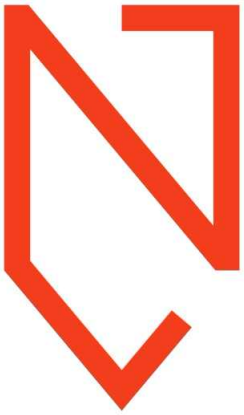

Noroff University College

DOES THE ADOPTION OF TECHNOLOGY MAKE A SOCIETY MORE SUSCEPTIBLE TO INFORMATION WARFARE?

Submitted in partial fulfilment
of the requirements of the degree of

BACHELOR IN CYBER SECURITY

of Noroff University College

Travis Clark

Kristiansand, Norway
June 2022

Declaration

I declare that the work presented for assessment in this submission is my own, that it has not previously been presented for another assessment, and that work completed by others has been appropriately acknowledged.

Name: Travis Clark **Date**: June 8, 2022

Abstract

As newer technologies fight to better connect the citizens of the world, the rapid adoption creates mountains of information about each user. Modern militaries, nation-state actors, and criminal groups are using the same off-the-shelf technologies to incorporate information warfare into hybrid warfare. Previously information was a weapon, however with the spread of technology information has also become a target. Military strategies have changed to include technology into their strategy and battle plans. In addition nation state actors and criminal groups are targeting the information itself. Information has become a global commodity and as societies around the world adopt technologies, they produce a myriad of data that can be turned into information, which in the end can be used against them. The internet provides freedom to the people looking to communicate and an opportunity for nation-states and criminal groups to monitor and control that communication. This paper explores the methods, and the factors that cause a nation to become susceptible to information warfare as technology is adopted by its citizens. The increasing complexity of the technology used to defend systems means it is often easiest to attack the users and not the system itself. The development of audio and video technologies facilitate the creation of false narratives or obfuscating the truth. As more people become IT literate and increase their use of the internet they also increase the level of risk of being a victim of information warfare.

Keywords: *Information Warfare, vulnerability, technology, misinformation, susceptibility*

Acknowledgements

I would like to acknowledge my supervisor Iain Sutherland for his help and guidance during the process of research and writing. I especially appreciate his willingness to check over my drafts and give honest actionable feedback. I would also like to thank Noroff University College for the opportunity and support. It was a journey getting to the end and I learned a great deal along the way. Lastly I would like to thank Leo, our puppy for timing his naps so I could do my research and finish my writing between walks.

Contents

List of Figures

1

Introduction

Information warfare can be divided into two categories. The first category is protecting one's own battlefield information and the attack or acquisition of the opponents battlefield information. The second category, which will be the focus of this paper, is how technology allows for the: "manipulation of information trusted by targets without their awareness, so that the targets will make decisions against their interest but in the interest of the one conducting information warfare."(Wikipedia 2021) Technology has democratized the internet allowing everyone with a device access to what was once only available to military, government, and universities. Technology has transferred that access from the desktop to the laptop to the smartphone. Most importantly the adoption of the smartphone, free or low cost internet access, and social media apps have all added up to greater communication and an increased interaction both locally and globally. Smartphones are used for news, shopping and communication. Daily communication across long distances has gone from being cost prohibitive a few decades ago to almost zero upfront cost to the consumer. The concept of upfront cost is important when looking at the democratization of the internet and the technologies that give us access to it. Many of the apps being used by consumers are free to download and free to use. Yet the companies producing and maintaining them are worth billions of dollars. The "value" of the app is the data it collects about its users. Some companies are using the data straight away to produce advertising revenue, while others sell the data to large brokers. The data is compiled into information about us. Who is using this information? Can political opinions be swayed by campaigns targeting based on this information? Can oppositions generate momentum? Can buying habits be influenced? Can networks and companies be compromised? The initial answer to all of these questions would be yes, but to what degree? Advertisers and marketers have been trying to manipulate buying habits for over 100 years through advertising. But what if those advertisements or campaigns can be so targeted, so specific, that the effect is dramatically increased and predictable, and better yet the targeted person or group doesn't even notice?

