|  |
| --- |
| Introduction to Information Warfare Assignment 2 |
| A Short Academic Paper |

Family Name: David Selvam

Given Name: Visahl Samson

Student Number: 10498743

Unit code and Title: CSI2104 Introduction to Information Warfare

Name of Lecturer: Kang Leng

Campus: PSB Academy, Singapore

Course: Bachelors of Science in Cyber Security (FT)

Due Date: 26th July 2019 (5 PM)

Contents

[Introduction 2](#_Toc14982444)

[Tactics 3](#_Toc14982445)

[Offensive 3](#_Toc14982446)

[Defensive 4](#_Toc14982447)

[Advantages 4](#_Toc14982448)

[Political consequences 4](#_Toc14982449)

[2016 USA Election 4](#_Toc14982450)

[Brexit 5](#_Toc14982451)

[Financial consequences 6](#_Toc14982452)

[Legal consequences 7](#_Toc14982453)

[Reputational consequences 7](#_Toc14982454)

[Ethics 8](#_Toc14982455)

[My assessment 8](#_Toc14982456)

[Conclusion 9](#_Toc14982457)

[References 9](#_Toc14982458)

# Introduction

Information warfare consists of static and tactical operations to gain advantage over information of the opponent. The ultimate goal of the information warfare is to gain information superiority which can provide national, social, economical and personal advantages. Currently, information warfare is conducted using advanced latest technologies. People have different views on information warfare. Some supports information warfare while others disagree with them. The primary purpose of this paper is to justify that all the measures in information warfare cannot be right and achieving information superiority do not compensate the political, legal, financial and reputational consequences. This paper starts with tactics used in information warfare which consists of types of operations used in information warfare then moves to benefits of information warfare then continues to consequences and ends with justified conclusion.

# Tactics

The 2 main tactics used in information warfare are offensive and defensive. As the word describes the offensive means the one who mounts the attack and the defensive is the one who protects the own data from the offensive one.

## Offensive

As mentioned earlier, the primary objective of the offensive information warfare is to attain information superiority. The main operations of offensive information to get the advantage are deny, exploit, corrupt, and destroy data (Chapple & Seidl, 2015) .

**Deny –** blocking enemies access to their own information.

**Exploit –** Make use of enemies information for own benefit.

**Corrupt –** Manipulating/altering the enemies information, so that it will lead to wrong decisions.

**Destroy –** Destroying the information may include physical destruction and software attack based destructions. It causes the enemy to surrender.

There are several ways that can be used to execute the offensive information warfare. They are Open Sources which targets privacy and piracy, Psychological Operations and Perception Management consists the actions that will cause psychological issues, Inside the Fence which includes corporate espionage, penetrating of the premises and insider attacks, Seizing the Signals covers packet/network/shoulder sniffing activities also covers wire taps, Computer Break-in and Hacking which consists of illegal access to the information, theft and tampering to get information, Masquerade includes forged documents and theft of identity to perform undercover operations. , Cyber attacks which generally consists of virus, malware attacks which will affect the systems (Denning, 2006).

## Defensive

The primary objective of defensive information warfare is to protect own information from the offensive operations of enemy. Defensive information warfare concerned with protective measure such as CIA of data, which is primarily focuses on data protection, recovery of information from offensive approaches, information verification to make sure offensive approach corrupt is not there. To implement these measures the defensive information warfare uses various security measures such as encryption, firewall, ACL, etc (William & Matthew, 2011)...

# Advantages

Usage of information warfare has its own merits and demerits. If we focus on its advantages, it enables us to get the critical information from our enemy easily, so that we can prepare ourselves either for offensive or defensive operations, where it useful for national security purposes. Then, it creates new job opportunities and leads to innovations of new security controls (Atgiller 2011). Apart from it information warfare eliminates all the form of physical warfare. Can be used to stop terrorists and threats to national security can be identified and stopped.

# Political consequences

As mentioned earlier, information warfare can be used by anyone who targets other. Since, the offensive warfare consists both legal and illegal actions there are several incidents in political sector that proves all the measures in information warfare is not acceptable. Some well-known incidents happened in political sector is provided below.

