketing data on thousands of consumers drew backlash from the federal government.[38] The loss of thousands of aggregated personal information profiles caused much of the current privacy debate to begin and caused state legislatures to begin introducing privacy laws nationwide.[39] The language used by US Congressional Representatives in a Hearing on Protecting Consumer Data as part of the 109th Congress, in the Committee on Energy and

35 Chavern, David. "The Power of Big Data." The Power of Big Data. October 16, 2014. Accessed August 11, 2015. https://www.uschamber.com/above-the-fold/the-power-big-data.
36 Ponemon Institute. "The True Cost of Compliance." January 2011.
37 Ponemon Institute.
38 Brodkin, Jon. "ChoicePoint Details Data Breach Lessons." PCWorld. June 10, 2007. Accessed August 14, 2015. http://www.pcworld.com/article/132795/article.html.
39 Sullivan, Bob. "ChoicePoint CEO Grilled by Congress." Msnbc.com. March 15, 2005. Accessed August 14, 2015. http://www.nbcnews.com/id/7189143/ns/technology_and_science-security/t/choicepoint-ceo-grilled-congress/#.Vc32ThRjZQI.

Commerce, is very significant to today's issues.[40] In Congressional testimony given by ChoicePoint legal staff and executives, Congress pointedly remarks that ChoicePoint was responsible for their buying, selling, and failing to protect customer data. In hindsight, it is evident that in many of the legal regulations of which ChoicePoint was noncompliant, federal agencies may also still be non-compliant. In fact, the hearing brought to light many data protection and privacy provisions under the Sarbanes-Oxley (SOX) and Gramm-Leach-Bliley Acts (GBLA) that require security standards under Securities and Exchange Commission (SEC) or Federal Trade Commission (FTC) regulations.[41] These data protection laws and regulations are relevant because according to a 2011 Ponemon data breach study, these laws were the most important corporate reason for a company to spend money on data security.

While the government's response to ChoicePoint was quick to denigrate their lack of data protection and privacy standards, it is unclear what the fallout will be for the loss of so much personal data in the OPM data breach. Furthermore, customers doing business with ChoicePoint had the option to choose other data providers in order to allow market forces to work on the data security expectations of the data compilation industry. OPM, on the other hand, was in the business of acquiring, storing, and managing employee data on millions of Americans, but had no market incentive to innovate and become more secure. Furthermore, it is unclear what federal regulations that apply to publicly traded companies also apply to government agencies as well. The data lost in the OPM data breach was far more extensive and personal in nature than any other breach to date. While other data breaches (ChoicePoint, Target, Home Depot, etc.) may have had financial effects on consumers and the economy, it remains unclear what damages will occur from the loss of OPM data, which included polygraph data, Standard Form 86 (SF-86) documents, and known associates and references for federal employees that underwent a security investigation.

When a major network intrusion to the extent of OPM occurs, incident responders may be able to quickly remediate the vulnerability that allowed unauthorized access and the loss of data. What is not known is if the intruder, while in the network, was able to insert other vulnerabilities such as malicious software or false credentials

40 Protecting Consumers' Data: Policy Issues Raised by ChoicePoint. Hearing before the Committee on Energy and Commerce, United States House of Representatives, 109th Cong. (2005).

41 Ibid

that could allow them re-entry even after the detected security flaws are corrected. A major step in an incident response is containment. In the case of total network compromise, it may take a long time before the network can be considered secure enough to resume normal operation and to fully trust that the data will not be lost again shortly after services are restored.[42] Given the comprehensive nature of the required response, organizations must be prepared to invest significant resources into the remediation of a cybersecurity event.

According to one security blog, suffering a major data breach "is like having a financial bomb go off in your company."[43] The cost cannot only be in loss of customer loyalty, but in legal and regulatory penalties, as well as costs for cleaning up after the breach. While it is certain that OPM is paying a financial cost at the expense of the federal budget, their primary objective is not to make profits and therefore financial damages will not help to fundamentally change the cybersecurity culture of the agency. Rather, the effects of the data lost by OPM to nation-state adversaries should cause all federal agencies to rethink their data security and protection measures and to be prepared for decades of vulnerabilities to network intrusions, insider threats, and espionage. In the absence of the market incentives that are proprietary to the private sector, public leaders must provide guidance that security is a priority for their organizations.

Impact to the DOD

The OPM breach is already being referred to as the "Biggest CI Threat in our Lifetime." It has clearly become the biggest breach in human history, affecting millions and virtually all current and former living government employees. Some employees are exposed more than others because of the breach (i.e. Americans with familial or social ties to Chinese, Russian or Korean foreign nationals), yet all are more vulnerable targets for financial fraud or foreign espionage.

