Weaponizing Information Systems for Political Disruption: The Actor, Lever, Effects, and Response Taxonomy (ALERT)[1]

Kevin C. Desouza[2]
Atif Ahmad[3]
Humza Naseer[4]
Munish Sharma[5]

Original Version: February 28, 2019
Revised Version: August 2, 2019

[1] We thank all participants at the Cyber Storm International Conference (Canberra, Australia, Feb 19-20, 2019) and Democracy in the Crosshairs: Cyber Interference, Dark Money, and Foreign Influence Conference (Philadelphia, Pennsylvania, USA; Nov 1-3, 2018) who provided valuable feedback on the ideas presented in this paper.

[2] Kevin C. Desouza is a Professor of Business, Technology and Strategy in the School of Management at the QUT Business School. He is a Nonresident Senior Fellow in the Governance Studies Program at the Brookings Institution and is a Distinguished Research Fellow at the China Institute for Urban Governance at Shanghai Jiao Tong University. He has held tenured faculty appointments at the University of Washington, Virginia Tech, and Arizona State University. In addition, he has held visiting appointments at the London School of Economics and Political Science, Università Bocconi, University of the Witwatersrand, and the University of Ljubljana. Desouza has authored, co-authored, and/or edited nine books. He has published more than 130 articles in journals across a range of disciplines including information systems, information science, public administration, political science, technology management, and urban affairs. For more information, please visit http://www.kevindesouza.net

[3] Atif Ahmad is a senior academic at the University of Melbourne's School of Computing & Information Systems. Atif leads Business Information Security research and serves as the Deputy Director for the Academic Centre of Cyber Security Excellence. His main areas of expertise are in the strategy, risk and incident response aspects of Information Security Management (ISM). He has authored over seventy scholarly articles in ISM and received over $3M in grant funding. His research has been published in high-impact journals such as Computers & Security and the International Journal of Information Management as well as leading conferences such as the International Conference on Information Systems. Atif has previously served as a cybersecurity consultant for WorleyParsons, Pinkerton and SinclairKnightMerz. He is a Certified Protection Professional with the American Society for Industrial Security. For more information, please visit https://www.atifahmad.me/

[4] Humza Naseer is a Research Fellow in the School of Computing and Information Systems at the University of Melbourne. His research interests include business analytics, cybersecurity and information systems management. He has published in leading conferences including the International Conference on Information Systems and the European Conference on Information Systems. He holds the professional designation of The Data Warehousing Institute's Certified Business Intelligence Professional with specialization in Business Analytics. In his PhD, he investigated how organizations improve agility in their cybersecurity incident response process using real-time analytics.

[5] Munish Sharma is a Consultant in the Strategic Technologies Centre at the Institute for Defence Studies and Analyses, New Delhi. His research interests include cybersecurity, critical information infrastructure protection, space security and geopolitical aspects of emerging technologies. Munish has authored research papers, articles, briefs and commentaries for various journals, magazines and websites. His recent publications include: India's Strategic Options in a Changing Cyberspace (2019), Cherian Samuel and Munish Sharma; "Decrypting China's Quantum Leap," The China Journal, no. 80 (July 2018); Securing Critical Information Infrastructure: Global Perspectives and Practices (2017); Securing Cyberspace: International and Asian Perspectives (2016), Cherian Samuel and Munish Sharma (eds.). He is UK Next Generation Scholar and a Chevening Cyber Security Fellow (2018).

Weaponizing Information Systems for Political Disruption: The Actor, Lever, Effects, and Response Taxonomy (ALERT)

Abstract

Information systems continue to be used by actors who want to undermine public institutions and disrupt political systems. In recent times, actors have engaged in acts of information warfare ranging from attempts to compromising voting systems, to spreading false propaganda and even direct attacks on public infrastructure via information systems. Initial analysis points to the fact that most of these attempts have been successful in achieving their intended objectives. Given this reality, we expect them to intensify and be more creative in the future. In this paper we draw on a critical analysis of the role of information systems in creating political disruption to propose that information systems can be 'weaponized' by compromising their goals and values even while they remain protected. Building on this proposition we develop a risk-based Actor, Lever, Effects and Response Taxonomy (ALERT) to assist security practitioners and policymakers to analyze and respond to attacks enabled by information systems aimed at political disruption. We illustrate the utility of ALERT using representative examples of weaponized attacks from credible news sources. Finally, we leverage the insights gained from ALERT to propose a theoretical framework where we assert that over time as actors gain maturity and experience using levers to disrupt political systems, so too does the public sector gain experience in response thus building their response capacity. This dynamic relationship increasingly pushes both actors and defenders to come up with more innovative, agile and sophisticated methods to weaponize and respond to information systems enabled attacks.

Keywords: information systems, information warfare, cyber, cybersecurity, cyber conflict, critical infrastructure, threat modeling, taxonomy

Introduction

- The US federal election of 2016 was subjected to a sustained, systematic and well resourced (millions of dollars and dozens of personnel) campaign of information warfare by the Russian state[6][7][8]. The Russians conducted two key operations. The first operation undermined the credibility of the candidates and the political system by using social media to disseminate political messaging. The messaging strategy promoted Donald J. Trump, denigrated his opponent Hilary R. Clinton and persuaded minorities to vote for selected candidates. The second operation hacked systems belonging to the Democratic National Convention and stole sensitive information including private email conversations involving Clinton. The stolen files were released to the public in order to drive a wedge between the Democrat candidates.
- In March of 2018, the data analytics firm Cambridge Analytica attempted to actively and systematically manipulate the US democratic system[9][10][11]. Their strategy was to engage in 'mass persuasion' by targeting tailored political messages to individual US voters. Cambridge Analytica used psychographic profiling techniques to develop algorithms that were trained on personal information about US voters (tertiary education, political affiliation, and personality assessment questions) that they linked with their social media behavior (e.g. likes, dislikes, and friend networks) on an industrial scale (87 million users).
- In February of 2018, Russian bots launched a comprehensive and systematic campaign to shape the political discussion around a flawed intelligence document[12]. The document purported to implicate the Obama administration in a series of abuses relating to the surveillance of the Trump campaign. Although the eventual release of the memo didn't have the effect the Republicans intended, the information operation driven by Russian twitter bots (#releasethememo) succeeded in creating a political storm that lead to the release of the memo and created the popular perception among Republican voters that key public institutions namely the FBI and the Department of Justice were trying to 'delegitimize' the Trump administration.

Information systems have been used to undermine democratic processes and institutions over the last several years. Only recently has the issue come to the forefront, but countries such as Estonia, Belarus, and Moldova have had to contend with the issue for a much larger period[13]. To complicate matters, our public institutions have become more dependent on information systems as they conduct elections. And, some have even been experimenting with new technologies (e.g. Blockchain)[14]. However, this has opened new avenues for those

---

[6] Matishak, M. (2018, 18 July). What we know about Russia's election hacking. Politico. Retrieved from https://www.politico.com/story/2018/07/18/russia-election-hacking-trump-putin-698087

[7] Lipton, E., Sanger, D., & Shane, S. The Perfect Weapon: How Russian Cyberpower Invaded the U.S. The New York Times. Retrieved from https://www.nytimes.com/2016/12/13/us/politics/russia-hack-election-dnc.html

[8] McKew, M. (2018, 16 February). Did Russia Affect the 2016 Election? Its Now Undeniable. Wired. Retrieved from https://www.wired.com/story/did-russia-affect-the-2016-election-its-now-undeniable/

[9] Cambridge Analytica Scandal Casts Spotlight on Psychographics. (n.d.) Association for Psychological Science. Retrieved from https://www.psychologicalscience.org/publications/observer/obsonline/cambridge-analytica-story-casts-spotlight-on-psychographics.html

[10] Halpern, S. (2018, March 21). Cambridge Analytica, Facebook, and the Revelations of Open Secrets. The New Yorker. Retrieved from https://www.newyorker.com/news/news-desk/cambridge-analytica-facebook-and-the-revelations-of-open-secrets

[11] Kozlowska, H. (2018, April 5). The Cambridge Analytica scandal affected nearly 40 million more people than we thought. Quartz. Retrieved from https://qz.com/1245049/the-cambridge-analytica-scandal-affected-87-million-people-facebook-says/

[12] McKew, M, (2018, February 4). How Twitter Bots and Trump Fans Made #ReleaseTheMemo Go Viral. Politico. Retrieved from https://www.politico.com/magazine/story/2018/02/04/trump-twitter-russians-release-the-memo-216935

[13] Dorell, O., (2017, September 7). Alleged Russian political meddling documented in 27 countries since 2004. USA Today. Retrieved from https://www.usatoday.com/story/news/world/2017/09/07/alleged-russian-political-meddling-documented-27-countries-since-2004/619056001/

[14] Desouza, K. & Somvanshi, K. (2018, May 30). How blockchain could improve election transparency. Brookings. Retrieved from https://www.brookings.edu/blog/techtank/2018/05/30/how-blockchain-could-improve-election-transparency/

that want to compromise the integrity of the process. In 2009, Electronic Voting Machines (EVMs) were shown to be vulnerable to hacking when the CIO of the city of Pune in India discovered spreadsheets on the website of the Election Commission of India that showed the results of elections that were yet to be held[15]. Since then IT experts have demonstrated at least two ways of hacking the EVMs that involve replacing parts of the machine with rogue devices.

Citizens' trust in their government and public institutions is also dependent on information systems. Today, almost all facets of the public sector leverage information systems to deliver public services. Compromise the technology, impact the service delivery, increase fear and frustration in the citizenry, and create political turmoil is a common flowchart for rogue actors. Sixteen hospitals were shut down across the United Kingdom in May of 2017 as part of a global WannaCry ransomware attack that affected 300,000 computers in Russia, Taiwan, Ukraine and India[1617]. Hospital staff in the UK cancelled or delayed all non-emergency procedures, turned back ambulances, and reverted to using pen and paper as medical records were inaccessible, systems were frozen, and files were encrypted. The systems had been penetrated using a specialized hacking tool dubbed 'Eternal Blue' that was stolen from the US National Security Agency. The tool allowed the perpetrators to penetrate and compromise systems running Microsoft Windows.

Given this background and the recent events, it is imperative that we take a critical look at how information systems, in all their forms and uses, can create and sustain political disruption. Political disruption can take many forms from undermining an activity (e.g. elections) to taking an agency hostage (e.g. through ransomware) to intermediate (indirect) actions (e.g. fake news meant to shape opinions leading to actions). In this paper, we address security policymakers and practitioners in primarily public institutions but also in private organizations. We describe how information systems impact political disruption through a simple Actor, Lever, Effects, and Response Taxonomy (ALERT), that outlines the nuances associated with various types of options that individuals, organizations, and nations have to weaponize information systems for political gain and to cause public unrest. We use illustrative cases from recent events to ground our framework.

The rest of the paper is organized as follows. First, we review background material on the nature of information systems disruptions to political processes and public institutions. Next, we outline the key elements of our taxonomy – actors, levers, effects, and responses. We then describe our taxonomy and share illustrative examples. This is followed by the development of a novel theoretical framework and future research avenues. The paper concludes with our analysis of how the future might unfold depending on how one chooses to combat the current threats to political stability, democratic institutions and processes, and the nature of technology-mediated political communications.