## 2016 USA Election

United States of America’s president election took place in November 2016 where the republican Donald Trump won against Democrat Hillary Clinton and became the 45th President of United States of America(David C., 2018) . This result surprised the entire world with a question of how it happened?. Because reports predicted (Long, 2016) that Hillary Clinton will win but what happened actually was totally opposite. According to reports (Graham-Harrison & Cadwalladr, 2018) a whistleblower revealed about Cambridge Analytica which had played vital role in Trump’s victory. So, when the investigations started and gone through everything the reports reveals that the company called Cambridge Analytica has involved in political scandal with the help of Facebook.

The report explains that Cambridge Analytica, a company which helps business people and politicians to change the behaviour of audience. So here in USA election, the company has collected Facebook data of 50 Million users. This data contains how they behave for different kind of Facebook posts. So, once they collected they analysed and provided ad based on that. At the end of the investigation Facebook has admitted that they have allowed Cambridge analytica to collect the information. The Cambridge analytica process reported (Agencies, 2018) to started in 2014 through an app which has only 270,000 Facebook users though this number is small the company collected the data of those 270,000 user’s Facebook friends resulted in collection of 50 Million users.

Once it collected, the company used technique psychographic microtargeting which identifies the voter based on their Facebook profile activities and started to feed customised advertisement according to their profile. Also it’s reported (Callum, 2017) that Russia tried to hack election systems of 21 states in United States of America during the election period in 2016.

## Brexit

Brexit stands for British Exit from European Union which was well-known topic in 2016 (Will, 2019). According to reports, a public voting method known as referendum took place on 23rd of June 2016. In this the leave from EU option had won with 58% (BBC, 2019). Many think that people have decided this but when researches have been conducted on results it revealed the background. Reports state that Russia has done infrastructure exploitation on United Kingdom by targeting their media, telecommunication and energy sector on the referendum day.

Also, it says, there are possibilities that the referendum website would have hacked and the results would have been modified (BBC, 2017). Also, according to reports UK accused Russia for using Facebook and Twitter bots/ fake accounts to spread fake news. It’s reported (David D, 2017) that 150,000 Twitter accounts posted several posts which supports UK to exit from European Union. So as a result United Kingdom has to exit from European Union.

While seeing these 2 we can come to know that both are kind of same. Because the strategies used by the offensive player here is same known as performing psychological operations. These psychological operations involve spreading false news/hate news which will affect the people from choosing their choice or compel to choose one particular choice.

This is one of the primary reason why I have selected all the ways in information warfare is not acceptable. Because these kind of actions directly affects innocent people. This is somehow similar with brainwashing. In this people are forced to choose one option even they don’t agree with that. As a consequence, in both the cases the outcome of election unacceptable by majority of people but they have no alternative other than accepting the results.

# Financial consequences

Reports about Brexit (Linda, 2018) clearly show how this incident affected UK’s financial action in multiple ways. It’s reported that the GDP has decreased 6.7%. Also, UK has to follow World Trade Organizations rules while trading with EU countries (Brian, Paul & Richard, 2019). These are just few primary issues caused. Also, in USA it’s reported (FEC, 2016) that president trump has spend 59 Million USD on Cambridge Analytica during the election period. These outcomes show that how the information warfare tactics used here are caused financial consequences that showed information warfare is expensive. Because spending 59 Million USD to perform Psychological operations is high. Also, in Brexit case it caused long term effects. If the amount of money involved in these 2 cases would have used for other defensive information warfare it would have been better. Apart from this it’s reported (Salvador, 2018) that after Cambridge analytic scandal the share prices came down nearly 40 percentages,

# Legal consequences

The legal consequences of information warfare cause both law related and financial related issues. Most of the information warfare action lawsuits end in huge penalties. For an example when we look at Cambridge analytica case (Sam, 2018) Facebook CEO Mark Zuckerberg was advised by Federal trade commission to testify regarding Cambridge Analytica before congress on 21st of March 2018. Now almost a year later the reports say (Wong, 2019) that Facebook is estimated to pay 5 Billion USD for privacy violations. UK also fined Facebook for 5, 00, 00 GBP (Waterson, 2018) for deteriorating to protect Facebook data of UK people. Also, both Facebook and Cambridge analytica are facing class action lawsuit (Bowcott & Hern, 2018).

