Reputation: Preventing Social Media from Souring Democracy

Completed Research

Colin Y Monroe
Niagara University
cmonroe@mail.niagara.edu

Nicole K. Merritt
Niagara University
nmerritt2@mail.niagara.edu

Dr. Petter Lovaas
Niagara University
plovaas@niagara.edu

Abstract

Democracy is always a potential Lemon Market, as everyone gets an equal vote but does not have equal knowledge on all topics. Social Media has increased the likelihood of this by propagating and legitimizing Fake News that bypasses the previous gatekeepers, newspapers and television, which mitigated this risk. It is therefore critical to create a new reputation system, using the theory that democracy is an information system, as it is the best known control to mitigate a Lemon Market. This research then looks to answer the question: How can criteria for a control be created that mitigates the risk, while maintaining democracy? To answer this, research was conducted by using the Attack Tree (AT) methodology to discover the attack surface of democracy. It was then used to create criteria for the control ensuring it mitigated the risks of social media while maintaining the functionality of democracy.

Keywords

democracy, fake news, lemon market, reputation system, attack tree

Introduction

Advancements in technology have seen the proliferation of Fake News throughout the world, making the question of "who should we trust?" much more complex. Fake News is prolific in society due to the Internet creating a platform where individuals now have the same accessibility to create and publish news as any large media institution. Therefore, this research aims to show the effect of Fake News on democracy, as an information system, and present a methodology to help create controls that mitigate this risk. As there are no current risk frameworks created to evaluate democracy, this research takes an exploratory approach utilizing the first stage of risk assessment, threat modeling.

First, this research defines traditional democracy and then perceives it as an information system in order to understand what data is needed, to be available, to remain functional. This research then looks at how, Democracy is always a potential Lemon Market, as everyone gets an equal vote but does not have equal knowledge on all topics (Vozna, 2018). A Lemon Market, when information asymmetry occurs, is when a consumer can not differentiate between the qualities of products, due to having less knowledge than the seller (Devos, 2011). Social Media has increased the likelihood of democracy becoming a Lemon Market, by propagating and legitimizing Fake News that bypasses the previous gatekeepers, newspapers and television, which mitigated this risk. It is therefore critical to create a new reputation system, using the theory that democracy is an information system, as it is the best known control to mitigate a Lemon Market. (Yamagishi & Matsuda, 2002; Thierer et al., 2016). Finally, this research seeks to discover a, information security, methodology to use and therefore, asks the question: How can criteria for a control be created that mitigates the risk while maintaining democracy?

To answer this question this research will show that an information security threat modeling methodology, of Attack Trees (AT), can be used to discover the attack surface, all vulnerabilities, of democracy. Taking into account the attack surface, criteria can be created so that controls not only mitigate the threats democracy faces but also does not create new or reinforce current risks. Therefore, this shows that AT can be used to create the necessary criteria for controls, such as a reputation system, while maintaining the functionality of democracy.

Perceiving Democracy as an Information System

What democracy needs to function

Democracy is defined as the "rule by the people" (Dahl, 2017). Citizens are active in the political process by electing their government officials in free and fair elections. Within a Democracy, the rights of all people are protected, and the rule of law is applied equally to all citizens. In order to function, a democracy requires: majority rule, transparency of information, the ability for citizens to challenge the government, and verified elections. The authority of the government comes from the votes of the governed.

Democracy as an Information System

Information in democracy can be defined in two categories: common-knowledge and contested-knowledge (Farrell & Schneier 2018). An important piece of common-knowledge would be that elections need to be conducted in such a way that the results are deemed legitimate. This is done through a secret ballot in a system where the counting of votes is void of corruption. All candidates in an election are treated equally and given a fair platform to campaign. Contested-knowledge is needed as democratic elections are "competitive, periodic, inclusive, definitive elections in which the chief decision-maker in a government is selected by citizens who enjoy broad freedom to publicly criticize and present alternative views" (Kirkpatrick, 1984).