Background

Central to the recent and rapid advancement in information systems is the increasingly fine-grained data generated from myriad types of sensors (humans, objects) embedded in a range of digital platforms from social (e.g. Facebook and Twitter), banking and financial (e.g. PayPal and SWIFT), health-based (e.g. Fitbit), transport & logistics (e.g. uber ride-sharing), ecommerce platforms (e.g. Amazon and eBay) and even food and entertainment (e.g. uber-eats and Netflix) among others. These rich sources of data can be used to

[15] Paskal, C. (2014, May 14). How Secure are India's Elections? HuffPost. Retrieved from https://www.huffingtonpost.com/cleo-paskal/how-secure-are-indias-ele_b_5317788.html

[16] Brandom, R., (2017, May 12). UK hospitals hit with massive ransomware attack. The Verge. Retrieved from https://www.theverge.com/2017/5/12/15630354/nhs-hospitals-ransomware-hack-wannacry-bitcoin

[17] Graham, C. (2017, May 20). NHS cyber attack: Everything you need to know about 'biggest ransomware' offensive in history. The Telegraph. Retrieved from https://www.telegraph.co.uk/news/2017/05/13/nhs-cyber-attack-everything-need-know-biggest-ransomware-offensive/

construct large datasets and apply computational methods of analysis to 'connect the dots' across multiple contexts such as time and space. The resulting knowledge about people including their beliefs, attributes, preferences and patterns of behavior is a source of insight that can be used to predict the behaviors and actions of the targeted population under various conditions.

The algorithms that have been designed for the computational processing of these large datasets and linking disparate patterns and threads of data are essentially sophisticated learning systems. Humans retain the power to secretly tweak or guide the algorithms, which places considerable power in their hands. For example, in 2012 Twitter was accused of engaging in 'algorithmic censorship' of #occupywallstreet. Twitter did not show the topic trending even in cities where protests were being held and tweets were spiking[18]. When Google was accused of proliferating fake news and put under considerable political pressure, the company announced that it had tweaked its search algorithm to give more weight to the authority of the source[19]. Today, when examining social networks, auditing algorithms is challenging due to their complex and opaque nature. However, they wield considerable power over the lives of the masses as they increasingly influence our real-life choices at every level of granularity. The dependence on information systems and the insights generated from them at the individual level raises the worrying issue as to the extent to which an individual is programmable. The route you choose to get to the pub, the next TV series you watch, and even what restaurant you will visit or news article you will read are seldom down to your own *independent* decision, rather most of the time, information systems augment your decision-making capabilities, and in some cases they even automate it for you. Here in lies the critical issue, if information systems are compromised, or worse, weaponized, by rogue actors, most individuals will a) not know that this is going on behind the scenes, and b) have limited alternatives in terms of how they traverse, and interact, with their physical and social environments.

Information Systems and Public Agencies

One of the most significant impacts of technological advancement has been the digitization of our public institutions and the modes of engagement with citizens and service delivery. Information systems has profoundly transformed the way public institutions conduct their routine internal operations and the way they interact with and deliver services to their citizens (Rowe and Frewer, 2005; Desouza and Bhagwatwar, 2012a; 2012b).

Information systems also plays a central role in how governments engage with citizens to solicit feedback, evaluate policies, and co-create public services. In cities across the US (e.g. SpeakUpAustin.org in Austin, Texas), technology-enabled crowdsourcing platforms are used to solicit ideas from citizens, ideate on options for public projects, and even conduct online votes on ideas to advance (Desouza and Bhagwatwar, 2012b).

Information systems can also open up government and permit easier collaboration with a range of external actors. Platforms such as Challenge.gov (Mergel and Desouza, 2013) promote the co-creation of public innovation by fostering networks of innovators and the development of innovative solutions by leveraging external actors outside the confines of the public workforce.

Increasingly, governments are using sophisticated algorithms to make decisions about housing, immigration, healthcare, and even criminal justice. As far back as 2012, the New Orleans police department commissioned Palantir, a data analytics firm, to create a state-of-the art predictive policing system to identify individuals

[18] Gillespie, T. (n.d.) Can an Algorithm be Wrong? Limn. Retrieved from https://limn.it/articles/can-an-algorithm-be-wrong/
[19] Darrah, K. (2017, November 14). The troubling influence algorithms have on how we make decisions. The New Economy. Retrieved from https://www.theneweconomy.com/technology/the-troubling-influence-algorithms-have-on-how-we-make-decisions

predicted to commit or be a victim of criminal behavior[20]. In 2017, Fairfax's Sydney Morning Herald reported that the Australian government had replaced human decision-makers in its 13 immigration centers that were previously assessing the security risk posed by asylum seekers with computer algorithms[21].

Information systems can also be compromised resulting in large-scale impact on the lives of the masses. For example, in June of 2015 a data breach at the Office of Personnel Management (OPM) resulted in the release of personal records of 4 million people including social security numbers, names, dates of birth and places of birth as well as addresses. Included in the breach was the theft of information collected as part of federal background investigations into existing, former and prospective members of the US Military and the US federal government. In a letter to the OPM director, the president of the American Federation of Government Employees stated "'We believe that the Central Personnel Data File was the targeted database, and that the hackers are now in possession of all personnel data for every federal employee, every federal retiree, and up to one million former federal employees'[22].

US government officials widely believe the OPM breach to have been conducted by an Advanced Persistent Threat (APT) group working for the Chinese military[23]. The suggested motivation for the attack has been the accumulation of a large database of identities to be used for future political, economic and military operations (e.g. blackmail, social engineering, and phishing attacks) against the US. As such the OPM breach impacted public trust in government however the expected fallout is likely to be significantly greater (and more difficult to notice) as these identities are used in future operations that have the potential to cause disruption to democratic processes and political stability.

Information systems and the services they provide can be taken offline as a result of a ransomware attack. Following a similar attack in Atlanta in March of 2018, digital extortionists effectively paralyzed city council services in Baltimore by locking their computer networks in May of 2019[24]. As a result, the citizens of Baltimore could not access essential services such as paying water bills, property taxes and parking tickets. The city was unable to process credit card transactions and its employees were locked out of their email accounts. A key component of the malware used to attack Baltimore was in fact developed by the National Security Agency (NSA)[25]. Code-named Eternal Blue, the tool has been harnessed by hackers to paralyze hospitals, airports, ATMs and even pharamaceutical production facilities producing vaccines. The Baltimore and Atlanta episodes show that weaponizatio of information systems affects all levels of government (federal, state, local).

---

[20] Reisman, D., Whittaker, M., & Crawford, K. (2018, April 10). Algorithms Are Making Government Decisions. The Public Needs to Have a Say. ACLU. Retrieved from https://www.aclu.org/issues/privacy-technology/surveillance-technologies/algorithms-are-making-government-decisions

[21] Bagshaw, E. Koziol, M. (2017, August 26). Computers replace humans in assessing danger of inmates in immigration detention. The Sydney Morning Herald. Retrieved from https://www.smh.com.au/politics/federal/computers-replace-humans-in-assessing-danger-of-inmates-in-immigration-detention-20170825-gy4i19.html

[22] Hackers stole data for every federal employee: union. (2015, June 11). Chicago Tribute. Retrieved from http://www.chicagotribune.com/news/nationworld/ct-federal-data-hackers-20150611-story.html

[23] Koerner, B. (2016, October 23). Inside the Cyberattack That Shocked the US Government. Wired. Retrieved from https://www.wired.com/2016/10/inside-cyberattack-shocked-us-government/

[24] Duncan, I., & Campbell, C. (2019, May 7). Baltimore city government computer network hit bit ransomware attack. The Baltimore Sun. Retrieved from https://www.baltimoresun.com/politics/bs-md-ci-it-outage-20190507-story.html

[25] Perlroth, N. & Shane, S. (2019, May 25). In Baltimore and Beyond, a Stolen NSA Tool Wreaks Havoc. The New York Times. Retrieved from https://www.nytimes.com/2019/05/25/us/nsa-hacking-tool-baltimore.html

Information Systems and Political Processes

Information systems play a key role in election campaigns and in shaping our political processes and public discourse. A number of factors have combined to make this happen. The first factor has been the explosion in the volume and diverse sources of data available on each individual citizen. The second being emergent computational methods that can extract semantic information, conduct social network analysis, and analyze large data sets for correlations and linkages. The third is the ability to create highly accurate models of inference such as voter preferences for individual citizens that have been constructed from datasets of the citizen's past behavior coupled with information about their social activities (friendship networks, social media conversations, likes, dislikes etc.). The fourth factor is advancement in behavioral science that explains how humans can be nudged or persuaded towards particular actions. The fifth factor is the ability to test behavior modification campaigns on a large-scale and in real-time at a relatively low cost. These factors have combined to create an opportunity for 'mass persuasion' as we previously illustrated through the vignette regarding Cambridge Analytica.

Information systems can be creatively used as 'political bots' to influence political campaigns (Escheveria and Zhou, 2017). For example, political bots can raise the profile of a candidate by posing as real followers - the aim being to raise the profile of the candidate and increase the real following through snowballing. Another method is to increase the number of followers to propel the topic to 'trending' status. Public opinion can also be manipulated by having political bots coordinate a campaign promoting positivity or negativity on a particular topic. This tactic has a second order effect as it can manipulate measures of public sentiment that are frequently reported through the news media to further distort perceptions of public sentiment (see our discussion on #releasethememo). Finally, 'astroturfing' is a tactic where an army of political bots are programmed to project a community of citizens that have reached consensus on a topic.