To the US defense community, this attack is particularly disturbing. DOD has a responsibility to defend the nation from attacks in any domain in order to ensure that American citizens are secure. Logically, this includes the protection of

42 SANS Institute. "Incident Handler's Handbook." SANS Institute – InfoSec Reading Room. The SANS Institute, 2012.

43 Charman, Morgaine. "Cost Fallout of a Data Breach Felt for Years." Cost Fallout of a Data Breach Felt for Years Comments. February 4, 2015. Accessed August 14, 2015. http://www.vitrium.com/document-security-protection-drm-blog/cost-fallout-of-a-data-breach-felt-for-years/.

assets in both the public and private spheres. It is difficult to instill confidence in the American public, however, when government agencies fail to protect their networks in accordance with federal law. As many cybersecurity case studies demonstrate, the bulk of security incidents are caused either by (1) apathetic or untrained users - i.e. the OPM breach caused by a simple phishing attack - or (2) poorly mismanaged security programs - i.e. OPM's non-compliance with FISMA standards. Both of these problems can be attributed to poor leadership and bad management. If the U.S. government is going to make headway in securing its networks, it must start with organizational leadership.

In the ChoicePoint case study, the firm lacked market incentives to drive the company to secure its customer's data. Through policy and legal interventions, however, ChoicePoint was forced to adjust its cost/benefit analysis in favor of securing the data in the face of financial penalties. As stated earlier, no such mechanisms exist in the public sector at this point in time. While government employees are susceptible to punishment for gross negligence, this practice is rarely done in the public sector. In order to incentivize change in the government, commanders and leaders must take charge of their organization's network security posture, which means that IG-identified deficiencies are quickly addressed and not allowed to subsist for over seven years, as is the case of OPM. National leaders must, in turn, hold those individuals accountable and these areas of emphasis must be demonstrated through the proper allocation of budgeting and hiring of trained personnel. Leaders can no longer see network security as an "IT problem", but as a problem that can - and has - undermined the entire organization's ability to accomplish its collective function.

Impact to the Nation

Beyond the organizational level, the ongoing campaign of cyber-attacks has the potential to undermine our national security in a damaging and lasting manner. The internet has leveled the playing field for our nation's adversaries, providing technology to collect and transmit intelligence on US programs with speed and ease. As a consequence, American adversaries are postured to continue their success at exploiting vulnerabilities in poorly defended networks to export technology, data, and intellectual property at an increasing rate. Since the fall of the Soviet Union in 1991, the US military has been dominant in traditional warfighting domains: land,

sea, air, space. With the growing reliance of network centric warfare and the advent of cyberspace as the latest warfighting domain, the US finds itself at a crossroads in its efforts to maintain its leadership in the global arena. While nations like China and Russia have been relatively benign over the last two decades, American leaders and policymakers must not discount the newfound power that these nations now possess in the age of cyber weapons and exploitation.

Because of this tremendous gap between the capabilities of the US and competitor nations, the world has been a relatively safe place to live in terms of interstate conflict. Unlike previous eras, however, cyber weapons are remarkably cheap to make, easy to reproduce, and are capable of traversing time and space in a matter of seconds. Perhaps most alarming, all of this can be done with complete anonymity, giving the U.S. little hope of punishing or deterring the perpetrator or the facilitating nation state.

The adversary's computer network operation against OPM did not meet the threshold of physical destruction that conventional weapons can cause, but the potential for such an attack has increased. The attack on OPM demonstrates that cyber activities are an effective capability against the world's largest superpower. It provides evidence that nations can challenge US military supremacy, which undermines the international community at large. As the world's largest superpower and a significant proprietor of many global institutions, some scholars predict that a contested US military is dangerous for the global community at large.[44]

Summation and Closing

The solution to the cybersecurity dilemma facing the nation lies in the responsiveness of our organizations' collective response to this event and adoption of a culture that values cyber defense as a critical mission necessary to every organization. The OPM data breach highlights several ongoing complex issues related to the developing discipline of cyber operations. There are no easy, quick wins to contain the damage from this event. If we are to maintain our preeminence in the cyber domain, however, we must come to grips with these issues and overcome these obstacles. As this paper argues, the OPM breach should not be viewed as a singular event, but as an ongoing cyber campaign against government and related systems. In concert with the "Cisco 2015 Midyear report" and the Mandiant "M-Trends

44 Kagan, R. (2012). *The world America made*. New York

2015" report, we have identified several trends that are particularly relevant and concerning in the wake of the OPM hack:

1. ***Increased regularity of data breaches*** – Data breach frequency, size, and scope have and will continue to rapidly increase within the coming years. Advanced Persistent Threat actors will continue to attack unclassified networks that contain government and related information. High visibility targets include those associated with transportation and financial critical infrastructures.