Are people unwillingly setting themselves up for information warfare campaigns by engaging more with their smartphones and social media? The companies creating the apps need engagement. Engagement equals information, which they can use for manipulation or sell. But what about the information we are willingly sharing with the world? Our likes, dislikes, opinions, and habits. The fast pace of technology and growing global inter-connectivity has made information itself one of the most valuable global commodities. Competition for such a valuable commodity means information warfare tactics are no longer reserved for nation-states and military forces of the world. There is an emerging civilian side to information warfare, not only on the victim's side but also on the attacker's side. Personal information that is willingly shared gives attackers knowledge about how and who to target. There are two battles that users are in-between. The battle by governments for who controls what is perceived as the truth? And the battle by companies and individuals who want to influence our everyday habits. To accomplish this tactics like censorship, disinformation, and misinformation are used. Some attack the integrity of information. These kind of attacks are growing as technology makes it easier to create fake versions of voice and video or change the data at its source. Attacking the integrity of information makes it harder to know what is real and who would have changed the data. Lack of attribution and a collective disagreement about the proper response for information warfare or cyber-attacks means most governments and criminal groups go unpunished. Without attribution and without prosecution there is little disincentive to engage in information warfare. How do these factors affect ones vulnerability and susceptibility? Technologies like the smartphone and mobile internet give us constant connection. This in turn generates a lot of data and, in turn, information. The role of this information has taken center stage with many state actors for new avenues to pursue Information Warfare campaigns.

1.1 Problem Statement

With the rapid adoption of technologies and greater percentages of our lives are spent online, does this make us more vulnerable? More specifically does the adoption and use of technology that is meant to connect us actually make us more vulnerable to attacks like information warfare campaigns?

1.2 Research Objectives

Looking at all of the research included in the Literature Review there are many attempts and ideas around how to defend against information warfare, or filter it out, and educate the public about it. There is a great deal of research indicating the looming dangers of information warfare in its most prolific forms of fake news and disinformation campaigns. Collectively the agreement in the research is that social media in particular makes the dissemination of both fake news and disinformation exponentially easier. How much danger are we really facing? The objective of this paper is to try and best answer the problem statement using existing research on information warfare. Instead of creating another framework or digital niche solution, instead look at a simple way to gauge a societies potential susceptibility to IW. The accomplish this objective a final output was to create a metric for comparison of nations and a system of weighting characteristics that would result in a score of a nations susceptibility. This score allows for comparison between two nations or a group of several nations.

1.3 Scope and Limits

The project had a limited time frame and therefore needed to be limited to existing research and a simple metric. The metric was created to be expandable for future work in the event that the study would have more time and resources.

1.4 Document Structure

- Abstract
- Introduction
- Literature Review
- Data Collection /Analysis
- Results
- Conclusion

2

Literature Review

2.1 Methodologies

Technologies have bridged the gaps between the academic, military, and private sectors. All three groups are reliant on similar or the same technologies: mobile phones, 4G access, fiber networks, ISPs, and search engines. Since the services and service providers are overlapping, the interaction between the different sectors overlaps and is described in Volume 3 of Technology for the U.S. Navy and Marine Corps. “Information and information infrastructure likely will not be wholly owned, operated, maintained, or protected by the adversary in any great part—just as the U.S. Department of the Navy will be using commercially provided data over commercially provided and maintained infrastructure elements, so also will the adversary. Those portions of the infrastructure may be off limits to attack due to some combination of commercial, international, or social concerns”.(Studies, Council, et al. 1997). Most of the technology the military will be using in the future will be coming from and developed by the private sector.

2.1.1 Convergence of Information Warfare

Nation-states waging a more hybrid type of warfare is only natural, according to Dr. Martin Libicki. Dr. Libicki has held many institutional positions within American academia and defense. In his 2017 article entitled “The Convergence of Information Warfare,” Dr. Libicki explains that as technology trends rise and other countries begin to exploit those trends, then it is “far less plausible to imagine a cyber attack campaign unaccompanied by other elements of information warfare—in large part because almost all situations where cyber-attacks are useful are those which offer no good reason not to use other elements of information warfare.” (Libicki 2020). The ethics and nonlethal nature of

Information Warfare make it an attractive addition to a military's cyber arsenal. The ethical boundaries and the undefined level of an appropriate response will make it essential to track the developments as more and more governments add the cyber dimension to their military. Will a physical response ever be relevant to an Information War campaign? More research and more international guidelines will be needed in the future.