Distributed networks of information systems such as the Internet can be used to create hidden or 'dark spaces' that are not indexed by search engines and where access requires special software. In these 'Dark Webs' or 'DarkNets', rogue actors can conduct activities privately and anonymously outside of the knowledge and jurisdiction of law enforcement. Although frequently referenced in popular media as a marketplace for illicit drugs, the phenomena of Dark Webs provides a haven for actors engaging in a range of illegal activities aimed at political disruption (Gupta, 2017) including: (1) trade in malware and exploits such as zero-day attacks (Ablon et al., 2014; Armin et al., 2015); (2) trade in identities (Broadhurst et al., 2017; Denic, 2017); (3) trade in knowledge (e.g. training, planning and recruitment) (Abbasi, 2007; Broadhurst, 2017; Chen et al., 2008; Ho and Ng, 2016; Scanlon and Gerber, 2014); (4) hiring hacking services (e.g. DDoS, ransomware, malware-as-a-service) Nunes et al., 2016; Tsakalidis and Vergidis, 2017); and (5) money laundering (e.g. bitcoin conversion) Dalins et al., 2017; Moore and Rid, 2016; Sabillon et al., 2016). At the time the Dark Web market Alphabay was shut down in July of 2017, it had over 400,000 users and was engaging in USD $600K-$800K every day making it historically one of the largest Dark Web markets. In addition to trading in illegal drugs, Alphabay transactions included the sale and purchase of hacking tools, the use of cryptocurrencies, and facilitation of money laundering activities that allowed customers to evade international banking infrastructure and the enforcement of economic sanctions[2627]. Dark Web markets remain an important tool for the facilitation of political disruption operations. As part of the investigation into the hacking of the 2016

[26] Jesdanun, A. (2017 July 21). Alphabay: how dark web marketplaces operate like eBay. Independent. Retrieved from https://www.independent.co.uk/news/business/news/alphabay-dark-web-marketplace-ebay-online-us-justice-department-illegal-drugs-a7852486.html

[27] Brewster, T. (2017, July 20). Forget Silk Road, Cops Just Scored Their Biggest Victory Against The Dark Web Drug Trade. Forbes. Retrieved from https://www.forbes.com/sites/thomasbrewster/2017/07/20/alphabay-hansa-dark-web-markets-taken-down-in-massive-drug-bust-operation/#7f631c395b4b

US federal elections, a number of charges were laid against 12 Russian intelligence agents[28]. Among these was the laundering of $95,000 through a complex network of transactions aimed at acquiring and using bitcoin to anonymously purchase tools (e.g. servers, domains) for hacking activities. As the indictment pointed out, a key reason for using bitcoin was to circumvent financial monitoring and controls enforced within traditional banking and finance institutions. The Dark Web can also be used to purchase voter records. As has been reported:

> "In 2017, one anonymous hacker offered more than 40 million voter registration records from at least nine states. Hackers sold copies of the Arkansas and Ohio databases for just $2 each. This year [2018], thousands of voter records from a robocall firm were leaked to the dark web."[29]

Towards a Risk Taxonomy of the Weaponization of Information Systems for Political Disruption

Our critical analysis of the role of information systems in creating political disruption highlights the multifaceted nature of how information systems can be used to create political disruption. An important and novel insight from the critical analysis is that even if information systems are protected they can still be *weaponized* through the compromise of their goals and values to create political disruption (e.g. see the vignette on Cambridge Analytica).

Drawing on the concept of weaponization of information systems we develop a useful tool for security policymakers and practitioners tasked with responding to political disruption. As such, since the aim is to mitigate the risk of such an eventuality we construct a risk-based taxonomy to assist in the practice of risk identification, impact assessment and response formulation to the political system. Our taxonomy provides a useful tool to analyze: (1) the full range of risks, (2) the aggregation of risks, and (3) a comparative analysis of risks over time.

Our contribution to research scholarship is that our taxonomy takes the first step in constructing a comprehensive analysis of how these attacks can take place and the role of actors and information systems in perpetrating the attacks. While there are other taxonomies in the literature (e.g. Killourhy et al., 2004; Simmons et al., 2009; Mirkovic and Reihner, 2004, and Kjaerland, 2006), most focus on protecting information systems and even data. Our ALERT taxonomy goes further by looking at how, even if information systems are protected, their goals and values can be compromised.

We draw on the classic definition of a risk, that being a hazardous scenario where a threat agent adopts a threat vector to create an impact (Webb et al., 2014). Therefore, we articulate hazardous scenarios as a combination of the Actor responsible for instigating, conducting or supporting the attack and the Lever as representing how the Actor can leverage information systems to perpetrate the attack (the threat vector). We articulate the potential impact or Effect (effect is broken down into a primary and secondary effect) and include the element of Response as a mitigation measure.

We use Information Warfare (IW) as the overarching term that encompasses the range of activities involving weaponization of information systems for the purpose of political disruption (Futter, 2018). Where IW is conducted specifically through digital networks against information systems we use the term Computer

---

[28] Gensler, G. (2018, July 18). Cryptocurrencies: Oversight of New Assets in the Digital Age. Transcript of Speech to Committee on Agriculture: United States House of Representatives. Retrieved from https://docs.house.gov/meetings/AG/AG00/20180718/108562/HHRG-115-AG00-Wstate-GenslerG-20180718.pdf

[29] Patterson, D. (2018, September 26). The dark web is where hackers buy the tools to subvert elections. CBS News. Retrieved from https://www.cbsnews.com/news/campaign-2018-election-hacking-the-dark-web/

Network Operations (CNOs). If the operation aims to specifically disrupt information systems (e.g. an attack on a power grid) we use the term Computer Network Attack (CNA) as opposed to Computer Network Exploitation (CNE) where the aim is theft of information / data. Where the security of computing devices, IT networks and data/information are concerned we use the overarching term Computer Network Defense (CND).

We will now describe the elements of our taxonomy – actors, levers, effects and responses.

Actors

An actor is any agent and/or organization that either 1) instigates the attack, 2) supports any aspect of planning the attack (e.g. through provision of funding, computing resources, and even human experts), 3) conducts the actual attack, 4) knowingly supports the concealment of the attack and/or source of the attack, and 5) unknowingly amplifies the attack due to their actions.

Russia is a prime example of an actor that deliberately instigates IW operations for the purposes of political manipulation. The Russian president Vladimir Putin frequently walks the fine line between using state resources to execute a computer network attack (as described in our vignettes) and instigating said attacks. In June of 2017 on the topic of the hacking the US Democratic National Committee he stated 'If they are patriotically minded, they start making their contributions – which are right, from their point of view – to the fight against those who say bad things about Russia'[30].

The recent arrest of Elena Alekseevna Khusyaynova for funding the Russian online propaganda campaigns in the 2016 and 2018 midterm elections is an example of an individual that supported the planning of attacks but was not involved in the execution of the attack itself [31]. The funds were used to buy information systems services (storage space on secure servers, domain names, social media analytics), online advertisements and to organize political rallies and protests.

We have presented a number of examples of actors that have weaponized information systems for political disruption. Key among these has been Russia (e.g. the hack of the 2016 US federal elections, #releasethememo campaign, attacks against Ukraine). However, in addition to Israel (Unit 8200 of the Israeli Intelligence Corp) and North Korea (the exploits of Park Jin Jyok and Korea Expo Joint Venture), China also uses weaponized information systems for political purposes (albeit the primary focus of China's CNOs activities has been industrial espionage and the theft of Intellectual Property). In 2013 Chinese hackers stole emails, files and contact lists of journalists from the New York Times, the Washington Post and the Wall Street Journal as part of what is believed to be a long-standing campaign of monitoring Western news coverage of China[32]. China has also hacked into the email accounts of the political leaders of its minority Tibetan and Uighur communities[33].

An example of a category of actor that weaponizes information systems to massive effect is Advanced Persistent Threat (APT). An APT is "An entity that engages in a malicious, organized, and highly sophisticated long-term or reiterated network intrusion and exploitation operation to obtain information from a target organisation, sabotage its operations, or both" (Ahmad et al., 2019). Examples of APTs are IW units attached to military forces around the world such as Unit 8200 of the Israeli intelligence Corp, the

[30] Townsend, K. (2017, June 6). Russian Outsourcing Provides Plausible Deniability for State-Sponsored Hacking. Security Week. Retrieved from https://www.securityweek.com/russian-outsourcing-provides-plausible-deniability-state-sponsored-hacking

[31] Polantz., K. (2018, October 19). Russian national charged with attempting to interfere in 2018 midterms. CNN. Retrieved from https://edition.cnn.com/2018/10/19/politics/elena-alekseevna-khusyaynova-russia-charged/index.html

[32] Perlroth, N. (2013, February 1). Washington Post Joins List of News Media Hacked by the Chinese. The New York Times. Retrieved from https://www.nytimes.com/2013/02/02/technology/washington-posts-joins-list-of-media-hacked-by-the-chinese.html

[33] Menn, J. (2016, January 1). Microsoft failed to warn victims of Chinese email hack: former employees. Reuters. Retrieved from https://www.reuters.com/article/us-microsoft-china-insight-idUSKBN0UE01Z20160101

Russian GRU affiliated team known as Fancy Bear, and Unit 61398 of the People's Liberation Army of China[34].

Actors might also include organizations that knowingly conceal an attack such as shell corporations that can anonymously transfer funds and engage in business transactions such as those located notoriously in Panama and the Cayman Islands but also within Western countries such as the US[35]. In what has been described as the largest hacking scheme in history targeting among others the US' largest bank JP Morgan and Dow Jones & Co, 75 shell companies and accounts around the world were used to launder money in 2007. The category also includes actors that conceal previous incidents where data has been compromised. For example, Uber suffered a breach whereby the personal data of 57 million customers and drivers was stolen in October of 2016[36]. Not only did the company not inform the affected customers of the breach but it actively tried to conceal the incident by paying $100,000 to the hackers for their silence (and for destroying the data).

An example of the final category of actor is the news media as it provides a platform through which messages can reach large audiences. For example, in the case of the Russian hacking of the Democratic National Convention, the New York Times reported that "Dozens of newspapers, television stations, bloggers and radio stations around the United States — including The New York Times, The Washington Post and The Wall Street Journal — pursued reporting based on the hacked material, significantly increasing the effects of the cyberattack[37]".

Actors can also operate at various levels from individuals, to groups, and even fully-fledged organizations. A class of organizations that have received relatively little attention when it comes to IW-influence operations is private military contractors (PMCs). PMCs have long played a critical role in international conflict and security operations. Leading PMCs have developed significant information warfare capabilities that can be leveraged for political disruption. Given the fact that PMCs often operate in grey zones when it comes to applications of laws and conventions, they have become increasingly attractive for carrying out information warfare engagements.[38] PMCs have the advantage of ensuring that they meet stringent security requirements of a state actor, while still being able to conduct operations that are state-supported and are hard to trace back to the original sponsor. PMCs operate within robust networks and their ecosystems are well-resourced so as to ensure global reach and sufficient local knowledge to conduct IW-interference operations.

Actors can be state supported, state sponsored, or non-state actors. An example of a state actor is Unit 8200 of the Israeli Intelligence Corp, widely believed to have been responsible for creating Stuxnet, the computer worm used to destroy the centrifuges in Iran's nuclear facilities in 2010[39]. Fancy Bear, a state-sponsored actor, is widely believed to be associated with Russian intelligence[40]. The actor has conducted many attacks targeting European governments and their armed forces, private corporations especially those linked to the military, but also run political influence campaigns. Non-state actors tend to be motivated by ideology (e.g. ISIS that tend to weaponize social media to recruit like-minded individuals that can cause political disruption outside of

[34] Cooper, H. (2018, June 8). Chinese Hackers Steal Unclassified Data From Navy Contractor. The New York Times. Retrieved from https://www.nytimes.com/2018/06/08/us/politics/china-hack-navy-contractor-.html
[35] Hicken, M. Ellis, B.(2015, December 9). These U.S. companies hide drug dealers, mobsters and terrorists. CNN. Retrieved from https://money.cnn.com/2015/12/09/news/shell-companies-crime/index.html
[36] Wong, J. (2017, Nov 22). Uber concealed massive hack that exposed data of 57m users and drivers. The Guardian. Retrieved from https://www.theguardian.com/technology/2017/nov/21/uber-data-hack-cyber-attack
[37] Following the Links From Russian Hackers to the U.S. Election. (2017, January 6). The New York Times. Retrieved from https://www.nytimes.com/interactive/2016/07/27/us/politics/trail-of-dnc-emails-russia-hacking.html
[38] Jeter, C. (2011, January 6). Hired guns: Cyberwarfare and cyber-mercs. SC Media. Retrieved from https://www.scmagazine.com/home/other/test-eset/hired-guns-cyberwarfare-and-cyber-mercs/
[39] Halliday, J. (2010, September 25). Stuxnet worm is the 'work of a national government agency'. The Guardian. Retrieved from https://www.theguardian.com/technology/2010/sep/24/stuxnet-worm-national-agency
[40] Satter, R., Donn, J. & Myers, J. (2017, November 2). Digital hit list shows Russian hacking went well beyond U.S. elections. Chicago Tribune. Retrieved from http://www.chicagotribune.com/news/nationworld/ct-russian-hacking-20171102-story.html

their immediate zone of conflict such as the US, UK and Australia)[41] or profit (e.g. Silence, responsible for stealing $800k from banking, ecommerce and news-media in Europe) [42].