Since, every country has their own Data Protection Policy the legal consequences of performing information warfare actions vary. Most of the times the legal consequence ends in financial fine.

# Reputational consequences

In information warfare reputational is one of the key factors to consider. Because if the offensive player get caught while performing information warfare activities it totally spoils their own name and reputation they had. In sometime the offensive operations are performed intend to spoil reputation of target. For example, when we consider Cambridge analytic incident the consequences caused potential damage to Facebook. According to survey conducted by fortune it surprise to know that Facebook is least trusted technology organization in terms of user data protection (Jonathan, 2018). So, this result clearly shows that how the information warfare causes reputational consequences to an organization. In business having good reputation is primary significant. Reputation can help business to grow so once it’s gone it’s very hard to earn it back. In Cambridge Analytica case Facebook has faced all those issue just because of one of its security policy and the company use that point to perform information warfare operation i.e. Psychology operations.

# Ethics

While information warfare has advantages it also causes concern between people about their data and privacy. Since, launching information war is very easy to do and little bit hard to detect it may cause frequent attacks. Also, it’s hard to trace back that who started the attack it’s because current digital era it’s very easy to add resources to network. Apart from it, there are possibilities that cyber attacks can be launched using common people without them knowing that hacker/intruder using their resources to attack. During this type of scenarios it’s hard to take any actions.

# My assessment

My assessment on information warfare measures is all the measures cannot be justified and achieving information superiority does not compensate the political, legal, financial and reputational consequences. Especially, Psychological operations performed on people to manipulate their mind to choose something they don’t want to choose. In this measure freedom of individual is getting denied. Since, every individual has their own freedom to express their own thoughts and freedom to support their desired leaders or politicians it’s wrong to force them to choose one specific choice. So, the question raise here is what the purpose of information superiority is when people are going to get programmed to get desired outcome of the one who program. One more reason why I choose this option is attacks on critical infrastructure. Critical infrastructure is assets that are important for a country to function the society and economy. Typical critical infrastructure assets include medical, communication, defence, emergency services, etc... Each country has its own critical infrastructure classifications (CPNI, n.d.). So, information warfare attacks on critical infrastructures causes potential losses to a nation. A best example is Ukrainian power outages caused in 2015. It’s reported that (BBC, 2017) Ukraine has been affected by cyber attacks on its critical infrastructure which caused power cut that affected almost 225,000 people. So, these kind of attacks that are causing issues to ordinary people are supposed to be stop and cannot be justified. Apart from these measure in information warfare there are other measures that are used to protect the country and nations that include threat intelligence which helps to prevent countries/organizations from cyber attacks. Usage of threat intelligence measures can be accepted since the nations can use them to protect themselves from terrorists.

# Conclusion

As a conclusion, it’s recommended to understand that information warfare has its own advantages and disadvantages. These advantages and disadvantages applies even to the each measures used in information warfare operations. It is one’s own right to either support and unsupported to all the measures in information warfare. According to myself there are some measures in information warfare that I don’t support and cannot be justified that’s the reason I have given few examples in this short academic paper. At the same time I want to make sure that information warfare is required in current era. Because it help us to protect ourselves. Avoiding some kind of information warfare activities as I mentioned in this short academic paper would be my recommendation.

# References

Chapple, M., & Seidl, D. (2015). Cyberwarfare. Burlington, MA: Jones & Bartlett Learning

Denning, D. (2006). Information warfare and security (1st ed.). Boston [etc.]: Addison-Wesley.

William, H., & Matthew, W. (2011). Information Warfare: Corporate Attack and Defence in a Digital World (1st ed.). Butterworth-Heinemann.