2. ***Security's struggle with quickening pace of innovation*** – Security professionals are struggling to keep up with the pace of innovation that the adversary has been able to maintain. Cyber actors acting offensively will continue to have the advantage in the cybersecurity world. Patch management programs are currently being outpaced by the enemy's ability to innovate and find new vulnerabilities in systems.

3. ***A lack of quality cybersecurity talent*** – Currently, there is a grave shortage of competent IT security professionals in the workforce. In the case of OPM, this shortage was apparent throughout the 2014 IG report, which stated that the agency had only been able to hire four trained security experts to maintain security for its vast network of systems.

4. ***Stopgap solutions are preferred over defense in depth*** – As seen in the OPM case, companies are too often relying upon singular technologies as a primary defense against APTs. The OPM case shows that this logic is deeply flawed, and that organizations must employ "defense-in-depth" strategies in order to make their networks more secure.

5. ***Phishing and Whaling activities are on the rise*** – These activities are on the rise, and are increasingly becoming more sophisticated. Adversaries are using sophisticated methods involving data science to craft computer generated "landing pages" that are more effectively exploiting users.[45]

6. ***Stolen data being used for a variety of purposes*** – Our adversaries use aggregated data and singular data sets to extrapolate information for both intelligence and financial gains. Specific to espionage concerns, there is a growing fear that nation states will use the data to cross-reference separate data sets for the purpose of further exploiting the information to expose identities of intelligence personnel

45 Merriam-Webster defines phishing as "a scam by which an e-mail user is duped into revealing personal or confidential information which the scammer can use illicitly". Whaling is a more targeted version of phishing: It aims to collect personal information from high-profile individuals such as CEOs or highly-visible individuals.

that are working abroad.[46] Worse yet, nation states like Russia and China are reportedly collaborating and sharing intelligence on their mutual efforts to exploit US systems.[47]

At the heart of the OPM event is a central question: What is our data worth? If we were to judge the value of the lost information based on the actions taken to mitigate the damages, failure to confront the adversary, and safeguard the victims, we might conclude that the data was worth nothing. If we assume a broader, more expansive view of the question we assess that this data should be valued in terms of trust, integrity, and confidence. These concepts are so inherent in our day to day actions and our assigned responsibilities that they often go unspoken in our review of performance and outlook for future operations and commitment of resources. In this case, the trust, confidence, and integrity of the US government's ability to protect itself from outside intrusion, safeguard the people executing the duties required in the everyday functions of our system, and maintain information assurance of its assets is now questioned. In our estimation, we should begin the process of assigning value to the data in our possession for the purposes of prioritizing its collective defense. In our view, if we are not able to commit to securing their data, then they should not be using or collecting it in the first place.

Achieving dominance in cyberspace implies that collectively America can safeguard its own networks from intrusion, and that any intrusion achieved by the adversary is limited, contained, and severed in short order with response actions to correct the deficiencies, prevent their reoccurrence, and hold the perpetrator accountable. Nearly six months have passed since the breach was acknowledged publicly, the accountable organization has still not begun in earnest the notification process to the 22 million Americans affected. Because of this, our credibility wanes ever more. The credibility of the government's ability to protect itself and her people has been damaged repeatedly. This in part creates a widening gulf between the

46 Betrand, Natasha. "Russia and China Could Be 'making It Impossible for the US to Hide' Its Intelligence Activities." *Yahoo Finance*. Yahoo, 31 Aug. 2015. Web. 4 Sept. 2015. http://finance.yahoo.com/news/russia-china-could-making-impossible-205952714.html.

47 "CNN and the Los Angeles Times reported this week that Russia and China – whose leaders are meeting in Beijing for two days to discuss bilateral negotiations – have used a massive database analysis to combine and cross-reference information obtained from cyberattacks on targets that range from the Office of Personnel Management to Ashley Madison to identify and potentially compromise operatives." Quote taken from http://www.upi.com/Top_News/World-News/2015/09/02/Russia-China-using-hacked-data-to-target-US-spies/6481441041586/, 2 September 2015.

public and private sector, leaving another vulnerability for the adversary to exploit and an obstacle for American cyber professionals to overcome. Perhaps this is the greatest impact. Trust and integrity play a great role in relationships. The US governments' relationships with its citizens and its dealings with foreign partners suffer when that trust is damaged.

In response to the question "what is our data worth?" in the public sphere, we propose a simple answer: that our data is only worth as much as the commander and organizational leaders value it. To correct our security deficiencies, the government must hold leaders accountable and instill a sense of urgency at the organizational level, just as General Washington did in the era of a post-Benedict Arnold army. Commanders at the "tactical level" must take ownership of their networks and instill a sense of urgency in their employees. This emphasis needs to be more than just rhetorical; it is something that needs to be appropriately reflected by standing orders, hiring processes, and security budgets.