The differences between these are non-trivial and have implications for the range of options actors have to conduct an attack. Whereas in the recent Cold War, most such conflicts were perpetrated by nation-states against other nation-states. However, in the modern era the weaponization of information systems has transformed the landscape to a crowded and connected ecosystem of actors that cooperate with one another, hedge their risks, and seek anonymity (see Figure 1 for a taxonomic view of actors).

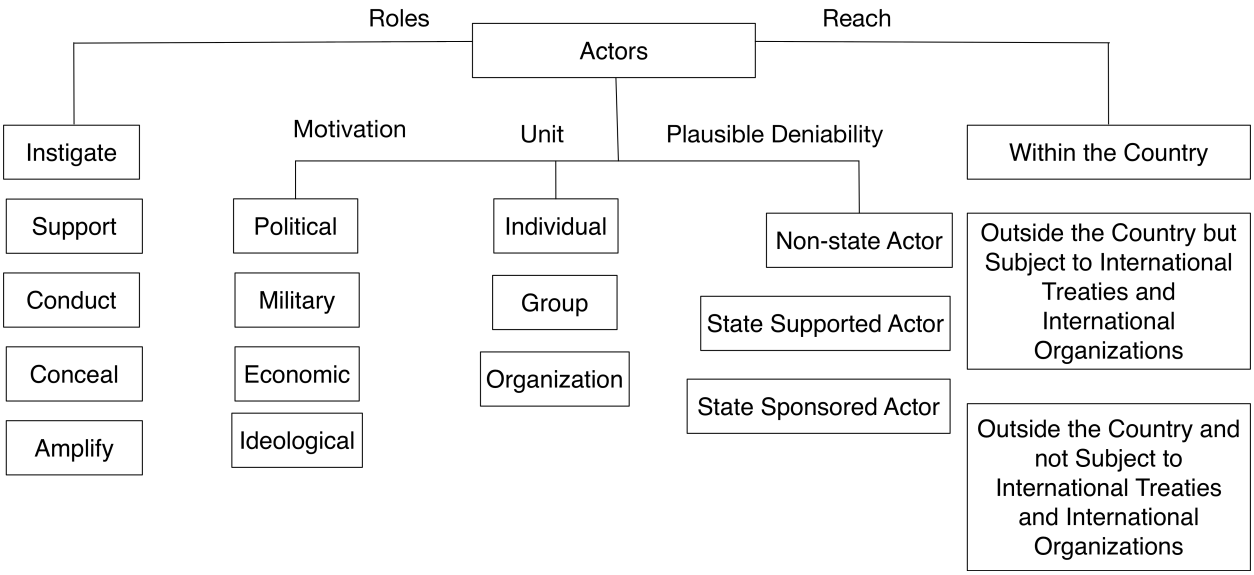

Figure 1: Taxonomic view of actors

An actor might take on active or passive role. Unlike in the majority of cases where actors directly engage in IW attacks against targets, some actors may adopt a more passive role allowing a proxy to conduct the attacks on their behalf. A key reason for this approach is the advantage of plausible deniability to remain immune from retaliatory measures and/or to buy time while the actor's interests are progressed. For example, pro-Russian hackers launched computer network attacks against Ukraine in 2016 as part of a larger campaign involving disinformation and unmarked special forces troops to consolidate the Russian position in the Crimea[43].

Actors reside within their target's environment (e.g. an actor who resides within the country they are seeking to attack, versus one that is operating from abroad). The former is subject to the country's law enforcement and legal systems versus the latter gets more complicated due to operating across international jurisdictions. An example of the former is the Arab Spring revolution which saw the Islamic Brotherhood party utilize social media to recruit and organize a leaderless resistance movement that successfully toppled the Egyptian government. Examples of the latter are numerous – the majority of instances discussed in this paper relate to actors that use weaponized information systems across jurisdictions to achieve their objectives.

---

[41] Callimachi, R. (2017, February 4). Not 'Lone Wolves' After All: How ISIS Guides World's Terror Plots From Afar. The New York Times. Retrieved from https://www.nytimes.com/2017/02/04/world/asia/isis-messaging-app-terror-plot.html

[42] Vijayan, J. (2018, September 5). Silence Group Quietly Emerges as New Threat to Banks. *Dark Reading*, Retrieved from https://www.darkreading.com/attacks-breaches/silence-group-quietly-emerges-as-new-threat-to-banks/d/d-id/1332742.

[43] Stowell, J. (2018, March 22). "Plausible Deniability" in Russia's Hybrid War in Ukraine. Global Security Review. Retrieved from https://globalsecurityreview.com/plausible-deniability-russias-hybrid-war-ukraine/

Actors have varying motivational factors that, in effect, shape the outcome of their acts. For instance, a state actor is generally driven by political, military and economic factors – an example of a campaign motivated by political strategy is the Russian campaign to influence the outcome of the US federal election of 2016 as described in the first of our three vignettes. Non-state actors may be motivated by ideology to raise funds, disseminate propaganda and recruit members from outside their locality using social media as in aforementioned example of the Arab Spring. Advanced Persistent Threats, such as Fancy Bear or PLA Unit 61398, target large enterprises and government bodies for political and economic gains. In contrast, acquiring trade secrets, business communication, product designs etc. motivate actors engaged in industrial or corporate espionage. Once a motive is established, actors need a medium or lever to inflict damage on the targeted entity, which could be an organization, enterprise or even a nation state.

Levers

Levers represent how actors can leverage information systems to interfere and compromise. Levers exist at four levels in our taxonomy (described below from lowest to highest in Figure 2):

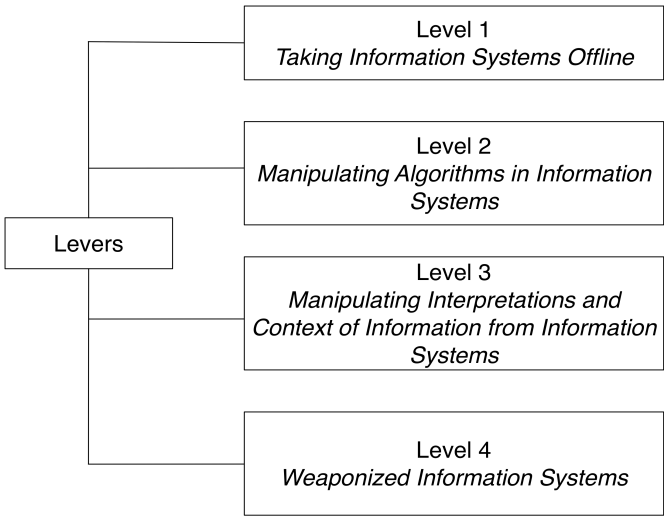

Figure 2: Levels of levers used by actors to interfere and compromise

Disrupting Sources of data in physical and logical systems (Level 1)

The lowest level of lever represents the disruption of sources of data. Sources are physical and logical systems that generate signals of interest. In the context of political disruption, these can involve systems that calibrate votes and transaction processing systems that authenticate voter registration among others. At the lowest level one can think of these systems being taken offline, held for ransom, or destroyed. An example of a level one lever is the WannaCry ransomware attack against UK hospitals described in our introduction to this paper. The ransomware attack disrupted the hospitals' access to medical records (taking their IT systems offline for a prolonged period) forcing them to cancel non-emergency procedures and reverting their routine operations to pen and paper. The Sednit/APT28 espionage campaign launched by Russian hackers in 2013, targeted South African embassies via an infected document sent to the embassies purporting to be from the Department of International Relations and Cooperation[44]. A ransomware attack on Riviera Beach[45], Florida

[44] FireEye. (2016). APT28: A window into Russia's cyber espionage operations? Retrieved from https://www.fireeye.com/current-threats/apt-groups/rpt-apt28.html

[45] Mazzie, P. (2019, June 19). Hit by Ransomware Attack, Florida City Agrees to Pay Hackers $600,000. The New York Time. Retrieved from https://www.nytimes.com/2019/06/19/us/florida-riviera-beach-hacking-ransom.html?action=click&module=Well&pgtype=Homepage&section=US

resulted in the city council paying a $600,000 ransom after hackers paralyzed the city's computer systems. The Riviera Beach attack started after a police department employee opened an infected email attachment.

Manipulating algorithms used in the processing of signals (Level Two)

At the next level (level two), levers can be manipulations to the algorithms used in the processing of signals. Here, the lever is in the manipulation of the data processing elements, thereby rendering the outputs useless and compromised. An example of the manipulation of an algorithm is the hacking of biometrics by exploiting their tolerance for minor changes in the biometric traits of authenticated users. This is done by gradually shifting the system's recognition of the authorized user to that of an unauthorized user[46]. The same principle of exploiting tolerances can be used to evade email filtering algorithms that protect organizations from links to malware. Another example is the concept of the 'AI nudge', i.e. persuading algorithms to change through collective human behavior. An experiment run by an MIT student demonstrated how the act of prodding users to behave in a particular way can change the behavior of an algorithm which, in turn, affects other users[47].

Manipulating interpretations associated with information (Level Three)

At the next higher level (level three), levers can involve manipulating the interpretations associated with information. This takes the form of either 1) placing valid information in a false context that is artificially generated, or 2) placing invalid information (e.g. fake news) within a true context. An example of how interpretations can be manipulated is the Russian twitter campaign #releasethememo that we discussed in the vignettes. The campaign amplified what was a false context – that there existed a secret memo that implicated the Obama administration in abuses of the Foreign Intelligence Services Act – to force the release of the memo into the public arena. In this way the coupling of private infrastructure platforms (e.g. Facebook and Twitter) and the democratized access to computational resources and expertise presents new challenges. Actors are able to perpetrate influence campaigns to sabotage public agencies on private platforms that were never designed to be used for political discourse. Another example is the technique of posting a strongly contrasting comment in order to manipulate the way readers interpret information. Figure 3 juxtaposes a positive and a negative comment to a post by Democrat nominee Hilary Clinton (Alashri et al., 2018).