Democracy demands a delicate balance of common and contested knowledge to function (Farrell & Schneier 2018). If something that needs to be common-knowledge, like validity of elections, becomes contested then the system will cease to function. (Farrell & Schneier 2018).

Examining democracy, as an information system, instead of analyzing each individual information system that exists within a society allows for a more holistic approach (Farrell & Schneier, 2018). This holistic approach takes ideas from the national security and technologists' approach to security, as both are lacking individually when evaluating common-knowledge attacks (Farrell & Schneier, 2018). The national security approach tries to use older terms such as information warfare or propaganda, which is about degradation not persuasion (Farrell & Schneier, 2018). While the technologist approach focuses solely on technology, networks and voting machines etc., ignoring all social aspects of the broader system (Farrell & Schneier, 2018). By taking the national security view of the broader picture but utilizing information security methodologies, as they are better at determining trade-offs, for analysis, the attack surface of democracy can be formed (Farrell & Schneier, 2018). It will also be important to have a structured methodology to help provide a point of view on these social systems which are factual and not based on political or personal views.

Recently there have been several controls proposed to mitigate Fake News. However, these proposed solutions only consider the Internet as the system and ignore its effect on the greater whole, democracy. For example, nations, such as Australia, have started to institute legislation to put backdoors in software to bypass encryption (Tarabay, 2018). This would allow for the Australian government to be able to potentially view any communications by their citizens. While this solution, control, seems practical due to creating attribution for users, allowing for the potential ability to track down Fake News creators, it ignores the greater consequences on society. A society that uses democracy requires the ability for the public to challenge and debate topics therefore, privacy is needed to avoid threats from opposing sides. Other countries such as France have suggested censorship, with the government deciding what is fake or real news (Alouane, 2018). The US has proposed that social media companies censor their own platforms, in the form of filtering and deleting Fake News (Warner, 2018). This again could make sense from an Internet only perspective as it allows the system to be rid of unwanted data. However, it does not work inside of a democracy, as all information, that is correct or not and that does not create harm for any person, needs to be able to be freely expressed and shared. As democracy requires many different views in order to create discussion and progress.

The tradeoffs in a system can only be determined by considering the likelihood that a threat will actually take advantage of a vulnerability. This is important within a system as large as democracy as there are numerous possible threats but overreacting to one or a few means the draining of resources and functionality.

Threats Democracy faces from Fake News through Social Media

How Democracy is always a potential Lemon Market

Democracy is always a potential Lemon Market, as everyone gets an equal vote but does not have equal knowledge on all topics (Vozna, 2018). The Lemon Market economic theory was conceived by Akerlof (Devos, 2011). It states that when there is information asymmetry between consumer and seller, the market will result in only low-quality products being offered (Devos, 2011). Information asymmetry is when the consumer cannot differentiate between low or high-quality products because of a lack of information or understanding of it (Devos, 2011). When information asymmetry cannot be avoided, consumers must rely on trusted sources to fill the knowledge gap (Devos, 2011). A reputation becomes incredibly important because usually, with highly complex products, people will not know someone personally who can advise them (Yamagishi & Matsuda, 2002; Thierer et al., 2016). Therefore, a reputation system helps consumers bridge the knowledge gap, by informing which strangers are giving out reliable information (Yamagishi & Matsuda, 2002; Thierer et al., 2016).

How, malicious, actors create effective Fake News through Social Media

Political actors can use Fake News, or the threat of Fake News, as an attempt to "undermine the credibility of what were formerly trusted, credible sources of information" (Laslo, 2017). In turn, this can be used to convince their constituents that any negative story published by these sources could not possibly be true. In the process, "defenders of a free press" are fighting a losing battle, as more and more people join in on the theory that news outlets present "biased, unproven, salacious, and misleading coverage" (Laslo, 2017).