Cyber Warfare Advantages Disadvantages - atgiller. (2011). Retrieved from <https://sites.google.com/site/atgiller/cyber-warfare-advantages-disadvantages>

David C., B. (2018). United States Presidential Election of 2016. Encyclopædia Britannica. Retrieved from <https://www.britannica.com/topic/United-States-presidential-election-of-2016>

Long, H. (2016). Key model predicts big election win for Clinton. Retrieved from <https://money.cnn.com/2016/11/01/news/economy/hillary-clinton-win-forecast-moodys-analytics/index.html>

Graham-Harrison, E., & Cadwalladr, C. (2018). Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach. Retrieved from <https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election>

Agencies. (2018). Retrieved from <https://www.scmp.com/news/world/united-states-canada/article/2139327/explainer-how-cambridge-analytica-exploited-facebook>

Callum, B. (2017). Retrieved from <https://www.washingtonpost.com/news/the-fix/wp/2017/09/23/what-we-know-about-the-21-states-targeted-by-russian-hackers/?utm_&utm_term=.0d609f2d5676>

WILL, K. (2019). Brexit Definition. Retrieved from <https://www.investopedia.com/terms/b/brexit.asp>

BBC, N. (2019). Brexit: A really simple guide. Retrieved from <https://www.bbc.com/news/uk-46318565>

BBC, N. (2017). UK security chief blames Russia for hacks. Retrieved from <https://www.bbc.com/news/technology-41997262>

David D, K. (2017). Signs of Russian Meddling in Brexit Referendum. Retrieved from <https://www.nytimes.com/2017/11/15/world/europe/russia-brexit-twitter-facebook.html>

Linda, Y. (2018). The Economic Impact Of Brexit And What It Means For Financial Stability. Retrieved from <https://www.forbes.com/sites/lbsbusinessstrategyreview/2018/11/28/the-economic-impact-of-brexit-and-what-it-means-for-financial-stability/#3a872b20383e>

Brian, W., Paul, S., & Richard, M. (2019). Brexit: All you need to know. Retrieved from <https://www.bbc.com/news/uk-politics-32810887>

FEC. (2016). Browse Disbursements - FEC.gov. Retrieved from <https://www.fec.gov/data/disbursements/?data_type=processed&committee_id=C00580100&recipient_name=cambridge+analytica&two_year_transaction_period=2016&min_date=01%2F01%2F2015&max_date=12%2F31%2F2016>

Salvador, R. (2018). Here are the scandals and other incidents that have sent Facebook's share price tanking in 2018. Retrieved from <https://www.cnbc.com/2018/11/20/facebooks-scandals-in-2018-effect-on-stock.html>

Sam, M. (2018). Facebook-Cambridge Analytica: A timeline of the data hijacking scandal. Retrieved from <https://www.cnbc.com/2018/04/10/facebook-cambridge-analytica-a-timeline-of-the-data-hijacking-scandal.html>

Wong, J. (2019). Facebook to be fined $5bn for Cambridge Analytica privacy violations – reports. Retrieved from <https://www.theguardian.com/technology/2019/jul/12/facebook-fine-ftc-privacy-violations>

Waterson, J. (2018). UK fines Facebook £500,000 for failing to protect user data. Retrieved from <https://www.theguardian.com/technology/2018/oct/25/facebook-fined-uk-privacy-access-user-data-cambridge-analytica>

Bowcott, O., & Hern, A. (2018). Facebook and Cambridge Analytica face class action lawsuit. Retrieved from <https://www.theguardian.com/news/2018/apr/10/cambridge-analytica-and-facebook-face-class-action-lawsuit>

Jonathan, V. (2018). Facebook Is the Least Trusted Major Tech Company When it Comes to Safeguarding Personal Data, Poll Finds. Retrieved from <https://fortune.com/2018/11/08/mark-zuckerberg-facebook-reputation/>

CPNI. Critical National Infrastructure | CPNI | Public Website. Retrieved from <https://www.cpni.gov.uk/critical-national-infrastructure-0>

BBC, N. (2017). Ukraine power cut 'was cyber-attack'. Retrieved from <https://www.bbc.com/news/technology-38573074>