[46] Radinsky, K. (2016, January 5). Your Algorithms Are Not Safe from Hackers. Harvard Business Review. Retrieved from https://hbr.org/2016/01/your-algorithms-are-not-safe-from-hackers

[47] Campbell-Dollaghan, K. (2017, January 3). The Art of Manipulating Algorithms. Fast Company. Retrieved from https://www.fastcompany.com/3068556/reminder-you-can-manipulate-algorithms-too

Figure 3: An example of interpretation manipulation of information

Advancements in video and audio editing have introduced a suite of new opportunities to manipulate interpretations of information. A recent article in the Washington Post profiled a range of editing techniques that can be used for political manipulation[48]. For example, the increasingly sophisticated and compelling outcomes from the superimposing of one individual's face on another individual's body using easy-to-use tools for the common person. Another example is manipulating an audience's reaction to a photograph by modifying the gaze of the subject in the image. An even more powerful technique is changing the expressions and mouth movements of subjects in video footage to make them appear to say something that they never said. In particular, in 2016 a group of researchers produced Face2Face, a process by which one individual's live expressions can be transferred to a subject in a video. Further, the context of spoken words can be changed by taking words spoken by a subject in one video and transferring it to another video (the trick being to correct the target video for mouth movements so the words appear to have been actually said). Another example of technological advancement is the generation of fake human faces and human voices from scratch that are realistic and unique but have never actually existed. This technique can be used to strengthen the apparent authenticity of social media accounts and communications and to create witnesses to events that don't exist. Recently, videos of House Speaker Nancy Pelosi were deceptively edited to make it appear that she had trouble speaking. The videos were likely aimed at creating a false narrative to manipulate political discourse in the US[49]. Other techniques allow for the manipulation of the words of a subject using samples of their own voice, and manipulating the appearance of a location where an important event took place.

Weaponizing information systems (Level Four)

At the final level (level four), we have information systems that are fully weaponized to cause direct political, physical, economic, and social damage. The Distributed Denial of Service (DDoS) attack against Dyn in 2016 was perpetrated using the Internet of Things (IoT)[50]. A large number of devices such as cameras and baby monitors that were infected using malware named Mirai were coordinated in a botnet attack against Internet services across Europe and North America resulting in major interruptions to their services. In February of 2019, the Ukrainian Central Election Commission (CEC) was subjected to a DDoS attack only weeks before the presidential election[51]. The Ukrainian government accused Russia of orchestrating the attack to influence the outcome of the election.

Effects

The levers act as the means for actors to achieve an effect on the targeted individual, organization or the country. Actors can use one or a mix of these to maximize the intended effect. The December 2015 Ukraine power grid CNA involved a malware attack on the supervisory control and data acquisition (SCADA) systems followed by a denial-of-service attack on a call center which denied consumers of access to information regarding the blackout. In 2013, the South African Police Service[52] website suffered a denial-of-service attack followed by the hacking of their communication servers which resulted in the release of approximately 16,000 details of whistleblowers and victims. Disinformation or manipulation of information using tools like

[48] Bump, P. (2018, February 12). Here are the tools that could be used to create the fake news of the future. The Washington Post. Retrieved from https://www.washingtonpost.com/news/politics/wp/2018/02/12/here-are-the-tools-that-could-be-used-to-create-the-fake-news-of-the-future/?noredirect=on&utm_term=.1b296071664a

[49] Abbruzzese, J. (2019, May 25). Doctored Pelosi videos offer a warning: The Interet isn't ready for 2020. NBC News. Retrieved from https://www.nbcnews.com/tech/tech-news/doctored-pelosi-videos-offer-warning-internet-isn-t-ready-2020-n1010011

[50] Franceschi-Bicchierai, L. (2016, October 22). Blame the Internet of Things for Destroying the Internet Today. Motherboard. Retrieved from https://motherboard.vice.com/en_us/article/vv7xg9/blame-the-internet-of-things-for-destroying-the-internet-today

[51] Lyngaas, S. (2019, Feb 26). Ukraine's president accuses Russia of launching cyberattack against election commission. Cyberscoop. Retrieved from https://www.cyberscoop.com/ukraines-president-accuses-russia-launching-cyberattack-election-commission/

[52] Tubbs, B. (2013, May 22). SAPS hack spells negligence. I T We b. Retrieved from http://www.itweb.co.za/index.php?option=com_content&view=article&id=64268:SAPS-hack-spells-negligence&catid=265

Face2Face is quite likely to be leveraged during vulnerable times such as election campaigns, social unrests, ethnic conflicts, or geopolitical standoffs.[53] The ultimate aim of any IW attack is to inflict damage on the targeted entity, which could be monetary, loss of information, loss of reputation, service disruption, or undermining confidence of citizens in their respective governments or state agencies and institutions.

Most effects have a cause, and effects frequently become causes of other effects[54]. In this way, the phenomena of cause and effect can occur in chains. Further, an effect that was planned can cause a secondary effect that was unplanned or unintentional and may actually be detrimental to the original intent. For every combination of actor and lever, one must account for 'first order' effects and 'second order' effects as a means of distinguishing between immediate and later consequences of an act. ISIS' weaponization of social media as a means of projecting their power and influence is an example of a cause that has first order and second order effects. The first order effect of their social media campaign is to create a sympathetic community that acts as an echo chamber for their political propaganda (Awan, 2017). The second order effect is that the ISIS followers recruit more followers, collect funds, and organize acts of war in support of ISIS objectives.

In addition to the chaining of the cause-effect relationship, we suggest that effects can also be categorized into three types: (1) IW-influence effects, where dialogue is shaped passively and through agents; (2) IW-interference effects, where dialogue is shaped actively for example through bots etc.; and (3) IW-hacking, where systems and infrastructures are compromised and/or damaged and data/information is stolen or otherwise compromised. IW can take various forms of effects on the targeted entity. They could lead to social unrest or undermining trust of people in their governments, if electoral processes and institutions are targeted. Terrorist propaganda can have social and psychological effects, as it instills fear in the mind of the onlookers distanced apart. Industrial and economic espionage can undermine business and economic growth with loss of intellectual property. Since information systems and physical linkages connect the infrastructure, disruptions at one point could be cascading, escalating or dampening as they traverse across the organizations, society and economy. Attacks on critical infrastructure, such as electricity grids, can easily cascade to other sectors. A grid blackout can essentially bring urban transportation, railways and communications to a standstill. Wannacry ransomware, in contrast, had an escalating effect as it spread to the hospitals in the UK forcing them to cancel non-emergency procedures[55], which was not the apparent effect the actor wanted to achieve from the ransomware. A key example of a dampening effect is the French Presidential elections of 2017, when leaked data from Emmanuel Macron's election campaign was dumped on Pastebin just 36 hours before the elections. The swift action on the part of the French electoral authority CNCCEP as well as the ethical standards adopted by the media[56] and the citizens ensured that the repercussions of the electoral intervention were warded off and the actors failed to influence the outcome of the elections – the apparent effect actor wanted to achieve.

Information systems play a key role in our political processes, and also in shaping and aggregating political sentiment, which ultimately defines electoral outcomes in democratic societies. Effects take shape when the actors exploit the vulnerabilities, which are either sown with the information systems or exist in the

---

[53] Solon, O. (2017, July 26). The future of fake news: don't believe everything you read, see or hear. The Guardian. Retrieved from https://www.theguardian.com/technology/2017/jul/26/fake-news-obama-video-trump-face2face-doctored-content

[54] Miller, M. (2006, Summer). Thinking About Second & Third Order Effects: A Sample (And Simple) Methodology. Retrieved from http://www.au.af.mil/info-ops/iosphere/iosphere_summer06_miller.pdf

[55] Dearden, L. (2017, August 26). NHS trust hit by cyber attack cancels operations and asks patients not to come to hospital 'unless it is essential'. Independent. Retrieved from https://www.independent.co.uk/news/uk/home-news/cyber-attacks-uk-nhs-lanarkshire-scotland-hospitals-affected-patients-operations-ransomware-wannacry-a7913896.html

[56] Conley, Heather A. (2018, June 21). Successfully Countering Russian Electoral Interference. Center for Strategic and International Studies. Retrieved from https://www.csis.org/analysis/successfully-countering-russian-electoral-interference

interpretation of information itself. Appropriate responses to deny the adversary from exploiting these vulnerabilities are the means available to the defenders to either reduce or manage the effects of IW.

Responses

Responses are the set of choices available to nations that have been targeted by IW. Responses can be categorized into four categories of measures: (1) IW defense, (2) IW offense, (3) diplomacy, (4) legal sanctions, and (5) economic sanctions. These measures are the full spectrum of response options available before the countries, which could be exercised individually or as an amalgamation. The anticipated effect of stringent responses is to inflict heavy cost on the perpetrators that could deter future attacks. Defensive and offensive means allow countries to practice deterrence by denial and deterrence by punishment to defend their legitimate interests in the cyberspace. IW defense and offense are exercised through cyberspace thereof, but the other three encompass foreign policy, trade, economics and legal frameworks, both with in the domestic and international realms.

IW defense focuses on hardening information systems from attack. Inputs to the hardening strategy can come from a range of sources including past learning from IW attacks and knowledge sharing through domestic and international collaborations. In September of 2012 the US experienced a massive DDoS attack against six leading banks[57]. The fallout from the attack was addressed by the banks themselves with the assistance of federal government officials. Although a IW offense or 'hack back' option was considered, it was rejected out of fear that the situation would escalate. The option of a diplomatic formal warning was also rejected for the same reason. Ultimately, the US government responded using diplomatic channels to prevent hackers from using servers on international networks as 'springboards'. This technical measure is credited with substantially reducing the impact of IW attacks.

IW offense is the oft discussed 'hack back' or retaliation against weaponized information systems. To date there appears to be little evidence that major IW attacks against the West have been met with proportionate retaliation. However, the long-standing US position on avoiding escalation of IW conflicts through retaliation appears to have reversed. In August of 2018 the Trump administration issued Presidential Policy Directive 20 allowing the use of IW means to preempt, interrupt or retaliate against an adversary's IW capability or attack[58]. In contrast to the US position, attacks against Israel have not gone unanswered. In 2013 Anonymous launched a large-scale CNO against Israeli government websites claiming to have caused over $3 billion in damages. The Israelis reacted within a few hours compromising the website set up by Anonymous for the attack and replacing the messages with the Israeli national anthem[59].

Diplomacy is the concerted action by the international community to establish norms and rules for 'cyberspace'. When Estonia experienced a Russian DDoS attack in 2007 resulting in the shutting down of government ministries, banks and media, the government focused on restoring its services and channeling international assistance through its Computer Emergency Response Team (CERT). Although the Estonian ministry of foreign affairs chose to make a public statement identifying Russia as the source of attack, its

[57] Foreign Policy Responses to International Cyber-attacks Some Lessons Learned (2015, September). Clingendael Netherlands Institute of International Relations. Retrieved from https://www.clingendael.org/sites/default/files/pdfs/Clingendael_Policy_Brief_Foreign%20Policy%20Responses_September2015.pdf

[58] Nakashima, E. (2018, August 16). Trump gives the military more latitude to use offensive cyber tools against adversaries. The Washington Post. Retrieved from https://www.washingtonpost.com/world/national-security/trump-gives-the-military-more-latitude-to-use-offensive-cyber-tools-against-adversaries/2018/08/16/75f7a100-a160-11e8-8e87-c869fe70a721_story.html?noredirect=on&utm_term=.f6ff2265166b

[59] Estes, A. (2013, April 7). Anonymous Hits Israel with a Massive Cyber Attack, Israel Attacks Back. The Atlantic. Retrieved from https://www.theatlantic.com/international/archive/2013/04/anonymous-hits-israel-massive-cyber-attack-israel-attacks-back/316538/

primary efforts were diplomatic and long-term – aimed at raising awareness of the problem among its European and NATO allies and seeking investment into an IW defense research center.