Carefully crafted fake narratives can leave citizens confused. For example, citizens may recognize that a news outlet is not trustworthy, but their social media reach can still be significantly large. Social media makes it easy to quickly share posts without taking a moment to critically assess their content. Caught up in the moment, sensationalized Fake News can spread faster than the truth, and its effects can spell trouble for a political campaign. Popular social media sites such as Facebook have introduced features to discourage Fake News, one such feature being the ability to "downvote" posts the user deems to be questionable content. This however, is not a fool proof method. David Rand, a professor at Yale noted that "people are going to be much more inclined to down vote things that they do not like instead of saving the down voting to things they think are actually false" (Christian, 2018). This downvoting system, in social media platforms, also makes it is easy for malicious actors to monitor how well their Fake News is being received by the public. Instant feedback greatly benefits these malicious actors as it can be used to slowly make their Fake News more effective on the target user base (The grugq, 2019).

Becoming more sophisticated than ever, "bots can generate personas that appear as credible follows" (Ferrara et al., 2016) making it even harder for the average user to determine if the content is authentic. Bots can be used to "mislead, exploit, and manipulate social media discourse with rumors, spam, malware, misinformation, slander, or even just noise" (Ferrara et al., 2016). Bots operate successfully on the fact that social media users repost first and ask questions later, "our vulnerability makes it possible for a bot to acquire significant influence". Political campaigns can also employ the use of bots to "artificially inflate" (Ferrara et al., 2016) the size of their base.

Fake News can also be created to feed into the hysteria of an active situation, aimed at affecting hot button issues. For example, during the Parkland school shooting, while tweets involving a second gunman were concerning, a yet more disturbing motive arose when a "fake screenshot of a BuzzFeed article with the headline 'why we need to take away white people's guns now more than ever'" (Lee, 2018) began to circulate. No such article was ever posted to the BuzzFeed website, its motives were to "incite anti-Semitic sentiment" (Lee, 2018) as well as push a false narrative on the nations gun control issue, making the issue about race, rather than safety.

The impact of Fake News through Social Media on democracy

The two most prominent types of trust in society are personal and institutional (Botsman, 2017). Personal trust comes from many factors such as: knowledge of a person's backgrounds, shared values, and if the person is predictable. Due to the large population of modern cities, and because it is impossible to know and trust outside of a certain number of individuals 5-150, there is a need for a trusted third party for society to function (MIT, 2016). Institutions have filled this void and provided society with a trusted way to close the knowledge gap. "Institutions [...] are essentially social structures made up of a history of practices, values and laws that are accepted and used by many people" (Botsman, 2017). Society perceives social media platforms as having both types of trust: institutional from their brand and personal from their users. Social media was able to gain institutional trust quickly because so many users were extending their personal trust to the platforms. This trust was then used to verify the integrity of the news shared by individuals by association, rather than endorsement. Malicious actors were then able to exploit this trust by association to legitimize the information they were spreading.

The Internet allowed the production and distribution of news media to become more accessible to all individuals within society. As before the Internet, traditional media were essentially gatekeepers, a control, which censored what people could publish to the wider public. As normal individuals could not afford to become a gatekeeper, the media was heavily centered around large TV, Radio, and Newspaper companies (Lepore, 2018). Although Fake News existed on the Internet, it was the social media algorithms that brought it forth and presented it as legitimate news to the user. This information was usually distributed through people sharing, threads, and/or the news feed that the user had customized (Tufekci, 2015).

The algorithms that social media used to bring news to users did not consider quality of journalism but rather if it interested the user (Tufekci, 2015). Since "it is estimated there are more than 3 million blog posts written in the world per day" (Botsman, 2017) there is a lot of sub quality, and potentially Fake, News available to be used by the algorithm. This had a huge impact on society, as "nearly two-thirds of Americans get news on social media" (Botsman, 2017). Due to the fact that the news resonated with the reader they were also more likely to trust it, "people are more likely to describe 'a person like me' as the most credible source of information" (Botsman, 2017).