ANNEX A – Accounting for Lost Data

The most critical system that was breached during the OPM hack was the EPIC system, which is an acronym based on its major components:

-**E**: Electronic Questionnaires for Investigations Processing (e-QIP) system. This is a web based system used to conduct background investigations. The system provides a "secure Internet connection to electronically enter, update, and transmit their personal investigative data to a requesting agency". This system contains the SF-86 data.

-**P**: Personnel Investigations Processing System (PIPS). This is a background investigation management system that handles individual investigations requests from agencies.

-**I**: Imaging, or the PIPS Imaging System. This is a viewer for digitized paper case files such as surveys, questionnaires, and reports.

-**C**: Central Verification System (CVS). This is the mother lode of background investigations data. It contains security clearance information, PIV credentials used for CAC cards, and 1.1 million fingerprints. Fingerprints are especially significant because they are physically and permanently attributable to each individual.[1]

Much of the government's concern about the breach lies in the broad amount of information that was taken from OPM's systems. Security experts agree that the breach has exposed all SF-86 documents, one of the most PII "rich" documents that is processed by the government. [2] SF-86 documents contain all information about any person who applied for a security clearance. It contains an enormous spread of data that includes all prior residencies, drug and criminal history, family information, travel records to foreign countries, social security numbers, and other personal information.

---

44 Gallagher, Sean. ""EPIC" Fail—how OPM Hackers Tapped the Mother Lode of Espionage Data." Security and Hacktivism. Arstechnica, 21 June 2015. Web. 17 Aug. 2015. http://arstechnica.com/security/2015/06/epic-fail-how-opm-hackers-tapped-the-mother-lode-of-espionage-data/.

45 Kyzer, Lindy. "Was Your SF-86 Stolen in the OPM Hack? - ClearanceJobs." News and Career Advice. ClearanceJobs, 13 June 2015. Web. 17 Aug. 2015. https://news.clearancejobs.com/2015/06/13/sf-86-stolen-opm-hack/.

ANNEX B – Cyber Kill Chain

Reconnaissance
Initial RECON conducted during USIS 2013 breach.
Adversary gained “blueprints” of OPM’s networks
RECON continued during the initial 2014 breach of OPM systems and its partners
Vulnerable systems and third-party relationships identified

Weaponization
Crafting of phishing emails
Sakula malware tooling against vulnerable servers
Crafting of malicious site: opm-learning.org

Delivery
Phishing emails sent to third party targets

Exploitation
OPM server credentials acquired by phishing and redirection to malicious site.

Installation
Sakula malware installed on OPM servers

Command and Control
Malware C2 domain: opmsecurity.org

Actions on the Objective
Exfiltration of sensitive government employee data to adversary C2 server

ANNEX C – ACI TAC Interpretation of Diamond Model of Analysis

CORE FEATURES

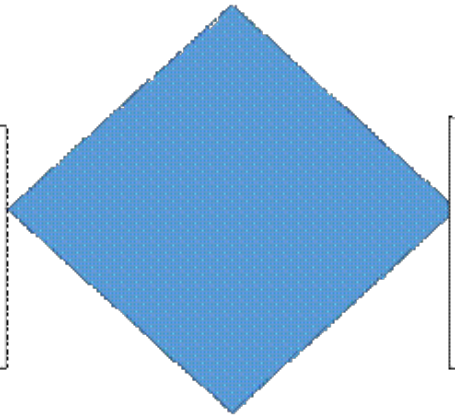
ADVERSARY, 95%: China

INFRASTRUCTURE, 100%:

-C2 node at opmsecurity.org

-opm-learning.org secondary means of maintaining access

-emails with attachments and links



CAPABILITES, 100%:

-spear phishing for contractor credentials

-outdated technology allowed for known malware

-poor intrusion detection system

VICTIM, 100%: United Stated Office of Personnel Management

META-FEATURES

- TIMESTAMP, 80%: As early as April 2013 to June 2015
- PHASE, 85%: Phase 1: Breach OPM, Phase 2: Send information out of OPM
- RESULT, 90%: Success
- DIRECTION, 100%: A2I then I2V then V2I then I2A.
- METHODOLOGY, 100%: Email spear-phishing attacks, insertion of Sakula malware, creation of backdoor
- RESOURCES:
  - Software, 100%: Sakula Malware
  - Knowledge, 60%: Experienced hackers with a clear target in mind
  - Information, 85%: Blueprints of OPM network from previous hack
  - Hardware, 0%: Unknown
  - Funds, 90%: Possibly unlimited funding from the Chinese government
  - Facilities, 90%: Probably located in China
  - Access, 100%: Obtained Contractor credentials, stolen certificate from DTOPTOOLZ Co., a Korean software company

ANNEX D – Timeline of OCO Campaign