In retaliation for hacking the 2016 federal election, the US government expelled 35 suspected Russian intelligence operatives and imposed sanctions on Russia's primary intelligence agencies[60]. Two waterfront estates were also shut down as part of the retaliatory measures. Russia immediately responded by expelling 755 members of 1000 strong American diplomatic mission[61].

Legal sanctions are penalties used to enforce obedience with the law typically applied by a state to a sub-state entity. In February of 2018, the US Department of Justice indicted 13 Russian nationals and 3 companies for wanting to 'promote discord in the United States and undermine public confidence in democracy' in relation to the hacking of the 2016 federal election. None of the Russian nationals were arrested (and are likely to be in the future) however the indictment makes it difficult for the entities to continue their operations undetected[62]. Legal sanctions tend to be more effective on offending domestic parties as they operate within the enforceable reach of local laws. The Cambridge Analytica scandal led to Facebook being fined 500,000 pounds sterling for failing to protect user data and for failing to be transparent about how the data was used by third parties[63].

Economic sanctions are commercial and financial penalties applied by one or more countries to the perpetrating party. In 2014 a group calling themselves the Guardians of Peace penetrated Sony Pictures Entertainment and began a campaign of extortion by periodically releasing sensitive corporate information while demanding money to cease their activities[64]. The US retaliated with limited economic sanctions (prohibiting US entities from engaging with any business relationship) against Park Jin Jyok, a programmer, and Korea Expo Joint Venture – both linked to North Korea. The entities were deemed responsible for the Sony hack, the WannaCry ransomware attack of 2017 and for participating in the theft of $81 million from a bank in Bangladesh[65].

Economic sanctions that have been leveled by the US as part of its arsenal of financial weapons of warfare include (1) the freezing of assets, (2) importing tariffs, (3) creating barriers to trade, (3) imposing travel restrictions on entities, and (4) embargoes (Lin, 2016). Anti-money laundering measures exist to control the flow of resources to and from designated actors. These are implemented by financial institutions and require them to monitor and report suspect financial transactions. Access to the global banking system can also be controlled effectively isolating countries, organizations or individuals and preventing them from engaging in transactions and/or securing funding for their activities.

The cases of the Sony Pictures hack and Wannacry ransomware saw the US and UK making a public attribution to the actors involved in the attacks. Attribution of CNOs involves thorough analysis of sparse factors such as the geopolitical context, political and economic relations of the states, intelligence inputs,

---

[60] Sanger, D. (2016, December 29). Obama Strikes Back at Russia for Election Hacking. The New York Times. Retrieved from https://www.nytimes.com/2016/12/29/us/politics/russia-election-hacking-sanctions.html?module=inline&login=email&auth=login-email

[61] MacFarguhar, N. (2017, July 30). Putin, Responding to Sanctions, Orders U.S. to Cut Diplomatic Staff by 755. The New York Times. Retrieved from https://www.nytimes.com/2017/07/30/world/europe/russia-sanctions-us-diplomats-expelled.html

[62] Apuzzo, M. & LaFraniere, S. (2018, February 16). 13 Russians Indicted as Mueller Reveals Effort to Aid Trump Campaign. The New York Times. Retrieved from https://www.nytimes.com/2018/02/16/us/politics/russians-indicted-mueller-election-interference.html

[63] Hern, A. & Pegg, D. (2018, July 11). Facebook fined for data breaches in Cambridge Analytica scandal. The Guardian. Retrieved from https://www.theguardian.com/technology/2018/jul/11/facebook-fined-for-data-breaches-in-cambridge-analytica-scandal

[64] ibid

[65] Whittaker, Z. (n.d.) US Treasury sanctions North Korea over Sony hack and WannaCry attack. TechCrunch. Retrieved from https://techcrunch.com/2018/09/06/us-treasury-sanctions-north-korean-hackers-over-sony-hack-wannacry-attack/

behavioral analysis and source code examination. Attribution with high certainty allows the country to justify the above stated response options to the domestic populace and the international community. Given the wide range of actors with varying capabilities, the levers they can employ, and the extent of possible effects deem it necessary to have a framework or classification to exercise the right response option.

ALERT: Actor, Lever, Effect, Response Taxonomy

Table 1 below links the elements of the taxonomy and demonstrate the utility of ALERT using selected representative examples. Two points are worth nothing. The cases described within the table are *illustrative* and not meant to signify that we only expect attacks that are exactly similar to the cases that will happen in the future. The cases are historic reference points of what these kinds of attack have looked like in the past. Going forward, we would expect the attacks to have similar signatures but be far more advanced.

Actor	Lever	1st Order Effect	2nd Order Effect	Response (examples)
Non-State (Organization) Actor: Hacktivist group Anonymous	**Level 1: Compromising Source Systems** Hacking of the South African Police service website[52]52	**IW-hacking:** Small to medium scale disruptions; Nuisance	Misuse of information; Loss of reputation; Low confidence in government agencies or bodies	Investment in IW defense and CND including awareness campaigns aimed at public/private institutions; Public Attribution; In practice it is difficult to retaliate against actors that have (1) plausible deniability; (2) are mobile; (3) operate outside the target's legal jurisdiction
State-Supported Actor: widely believed to be Hackers working for China	**Level 1: Compromising Source Systems** Data breach at the U.S. Office of Personnel Management (OPM)[22]. (Theft of personally identifiable information)	**IW-hacking:** Exposed background investigations and fingerprint data on millions of American citizens; Loss or theft of information	Fraud; Misuse of information; Low confidence in government agencies or bodies.	Investment in IW defense and CND including awareness campaigns aimed at public/private institutions; Retaliation and Sanctions through Global Governance Bodies
State-Sponsored Actor: Shadow Brokers	**Level 1: Compromising Source Systems** WannaCry Ransomware attack rendered medical records inaccessible, systems were frozen, and files were encrypted[16];	**IW-hacking:** May, 2017 (UK) 16 hospitals had to shut down non-critical operations; globally 300,000 systems in Russia, Taiwan, Ukraine and India affected.	Social unrest if the government fails to restore essential services (healthcare, electricity, transportation etc.)	Investment in IW defense and CND including awareness campaigns aimed at public/private institutions; Retaliation and Sanctions through Global Governance Bodies; Public Attribution In practice it is difficult to retaliate against actors that have (1) plausible deniability; (2) are mobile; (3) operate outside the target's legal jurisdiction

Actor	Lever	1st Order Effect	2nd Order Effect	Response (examples)
Non-State (Organization) Actor: Twitter	**Level 2: Compromising Algorithms** Twitter is accused of engaging in 'algorithmic censorship' of #occupywallstreet[18]	**IW-influence:** Twitter did not show the topic trending even in cities where protests were being held and tweets were spiking	Shaping or controlling opinion formulation; Information suppression; Loss of reputation if the actor has a brand value.	Retaliation and Sanctions through Global Governance Bodies; Public Attribution; Legal action if the entity has a registered office in the country In practice it is difficult to retaliate against actors that have plausible deniability
State-Supported Actor: widely believed to be the Syrian Electronic Army	**Level 2: Compromising Algorithms** Twitter handle of Associated Press was hacked and used to put out a message reading "Two explosions in the White House and Barack Obama is injured."[66]	**IW-influence:** This message caused a drop and recovery of roughly $136 billion in equity market value over a period of about five minutes.	Monetary loss; Loss of reputation for the entities targeted;	Public attribution; Investment in IW defense
State-Sponsored Actor: Bangladesh Bank Heist	**Level 2: Compromising Algorithms** In 2016, North Korean hackers carried out an $81 million heist by breaching Bangladesh Bank's systems and using the SWIFT network.	**IW-hacking:** Monetary loss.	Loss of reputation for government agencies.	Legal actions; Public attribution; Investment in IW defense
Non-State Organization Actor: ISIS	**Level 3: Manipulating Information Interpretations** Insurgent movements exploit the decentralised and colloquial nature of social media to counter main-stream narratives and recruit followers in foreign countries to extend their influence and the boundaries of the conflict to societies with softer targets[67]	**IW-interference:** Recruitment of followers outside of the conflict zone to commit acts of war; Terrorizing people outside of the conflict zone	Law and order issue in countries prone to terrorism; Spike in lone wolf terror attacks	Legal sanctions; Economic Sanctions; IW offense including propagating a counter narrative
Non-state Actor / State-Supported Actor: Cambridge Analytica / **State Supported Actor:** Russian State	**Level 3: Manipulating Information Interpretations** Using social media messaging to undermine the credibility of the electoral system and particular candidates to favor other candidates (see vignette #2)[9][10][11]	**IW-interference:** Mass Persuasion of voters in an election; Influence the outcomes of elections in democratic political systems	Diminished confidence of populace in electoral processes, elected governments and representatives	Legal sanctions; Economic Sanctions; IW defense including sensitization and awareness of IW-interference campaign

[66] Chozick, A., & Perlroth, N. (2013, April 28). Twitter Speaks, Markets Listen and Fears Rise. The New York Times. Retrieved from https://www.nytimes.com/2013/04/29/business/media/social-medias-effects-on-markets-concern-regulators.html

[67] Koerner, B. (2016). Why ISIS Is Winning the Social Media War. Wired. Retrieved from https://www.wired.com/2016/03/isis-winning-social-media-war-heres-beat/

Actor	Lever	1st Order Effect	2nd Order Effect	Response (examples)
State-Sponsored Actor: United Kingdom, the 77th Brigade (maintains a small presence on Facebook and Twitter under its own name)	**Level 3: Manipulating Information Interpretations** Government-sponsored accounts, websites and applications designed to spread political propaganda[68]	**IW-influence:** Organized social media campaigns to manipulate public opinion over social media	Diminished confidence of populace in electoral processes, elected governments and representatives	Legal sanctions; Economic Sanctions; IW defense including sensitization and awareness of IW-interference campaign
Non-State (Organization) Actor: widely believed to **be** New World Hackers	**Level 4: Weaponizing Information Systems** Multiple DDoS attacks targeting systems operated by Domain Name System (DNS) provider Dyn**Error! Bookmark not defined.**	**IW-hacking:** Thousands of websites unavailable including DNS servers of Dyn	Service disruption; Loss of business activity	IW Offense including hack back
State-Sponsored Actor: Russian-affiliated APT[69]	**Level 4: Weaponizing Information Systems** A full spectrum of CNO tools[70] used including spear phishing, theft of credentials, VPN hacking, RAT implantation, and use of Black Energy[71] – a Trojan used to conduct DDoS attacks, espionage and information destruction attacks	**IW-hacking:** 6,500 attacks on the media, finance, transportation, military, politics, and energy sectors of Ukraine in a period of two months in 2016	Loss of economic competitiveness in the long run; Impact on society due to incessant degradation of essential services	Public attribution, Private attribution, IW Offense including hack back
State-Supported Actor: Stuxnet; Flame; Duqu; Mirai	Weaponizing Information Systems Sophisticated malware targeting classified information, intellectual property, research and defense organizations; Malware designed to disrupt, degrade, or destroy information systems, networks or industrial control systems.	**IW-hacking:** Surveillance; Theft of classified information or intellectual property; Loss of data; Malfunctioning of industrial control systems	Loss of business activity; Loss of economic competitiveness; Loss of industrial functions in strategic installations or enterprises.	Public attribution, Private attribution, IW Offense including hack back

Table 1: The ALERT: Actor, Lever, Effect, Response Taxonomy

A Theoretical Framework for Weaponizing Information Systems for Political Disruption

Drawing on the four categories of Actors, Levers, Effects, and Response, we propose a theoretical framework to explain the weaponization of IS for political disruption. The framework is constructed in four quadrants with each of the quadrants representing a key construct. The top two quadrants representing Actors and the Levers they select while the bottom two quadrants represent the Effects and the Responses.