When political candidates are not transparent in their actions it can lead to democracy becoming a Lemon Market (Vozna, 2018). To make an informed decision, voters rely on prominent voices to guide their decisions. The average citizen needs factual information, to be presented by experts, in order to inform them and bridge the knowledge gap. The news media has always been an essential cog, as it provided the medium for these experts to distribute the necessary information, in the system. It is a cog that had institutional trust, which is why the older generation still use it, as it acted as a gatekeeper, control (Shearer, 2018). Social Media has now made this control weaker, leading to the likelihood of democracy as a Lemon Market being higher.

How risks can be mitigated through the use of reputation

How Reputation can fill the knowledge gap

When discussing closing the knowledge gap most people will point towards education. However, education is not just about facts, it is about interpretation of the facts by the people teaching and learning, which can lead to bias. When students learn the facts of history, dates, names, etc., they also learn about people themselves and their actions. How this information is interpreted by them, or for them, shapes how they view this information and their own thinking on the topic.

For example, if someone on the street was waving around their homemade newspapers, people would be unlikely to stop and listen to what they have to say. These individuals are deemed untrustworthy and the information they provide is not seen as valuable or reliable. However, if this same individual was to post their information online they would have a much easier time getting people to listen to their message. Why? Reputation of the author matters. People cannot see who is posting but as long as the message resonates with the reader they are more willing to repost it or share it with their friends. Therefore, if reputation is needed, to prevent social media from leaving democracy in a permanent Lemon Market state, the question becomes: How can criteria for a control be created that mitigates the risk while maintaining democracy? This paper seeks to answer this question through the use of the Attack Tree methodology.

Conducting threat modeling through building Attack Trees

To create a control that mitigates the effect of Fake News through Social Media, this research used Attack Trees (AT), as the information security methodology, to explore and create the attack surface of democracy. By examining the likelihood of all possibilities due to the threats that exist, this paper determined what the known crucial vulnerabilities currently are. This was accomplished through the researching of real-world events, shown in the, How, malicious, actors create effective Fake News through Social Media section. The results of the AT were used during the creation of the criteria for a reputation system by ensuring that it mitigates vulnerabilities while not creating or reinforcing new ones in democracy.

To determine the security of a system, AT can be used as they are a formal and methodical way of discovering an attack surface (Schneier, 1999). Once the boundaries and goals of the system are determined, then by using data from historical events and theoretical attacks, it can be determined what attacks may impede the system. A separate tree should be created for each attack goal (Schneier, 1999). The tree allows for the exploration and description of all the possible ways an attacker could succeed (Schneier, 1999). Probability and values can be assigned to each node of the tree (Schneier, 1999). A node is either an AND or an OR, usually if the node is not labeled AND then it is an OR (Schneier, 1999). OR nodes mean that they are alternative possibilities while AND nodes show different steps toward the same goal (Schneier, 1999).

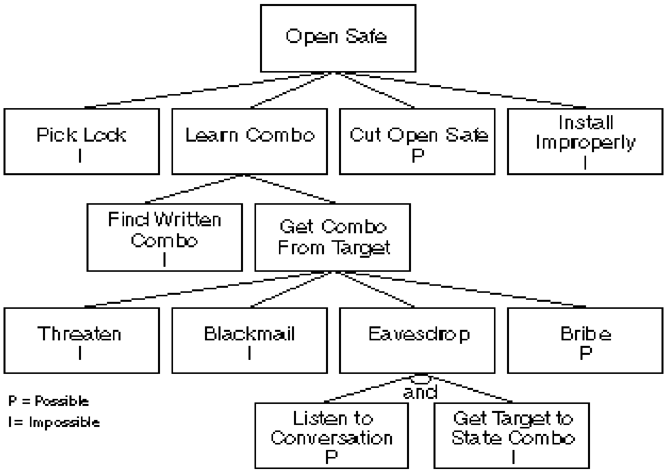

Figure 1: Example Attack Tree (Schneier, 1999)

While there are more complex ways to evaluate systems, such as a full risk assessment using a risk framework, this is currently not possible. There are currently no risk frameworks that have been created that can evaluate the information flow within a society. Therefore, this research takes an exploratory approach by starting at the basics of risk assessment, threat modeling, to discover the basic criteria the system needs to function. Attack trees are the first fundamental step, as it creates the attack surface and can lead to the creation of a more comprehensive risk framework in the future.