2.1.2 Hybrid Approach

Many different militaries worldwide have begun to adopt a hybrid approach to warfare which includes, to varying degrees, Offensive cyber-operations. More specifically, concerning Information Warfare. Dmitry Adamsky produced a report detailing Russian nuclear policy and how it applies to geopolitics and the new generation of war. Adamsky feels that the Russian use of western termed "hybrid" war has always been a part of Russian military engagement and not a new addition to its military policy. Technology is just another avenue for strategy. "By employing asymmetrical means, the "weak player" can inflict serious damage to the "stronger" one, even impose its political will, without traditional decisive battlefield victory. Success in such a campaign is not a function of the correlation of forces but of a skillful orchestration of military and non-military (political, psychological, ideological, informational) means. Today, the ability to master an "indirect approach" manifests operational art excellence, and its culmination is to employ a variety of means, primarily informational dominance, to neutralize the enemy without the use of force." (Adamsky 2015). This hybrid approach again emphasizes the belief that Information Warfare is a less lethal companion to kinetic warfare.

2.1.3 3 layers IW research

Three US researchers looked at applying a strategic model originally put forth by two of the researchers. Ma&Krings created a three layer survivability structure in 2008. This structure was then later applied to strategic information warfare analysis. The three layers are Strategic, Tactical, and Operational. Like the previous study it is an advanced gamification study. Where it differs and can allow for conclusive research is in how it deals with three of the major difficulties with researching IW "the core of the three-layer survivability analysis possesses unique and powerful functionalities in dealing with three fundamental difficulties in studying IW, i.e., rationality (an assumption of tradition game theory), uncertainty (vulnerability), and deception."(Ma, Krings, and Sheldon 2009)

2.1.4 Offensive Cyber Capabilities

A recent paper published in the European Journal of International Security explores state violence as less evil and less violent than traditional state violence. Egloff and Shires, the authors of the article, do not necessarily agree. They contend that more research into the topic is needed. Technology may open doors for states to use Offensive Cyber Capabilities domestically and abroad in ways that traditional state violence would never be considered. If the acts are less violent but used more often and on people than traditionally would be out of scope for such measures, does that make them evil?(Egloff and Shires 2021). Regardless of the tactics' perception or ethics, it is clear that nation-states have allowed technology to change its perception of what is in and what is out of scope. Campaigns that would have been "off the table" because of the kinetic use of force or potential domestic or international ramifications could now be possibilities. Military strategies have evolved to include cyber,

especially when it comes to Information Warfare. Attribution of these acts is still very difficult, so there is greater incentive to use them since potential international repercussions are almost none.

2.1.5 Global Disinformation Order

Monitoring of the changing landscape of social media manipulation has been conducted by University of Oxford's Oxford Internet Institute. Organized social media campaigns intended to manipulate have been conducted in over 70 countries in 2019 which is almost double of the amount that was seen in 2018. The study showed that many countries are actively engaging in international social media manipulation campaigns. Some countries were also engaging in domestic campaigns, however they were out of the scope of the report. The report demonstrates through various graphics the different techniques, budgets, and capabilities of the threat actors. There is no data to demonstrate the effectiveness of the campaigns. However, the paper concludes with this point "A strong democracy requires access to high-quality information and an ability for citizens to come together to debate, discuss, deliberate,empathize, and make concessions. Are social media platforms really creating a space for public deliberation and democracy? Or are they amplifying content that keeps citizens addicted, dis-informed, and angry?"(Bradshaw and Howard 2019). Ultimately this constant disruption of high-quality information could over time cause the campaigns to be indirectly successful.