To construct the framework we assert that over time as actors gain maturity and experience using levers to disrupt political systems, so too does the public sector gain experience in response thus building their response capacity. This dynamic relationship increasingly pushes the actor to come up with more innovative,

[68] Bradshaw, S. and Howard, P., 2017. Troops, trolls and troublemakers: A global inventory of organized social media manipulation. Retrieved from http://comprop.oii.ox.ac.uk/wp-content/uploads/sites/89/2017/07/Troops-Trolls-and-Troublemakers.pdf
[69] Greenberg, A. (2017, June 20). How an Entire Nation Became Russia's Test Lab for Cyberwar. Wired. Retrieved from https://www.wired.com/story/russian-hackers-attack-ukraine/
[70] Analysis of the cyber attack on the Ukrainian power grid. (2016). Electricity Information Sharing and Analysis Center (E-ISAC).Retrieved from https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf
[71] BlackEnergy APT Attacks in Ukraine. (n.d). Kaspersky Lab. Retrieved from https://www.kaspersky.com.au/resource-center/threats/blackenergy

agile and sophisticated methods to weaponize IS. Mature and experienced actors may employ levers drawn from a combination of levels to take best advantage of opportunities to create disruption in political systems towards achieving their desired objectives through first and second order effects. Hence the target/defender has to act accordingly and come up with a highly sophisticated, innovative and agile response in return.

An interesting paradoxical phenomenon emerges between actors and defenders where the responses of defenders in fact create new opportunities for actors to weaponize information systems. As Deibert and Rohozinski (2008) point out, mitigating security risks *through* cyberspace defenders do not always go hand in hand with mitigating security risks *to* cyberspace. For example, in order to protect political systems from disruption through the weaponisation of information systems, defenders may respond by introducing policies and engaging in IW-offensive activities that render information systems less secure and more vulnerable to weaponization. An example of this phenomenon is the rise of private firms working for nation-states conducting surveillance and IW-hacking (e.g. Dark Matter, NSO, Black Cube) and social media manipulation (e.g. Psy-Group) on their behalf[72]. These firms create and exploit vulnerabilities in information systems to achieve their objectives (e.g. installing malware, compromising IoT devices such as baby monitors for the purpose of espionage). Another example is the previously mentioned use of EternalBlue, a weapon created by the NSA that has been used by digital extortionists to paralyze the computers networks of the city of Baltimore. This paradoxical phenomenon is a promising area of future research.

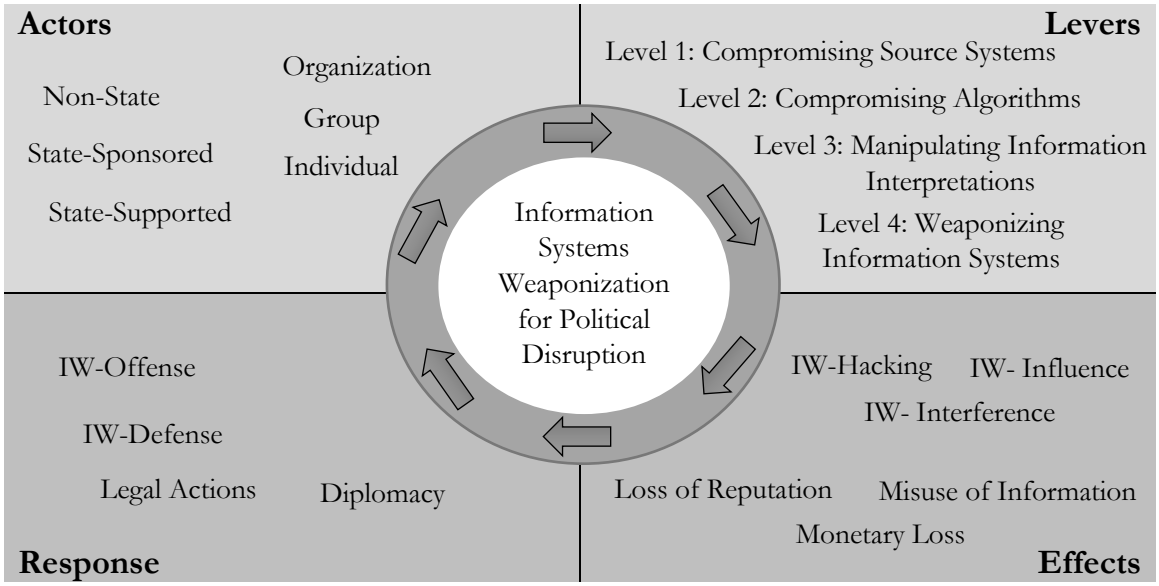

Figure 4: A Theoretical Framework for Weaponizing Information Systems for Political Disruption

There is considerable potential for further work into studying the relationship between Levers and Effects. In this paper we posited that particular Levers create particular Effects. However, significant further work is required to explain the causal mechanisms in the context of a complex and evolving multi-dimensional environment that lead to successful 1st order and 2nd order effects. In particular, (1) what these causal mechanisms are, (2) how and why they are successfully able to create particular effects, and (3) and what key

[72] Mazetti, M., Goldman, A., Bergman, R. & Perlroth, N. (2019, March 21). A New Age of Warfare: How Internet Mercenaries Do Battle for Authoritarian Governments. Retrieved from https://www.nytimes.com/2019/03/21/us/politics/government-hackers-nso-darkmatter.html?module=inline

factors (e.g. technological, political, social) in the environment enable the Actor to operationalize their strategic plans.

A key avenue for future research is the use of game theory to study the strategic interactions between actors and defenders given both parties are rational, seek to gain a strategic advantage over the opposing party, act deliberately and according to how they perceive the opposing party will react, and are subject to a strategic environment where there is considerable uncertainty and opportunities to learn (Sandler, 2003). Research using game theory must holistically contend with the full range of levers, effects and outcomes and how these will impact the way in which a network of nation-states will engage actors. Unlike in the past where the identity of actors and their strategies was largely known, today actors are emergent and their networks are complex and evolving (e.g. collaborations between Russia and Syria), and their attacks are multifaceted.

Discussion

In this paper, we have described the wide assortment of ways in which information systems can be employed to disrupt political processes and public institutions, which are the foundations of our modern societies and economies. We have put forth a working model of a taxonomy that links actors, lever, effects, and response strategies. We believe the taxonomy can help policymakers and practitioners appreciate the breadth of information systems-enabled disruption and the myriad combinations one must deal with when contending with heterogenous actors, levers, and effects put together. Furthermore, the taxonomy can be used to analyze previous incidents to determine successful matches between threats (Actors seeking to create political disruption), instruments (Lever or weaponized information systems), Effects (the outcome of the incident) and Responses. These matches can be used as a basis for a risk response strategy (what previous responses worked, which ones didn't work). The taxonomy also assists in distinguishing between the types of operations in a political disruption campaign: IW-influence, IW-interference and IW-attack, and how actors can begin with one operation and evolve or mature into a second such operation. For example, consider the two operations in 2016 profiled in the first vignette of the paper where the first focused on using social media to disseminate political messaging (IW-influence) and the second focused on hacking the systems belonging to the Democratic National Convention and stealing sensitive information for release to the public. Identifying the actors behind CNOs, their motivations, *modus operandi*, extent of information and monetary losses thereof etc. are all very difficult to ascertain at the first place. Sustained low-intensity influence operations in cyberspace, through media, news channels, social media, video sharing platforms etc., may remain well under the radar for a long time. Over and above, the second order effects become increasingly difficult to identify amidst a plethora of actors and leverages they could employ, but remains critical from the decision-making point of view. The network of information systems is complex and the interdependencies of various functions are difficult to assess. It is practically infeasible to anticipate the effects of IW attacks. The proposed taxonomy could also be helpful in containing the spread and reach of effects, or in a way, stop the effects from escalating.

A key reason for the weaponization of information systems by Actors is the poor level of CND among public and private organizations. This observation has lead to some argument in the literature suggesting that the private sector in particular has not invested sufficiently to protect its infrastructure from being weaponized and that governments should take a more active role in regulating the security of IT platforms (Etzioni, 2013). The government line has long been that corporations are rational actors that can be expected to take the necessary actions to secure their own interests (e.g. competitive advantage in the form of trade secrets, sensitive information and availability of IT service infrastructure). However, there are rational reasons why this has not been the case as Etizioni (2013) points out. For example, the consequences of significant data breaches are long-term whereas the focus of CEOs tends to be short-term. Also, most senior managers come from older generations and are not able to mitigate technology risk like they do business risk. Further,

weaponization of information systems is a 'negative externality' akin to environmental pollution – a category of risk that senior managers consider to be shared with others.

The world is coming to grips with the murder of Jamal Khashoggi, a prominent journalist and a citizen of Saudi Arabia, who was a vocal critic of the Crown Prince Mohammed bin Salman. The Saudi government used Twitter trolls to routinely harass critics of the government, including Mr. Khashoggi. The troll-farm based in Riyadh not only harasses critics and aims to silence dissident opinion, but also uses the features of Twitter to sensor conversations (e.g. by marking them as sensitive which flags them for Twitter. As reported, "They then turn to their well-organized army of 'social media specialists' via group chats in apps like WhatsApp and Telegram, sending them lists of people to threaten, insult and intimidate; daily tweet quotas to fill; and pro-government messages to augment."[73] The Saudi government also was successful in placing a mole within Twitter that gave them insider access to sensitive user data, including phone numbers and IP addresses. This case points to what we would expect to see as routine going forward. Not only will information systems be used by outsiders to meddle with a nation's democratic processes, but there will be cases where a nation's own leaders use information systems to censor dissident opinion. Social media platforms, due to their inherent characteristic of participatory communication, can reveal a lot personal information, particularly related to political and religious preferences. State control on these platforms could also meet a multitude of purposes; such as to censor politically sensitive information, garner support through opinion formulation in the favor of an authoritarian regime or leadership, or to quell dissent or intimidate political and ideological opposition. Eventually, the proliferation of online media and social media platforms has opened a whole new domain for states to interfere in the internal affairs of other countries – of course with a high degree of plausible deniability.