Threat modeling is a way of discovering every conceivable way that something could go wrong and disrupt the system. For example: think of what your goal is today or tomorrow, then think of every possible way something could go wrong and prevent you from achieving it. Attack Trees provide a structured methodology for mapping out all these possibilities for complex systems.

For this paper Attack-Defense tree software tools (AD) was used to create the Attack Tree (Fraile et al., 2016). AD tools is an academically tested software for the creation of Attack - Defense Trees (Fraile et al., 2016). However, the Social Media and Election Branches of the AT were recreated using Gliffy for viewing purposes. The first step to creating the Attack Tree was to fundamentally understand how the system works (Fraile et al., 2016). To do so, a formal definition of what democracy is and what information it needs to function was created. Research was then conducted to see what real world events had taken place that had compromised the components necessary to the information flow of democracy. This information was gathered using a qualitative document-based methodology. The Attack Tree was then created with each primary node representing a component and each subsequent node showing vulnerabilities that real world actors had exploited. Basic countermeasures for each primary node were then inserted to show how technology is changing the needs for controls within democracies information system.

Steps for Attack Tree Creation	
1. Understand Fundamental System	Formal definition of democracy created
2. Create primary nodes (vulnerabilities)	Qualitative document-based research into real world events that adversely affect the functionality of democracy.
3. Branches and subsequent nodes	Sub nodes of the primary were created by considering how these main vulnerabilities could come to fruition.
4. Countermeasures / Controls	Each primary node was linked to a potential control that could mitigate the likelihood.

Table 1. AT Creation (Schneier, 1999)

Attack Tree methodology – Controls for Democracy

The results of the Attack Tree, see figure 2 below, reveal what the general attack surface of the social media branch of democracy currently looks like. Examining the social media branch of the Attack Tree shows the main vulnerabilities that need to be currently mitigated. Real world events such as the botnet attacks, events after Parkland, and Fake News generated by political campaigns were categorized into the vulnerabilities; Trolls, Botnets, and Polarization. These are the current major vulnerabilities that a reputation system, individual and institutional, could provide mitigation for. This type of reputation system would provide the user the ability to verify the history of the source and see other user's opinions so they can differentiate the quality of news. It could also, potentially make it harder for malicious actors to get instant feedback, as users may be less inclined to interact with unknown sources of information. Users are also motivated to be honest with their opinions since their own reputations are also now being staked in their actions.

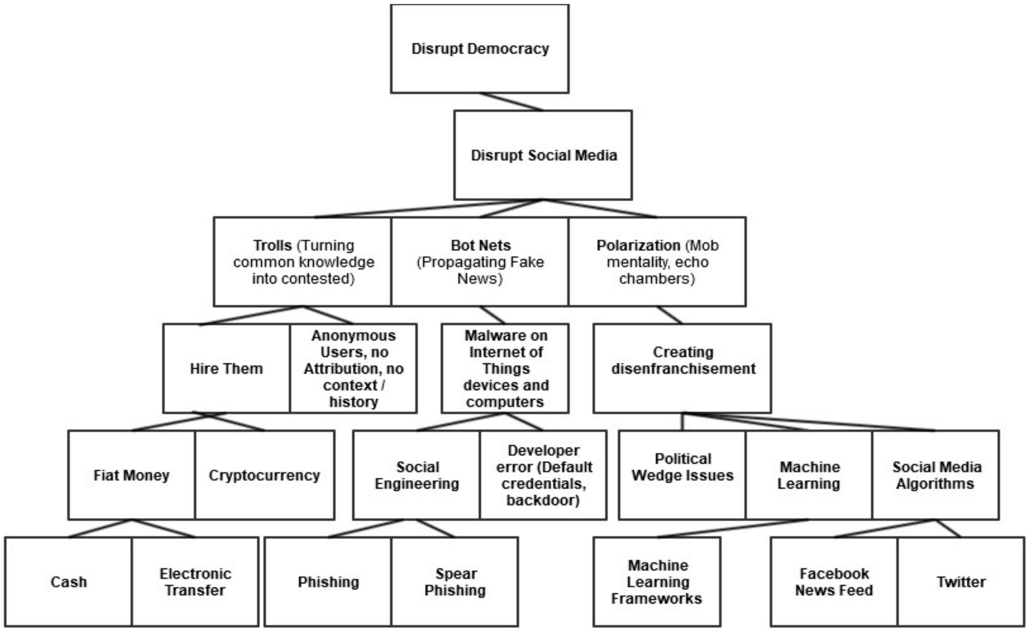
Disrupt Democracy
Disrupt Social Media
Trolls (Turning common knowledge into contested)
Bot Nets (Propagating Fake News)
Polarization (Mob mentality, echo chambers)
Hire Them
Anonymous Users, no Attribution, no context / history
Malware on Internet of Things devices and computers
Creating disenfranchisement
Fiat Money
Cryptocurrency
Social Engineering
Developer error (Default credentials, backdoor)
Political Wedge Issues
Machine Learning
Social Media Algorithms
Cash
Electronic Transfer
Phishing
Spear Phishing
Machine Learning Frameworks
Facebook News Feed
Twitter