Meddling in a foreign nation's affairs, including elections and influencing the choice of political leaders is not a new issue. For decades, the US, UK and other nations have conducted operations in this space,[74][75][76] through both covert and overt means, which include monetary support, training programs and public relations assistance. What has changed in recent years is the nature of these engagements on several fronts. First, rather than being covert, small-scale, and highly human-driven operations, we now have moved to overt, large-scale, and information systems-driven operations. Personalized data is readily available and there is no dearth of sophisticated analysis tools to extract information, which could further be used to devise precise and targeted political campaigns. Second, in the past most of the citizenry of the nation were not directly involved in the manipulation efforts earlier. Today, due to the nature of our online platforms, citizens are co-creating the interference, knowingly or unknowingly. Also, a significant proportion of the population has access to the Internet and social media platforms, which increases the spread and speed simultaneously. Fake news, false information and hate messages travel quickly over social media and personal messaging platforms. The citizens not just consume this information, but they extend it further to their respective networks. Citizens become both the targets and the carriers. In particular with social media platforms citizens have active participation in political discourse, and the content on these platforms could shape their decisions and political preferences to a great extent.

---

[73] Benner, K., Mazzetti, B., & Isaac, M. (2018, October 20). Saudis' Image Makers: A Troll Army and a Twitter Insider. The New York Times. Retrieved from https://www.nytimes.com/2018/10/20/us/politics/saudi-image-campaign-twitter.html

[74] Carothers, T. (2018, March 12). Is the U.S. Hypocritical to Criticize Russian Election Meddling? Carnegie Endowment for International Peace. Retrieved from https://carnegieendowment.org/2018/03/12/is-u.s.-hypocritical-to-criticize-russian-election-meddling-pub-75780

[75] Binary, P. (2018, July 22). The U.S. Needs to Face Up to Its Long History of Election Meddling. The Atlantic. Retrieved from https://www.theatlantic.com/ideas/archive/2018/07/the-us-has-a-long-history-of-election-meddling/565538/

[76] Shane, S. (2018, February 17). Russia Isn't the Only One Meddling in Elections. We Do It, Too. The New York Times. Retrieved from https://www.nytimes.com/2018/02/17/sunday-review/russia-isnt-the-only-one-meddling-in-elections-we-do-it-too.html

Third, in the past, the number of media platforms were limited (e.g. TV, radio or print) and the approaches on how to engage in disinformation campaigns were clearly known. Today, not only have the number and sophistication of media platforms evolved, but also the dominant ones are not controlled by state-actors and are not confined to operations within a nation. In the aftermath of intervention in the US and French Presidential elections, various media reports and intelligence assessments accused Russia of influencing public opinion through its media arms, Russia Today and Sputnik. The state has no or limited control on web content *per se*, and it could be easily manipulated or manufactured to influence public opinion on key political decisions, at the behest of foreign actors. Finally, the actors that are conducting these operations are not directly employed by, or contracted by, sanctioned public agencies (e.g. intelligence agencies) exclusively. The actors need not have access to sophisticated assets or even training to conduct current election and political meddling campaigns. These are also available as paid services, such as trolls or bots for fake followers, message amplification or spewing fake news of disinformation. IW means have, in essence, opened a virtual Pandora's Box before decision makers, and it needs a systematic approach to mitigate the arising risks to our social and political security. The consequences are severe, especially for countries with democratic form of governance, which depends heavily on the ethos of consultation, public opinion, freedom of speech and expression, and transparent participative electoral process.

ALERT was developed on the basis of liberal democratic values as practiced in the West. An interesting avenue for future research would be to develop an ALERT for parties that don't share the same values. A comparison could be the basis of an interesting study into the multiple perspectives on IW conflict towards a common and unified understanding that could inform standards enshrined in international law.

Conclusion

Actors, state-supported and state-sponsored, across a range of nations engage in information systems-enabled disruption of political systems and processes. In addition, these actors may seek to undermine trust in government and cause political instability through compromising public information system infrastructures. Understanding the threat landscape holistically is the first step towards being able to prepare for these attacks. The defense strategies that a nation might employ are diverse. Our analysis points to the fact that adequate response strategy arises from a nuanced understanding of the actor, the levers used to facilitate disruption, and their effects.

The ALERT is an important contribution given the trend towards weaponizing information systems is likely to continue as public institutions become more dependent on increasingly sophisticated information systems to conduct elections and deliver public services. In particular, our conceptualization of the phenomena of weaponization of information systems and the possible levers and corresponding effects provide a useful means of analyzing, categorizing and describing information systems-enabled political disruption for practitioners and policymakers.

References

Abbasi, A., & Chen, H. (2007, May). Affect intensity analysis of dark web forums. In *2007 IEEE Intelligence and Security Informatics* (pp. 282-288). IEEE.

Ablon, L., Libicki, M.C., Golay, A.A., 2014. *Markets for cybercrime tools and stolen data: Hackers' bazaar*. Rand Corporation.

Ahmad, A., Webb, J., Desouza, K.C., and Boorman, J. (2019). "Strategically-Motivated Advanced Persistent Threat: Definition, Process, Tactics and a Disinformation Model of Counterattack," *Computers & Security*. Vol 86, pp. 402-418.

Alashri, S., Srivatsav Kandala, S., Bajaj, V., Parriott, E., Awazu, Y., & C Desouza, K. (2018, January). The 2016 US Presidential Election on Facebook: an exploratory analysis of sentiments. In *Proceedings of the 51st Hawaii International Conference on System Sciences*.

Armin, J., Foti, P., & Cremonini, M. (2015, August). 0-day vulnerabilities and cybercrime. In *2015 10th International Conference on Availability, Reliability and Security* (pp. 711-718). IEEE.

Awan, I. (2017). Cyber-extremism: Isis and the power of social media. *Society*, *54*(2), 138-149.

Broadhurst, R. (2017). Cybercrime: thieves, swindlers, bandits and privateers in cyberspace. *Swindlers, Bandits and Privateers in Cyberspace (July 27, 2017)*.

Broadhurst, R., Woodford-Smith, H., Maxim, D., Sabol, B., Orlando, S., Chapman-Schmidt, B., & Alazab, M. (2017). Cyber Terrorism: Research Review: Research Report of the Australian National University Cybercrime Observatory for the Korean Institute of Criminology. *Available at SSRN 2984101*.

Chen, H., Chung, W., Qin, J., Reid, E., Sageman, M., & Weimann, G. (2008). Uncovering the dark Web: A case study of Jihad on the Web. *Journal of the American society for information science and technology*, *59*(8), 1347-1359.

Dalins, J., Wilson, C., & Carman, M. (2018). Criminal motivation on the dark web: A categorisation model for law enforcement. *Digital Investigation*, *24*, 62-71.

Deibert, R. J., & Rohozinski, R. (2010). Risking security: Policies and paradoxes of cyberspace security. *International Political Sociology*, *4*(1), 15-32.

Denic, N. V. (2017). *Government Activities to Detect, Deter and Disrupt Threats Enumerating from the Dark Web*. US Army Command and General Staff College Fort Leavenworth United States.

Desouza, K. C., & Bhagwatwar, A. (2012). Leveraging technologies in public agencies: The case of the US Census Bureau and the 2010 Census. *Public Administration Review*, *72*(4), 605-614.

Desouza, K. C., & Bhagwatwar, A. (2012). Citizen apps to solve complex urban problems. *Journal of Urban Technology*, *19*(3), 107-136.

Echeverria, J., & Zhou, S. (2017, July). Discovery, Retrieval, and Analysis of the'Star Wars' Botnet in Twitter. In *Proceedings of the 2017 IEEE/ACM international conference on advances in social networks analysis and mining 2017* (pp. 1-8). ACM.

Etzioni, A. (2014). The private sector: A reluctant partner in cybersecurity. *Geo. J. Int'l Aff.*, *15*, 69.

Futter, A. (2018). 'Cyber'semantics: why we should retire the latest buzzword in security studies. *Journal of Cyber Policy*, *3*(2), 201-216.

Gupta, A. (2018). The dark web as a phenomenon: a review and research agenda (Masters minor thesis). University of Melbourne. School of Engineering. Parkville. Victoria, Australia.

Ho, T. N., & Ng, W. K. (2016, November). Application of stylometry to darkweb forum user identification. In *International Conference on Information and Communications Security* (pp. 173-183). Springer, Cham.

Killourhy, K. S., Maxion, R. A., & Tan, K. M. (2004, June). A defense-centric taxonomy based on attack manifestations. In *International Conference on Dependable Systems and Networks, 2004* (pp. 102-111). IEEE.

Kjaerland, M. (2006). A taxonomy and comparison of computer security incidents from the commercial and government sectors. *Computers & Security*, *25*(7), 522-538.

Lin, T. C. (2016). Financial Weapons of War. *Minnesota Law Review*. 100 (4): 1377–1440.

Mergel, I., & Desouza, K. C. (2013). Implementing open innovation in the public sector: The case of Challenge. gov. *Public administration review*, *73*(6), 882-890.

Mirkovic, J., & Reiher, P. (2004). A taxonomy of DDoS attack and DDoS defense mechanisms. *ACM SIGCOMM Computer Communication Review*, *34*(2), 39-53.

Nunes, E., Diab, A., Gunn, A., Marin, E., Mishra, V., Paliath, V., & Shakarian, P. (2016, September). Darknet and deepnet mining for proactive cybersecurity threat intelligence. In *2016 IEEE Conference on Intelligence and Security Informatics (ISI)* (pp. 7-12). IEEE.

Rowe, G., & Frewer, L. J. (2005). A typology of public engagement mechanisms. *Science, Technology, & Human Values*, *30*(2), 251-290.

Sabillon, R., Cano, J., Cavaller Reyes, V., & Serra Ruiz, J. (2016). Cybercrime and cybercriminals: a comprehensive study. *International Journal of Computer Networks and Communications Security, 2016, 4 (6)*.

Sandler, T. (2003). Terrorism & game theory. *Simulation & Gaming*, *34*(3), 319-337.

Scanlon, J. R., & Gerber, M. S. (2014). Automatic detection of cyber-recruitment by violent extremists. *Security Informatics*, *3*(1), 5.

Schmidt, R., Rattray, G. J., & Fogle, C. J. (2008). Methods and apparatus for developing cyber defense processes and a cadre of expertise. *U.S. Patent Application No. 11/947,655*.

Simmons, C., Ellis, C., Shiva, S., Dasgupta, D., & Wu, Q. (2014, June). AVOIDIT: A cyber-attack taxonomy. In *9th Annual Symposium on Information Assurance (ASIA'14)* (pp. 2-12).

Stewart, D. (2008). *Building enterprise taxonomies*. BookSurge Publishing.

Tsakalidis, G., & Vergidis, K. (2017). A systematic approach toward description and classification of cybercrime incidents. *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, *49*(4), 710-729.

Webb, J., Ahmad, A., Maynard, S.B., & Shanks, G. (2014). A Situation Awareness Model for Information Security Risk Management. *Computers & Security*. 44, (pp. 1-15).