Figure 2: Example of Social Media Branch of Attack Tree

A reputation system relies on the transparency of enough information so that the user can understand and trust the source. For example, if a person is writing a political piece then knowing if they are biased, due to having ties to Russia or China, can be relevant (Lim & Bergin, 2018). This is done through the revealing of information about the source and can be from full transparency to full anonymity. If too much information is revealed, then trust will start to deteriorate in society as people will only gravitate towards people like them. This will lead to echo chambers in the real world just like how it occurred in social media (Tufekci, 2016). For example, in a fully transparent system, a user could see the full internet history of someone else and then could decide to interact or not interact with them based upon the user's viewpoint on topics from politics to sports. To find the correct attributes for a reputation system within democracy, the information revealed to other users will be compared to the Attack Tree to check for the possibility of new, or the reinforcement of current, vulnerabilities. If that occurs, then the tradeoff between the two vulnerabilities should be compared to see if it is worth implementing.

To determine the information that a reputation system should use the Attack Tree should be examined. For instance, if considering identity, the user should be allowed to choose and utilize a permanent pseudonym, unless they want to reveal their real identity. This is important as democracy requires that people can try and convert contested-knowledge into common-knowledge, by protesting and debating. If the people who are in favor, or especially empowered by the common-knowledge, know the people trying to change it, they are more likely to be able to threaten them. This would reinforce vulnerabilities such as government manipulation and voter intimidation, which can be seen below in figure 3. Information such as a person's work history should be used alternatively as it does not a) identify the user and/or b) create or reinforce any major vulnerabilities in democracy. However, no single piece of information should ever be used to draw a conclusion about any individual but rather the sum of all pieces should be considered. For example, if a person’s work history showed they wrote a pro Chinese piece, it should not be assumed that they are in fact supporters of China. The rest of their total history should be taken into account as perhaps it was just on that particular topic that their interests aligned.

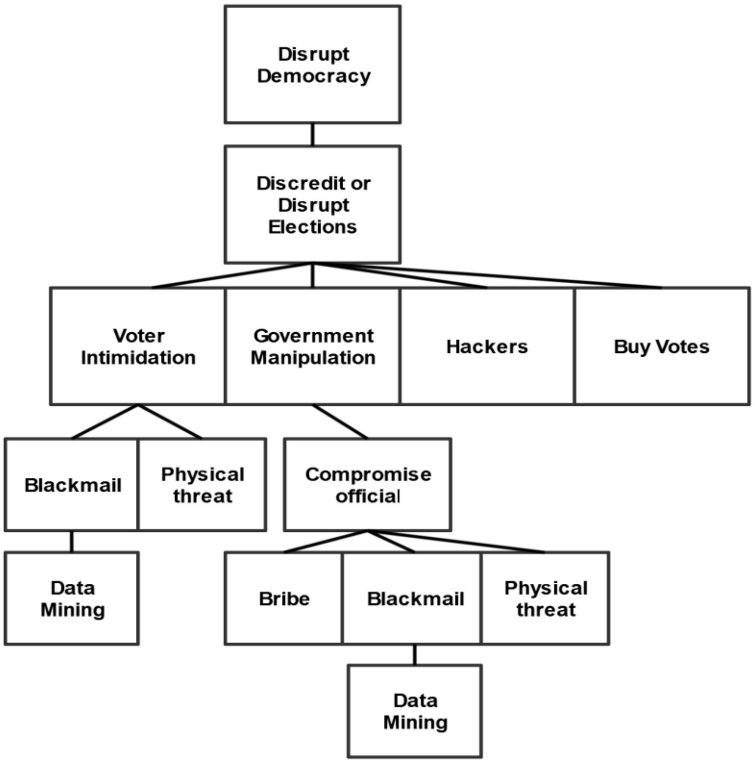

Figure 3. Example of Election Branch of Attack Tree

A Vulnerability to news media	**Information used to mitigate**	**Control Effectiveness (High-Medium-Low)**	**Vulnerabilities created or reinforced in democracy**	**Worth the tradeoff**
Trolls	**Permanent pseudonyms (Assumption cannot be linked to real identity)**	**Medium**	**Social Engineering,**	**Yes if the assumption to holds true**
	Real Identity	**High**	**Voter Intimidation, Government manipulation, Blackmail, Physical, Social Engineering**	**No**
	Usage history on the platform	**Medium**	**Data Mining, Political Fake News, Social Engineering**	**Depends on how much and what is in the usage history**
	IP Address	**Low**	**Government manipulation, Hackers, Anonymous Users**	**No**

Table 2. Analysis of attack surface example

Conclusion & Future work

Future work should start by constructing a fully comprehensive attack tree for democracy. Doing so will allow for the discovery and evaluation of other controls for democracy and lead to the construction of a risk framework. Design science methodology can then be utilized, using the risk framework as the artifact, to show how it would improve the system, democracy. This framework could then also potentially be used to consider if there is a way to modify the system, democracy, to preserve the values of society but decrease the potential vulnerabilities that exist.

An examination of other AT, under the media attack tree, such as the traditional media, TV & Radio, should be furthered examined. As if the risk to social media becomes mitigated, malicious actors may look towards these sources to further their goals.

Progression, especially technological, destroys and creates simultaneously. Therefore, if society does not keep pace, its vulnerabilities will increase. This paper presents a possible defense for democracy against Fake News propagated by Social Media. The approach taken was to: 1) Identify that democracy is a potential Lemon Market, 2) Show that Social Media has increased the likelihood of democracy being a Lemon Market, 3) Discover that reputation systems can mitigate a Lemon Market, 4) Showed how information security methodology, Attack Trees, can be used to create criteria for controls in, democracy as information system, and 5) Displayed how the attack surface can be used to prove that a reputation system can help mitigate the threat of Fake News without harming democracy.

References and Citations

Alouane, R. May 29, 2018. "Macron's fake news solution is a problem," in: Foreign Policy. Retrieved January 30,2019, from https://foreignpolicy.com/2018/05/29/macrons-fake-news-solution-is-aproblem/

Botsman, R, October, 2017. "Who can you trust? How Technology Brought us Together and Why It Might Drive Us Apart", Hachette Book Group, New York, NY

Devos, J, 2011. "The Theory of the Lemon Markets in IS Research", in: Information Systems Theory: Explaining and Predicting Our Digital Society, Vol. 1 (pp.213-229). Retrieved December 2, 2018 from https://www.researchgate.net/profile/Jan_Devos/publication/226469192_The_Theory_of_the_Lemon_Markets_in_IS_Research/links/0046352bc031197f25000000/The-Theory-of-the-LemonMarkets-in-IS-Research.pdf

Farrell, H., and Schneier, B. October, 2018. "Common-knowledge attacks on democracy", in: Berkman Klein Center Research Publication. Retrieved December 16, 2018 from https://ssrn.com/abstract=3273111

Fraile, M., et al. 2013. "Using attack-defense trees to analyze threats and countermeasures in an ATM: a case study", in: The Practice of enterprise Modeling. Retrieved January 12, 2019 from http://satoss.uni.lu/members/rolando/papers/FFGKST2016.pdf

Kirkpatrick, J, 1984. "Democratic elections and democratic government," in: World Affairs. Retrieved on February 18, 2019 from https://www.jstor.org/stable/20672013?seq=1#page_scan_tab_contents

Lepore, J, 2018. "These truths: A History of the United States," W.W. Norton & Company, New York, N

Lim, L., Bergin, J., December 7, 2018. "Inside China's audacious global propaganda" in: The Guardian Retrieved on February 12, 2019 from https://www.theguardian.com/news/2018/dec/07/china-planfor-global-media-dominance-propaganda-xi-jinping

MIT, April 29, 2016. "Your brain limits you to just five bffs" in: MIT Technology Review. Retrieved on February 19, 2019 from https://www.technologyreview.com/s/601369/your-brain-limits-you-to-justfive-bffs/#/set/id/601360/

Schneier, B, 1999. "Attack Trees", in: Dr. Dobbs Journal. Retrieved on November 20, 2018 from https://www.schneier.com/academic/archives/1999/12/attack_trees.html

Shearer, E, "Social media outpaces print newspapers in the U.S. as a news source" in: Fact Tank, Retrieved on January 12, 2019 from http://www.pewresearch.org/fact-tank/2018/12/10/socialmedia-outpaces-print-newspapers-in-the-u-s-as-a-news-source/

Tarabay, J, December, 2018. "Australian Government Passes Contentious Encryption Law," in: The New York Times, Retrieved on December 7, 2018 from https://www.nytimes.com/2018/12/06/world/australia/encryption-bill-nauru.html

The grugq, March 20, 2019. "Bonus Episode: The grugq illuminates influence operations" in : The Cyberwire, Retrieved on April 19, 2019 from https://www.youtube.com/watch?v=0u7wlYdpcbc

Thierer, A, et al, May 1, 2016. "How the Internet, the Sharing Economy, and Reputational Feedback Mechanisms Solve the Lemon Problem", in: University of Miami Law Review, Vol. 70, No. 3, 2016, Retrieved on December 2, 2018 from https://poseidon01.ssrn.com/delivery.php?ID=621088068104090084116123109114089106036027002004054026093006105094086089103116102112126054119097105100002113092080118022074120008022042062050091110096088069110067059013042068102009003065022096007003075022017007003003002073125092110084069067115000092&EXT=pdf

Tufekci, Z, May, 2015. "Facebook said its Algorithms Do help to form echo chambers. And the Tech Press Missed It," in: Huffington Post, Retrieved on December 3, 2018 from https://www.huffingtonpost.com/zeynep-tufekci/facebook-algorithm-echochambers_b_7259916.html

Vozna, L, 2018. "The Political Market with Asymmetric Information and Hybrid Democracy", in: Italian Association for the History of Political Economy. Retrieved on January 18, 2019 from https://www.researchgate.net/publication/328293918_The_Political_Market_with_Asymmetric_Information_and_Hybrid_Democracy

Warner, M. July, 2018. "Potential policy proposals for regulation of social media and technology firms" Retrieved on January 19, 2019 from https://graphics.axios.com/pdf/PlatformPolicyPaper.pdf

Yamagishi, T & Matsuda, M, May, 2002. “Improving the Lemons Market with a Reputation System: An Experimental Study of Internet Auctioning,” in: Hokkaido University. Retrieved on November 22, 2018 from https://repository.law.miami.edu/cgi/viewcontent.cgi?article=4469&context=umlr