2.1.6 Effectiveness of Influence Activities in IW

The Australian Military conducted a study of the effectiveness of influence activities in information warfare. The Presidency campaign of Donald Trump and Russian influence on the 2016 election. The paper asserts that Western democracies are already at war in the information domain and are out-communicated by their enemies. The study fuses three research disciplines: systems thinking, influence, and behavioural science to better understand mental models and enable a deeper understanding of influencing tactics. This is summed up succinctly as: "Until now, Australia was a key beneficiary of the rules-based global order and geographically protected from conventional threats. These contemporary threats against democracy, sovereignty and truth, which are enabled by modern communications technology and which blur the lines between East and West, civilian and military, and innocent civilian and government agent, 401 mean Australia needs to urgently engage,compete, and assert its dominance in the information environment." (Brooker 2021)

2.1.7 IW Impact on National Security

To better understand where we have come from in our understanding of information warfare and the changing threat level it was important to look at some older research to get a more holistic perspective. A study from 1997 studying the impact of IW on US national security done by the US Naval War College was included. The shift from reliable sea cables for communication to digital means. There are several broad strokes when depicting the various types of warfare. Many of these are more labeled in more detail today. Over 25 years ago the threat that one click could turn electricity, or power supplies would have happened in epidemic proportions would have happened by now is evident in the paper. "To date, we have been lucky. Yes, there have been disruptions, compromises,and theft of information. But, as far as can be ascertained, there has been no successful systematic attempt to subvert any of our critical computing systems. Unfortunately, there is reason to believe that our luck will soon run out

and that our national security will be challenged by information warfare targeted against our national information infrastructure."(Devries 1997)

2.1.8 No one is Immune to Misinformation

Misinformation is not only spread by ill-willed nations or individuals. There is still a troublesome percentage of misinformation that is shared unintentionally. Individuals that do not realize what they are sharing is in fact misinformation or it is shared in good faith makes up this percentage group. A 2021 study looking at the COVID-19 pandemic and the massive demand for information opened up for not only ill-intentioned misinformation, but the sharing of misinformation by good natured users. The study by design was made of a group that subscribed to a website that checks for validity of Covid-19 news. The survey revealed that a significant percentage of the group had shared information in the past that they were unsure of its validity. "It is puzzling that sharing of possible misinformation persists in a cohort who are both attuned to and concerned about misinformation and who actively seek the debunking of mis-information."(Saling et al. 2021)

2.1.9 Russia Fire Hose

The word disinformation comes from the Russian word dezinformatsiya, so it should only stand to reason that Russia is not only good at IW and disinformation campaigns, but that they have a special style. The Rand Corporation analyzed Russian propaganda and its development since 2008 to the present. The title "The Russian Fire hose of Falsehood' Propaganda Model" aptly describes the model created and widely used by Russian nation state actors. The fire hose of falsehood refers to the two techniques: using a high number of channels to spread a high volume of messages with a total disregard for what is fiction and what is the truth. Overwhelming the enemy with a mix of truth, half-truth, and complete falsehood. The result is confusion and disbelief for the enemy to try and deal with. According to the paper this tactic is the opposite of traditional IW strategy, where an emphasis on truth, credibility,and avoidance of contradiction. "New Russian propaganda entertains, confuses and overwhelms the audience"(Paul and Matthews 2021) The paper offers a few countermeasures. Traditional counter propaganda measures are not surprisingly ineffective against the Russian model. Or as the describe in the paper "don't expect to counter the fire hose of falsehood with the squirt gun of truth."(Paul and Matthews 2021) Forewarning is one of the most effective counter measures. Not refuting the points themselves, but informing the public that they are coming and to be aware. We have seen this counter measure most recently used by the US against Russian propaganda following the 2022 invasion of Ukraine.

2.1.10 Gameification of Information Warfare Strategy

This attitude ties in with a Finnish study that explored Information Warfare using gameification models. The study presented four models for the player strategy with mathematical formulas based on OODA loops. An OODA loop stands for Observe, Orient, Decide, Act and is a common decision making procedure used by military strategists. The four categories were:

- Terrorism- which focused on domination
- Evildoer – which focused on reduced domination

- Vandal -which focused on short-duration domination
- Rebel – which focused on rebellion leading to domination

The study concluded that when the pain level of the victim goes too high, they will rebel. According to Jormakka and Mölsä, the key to maintaining dominance was to dominate without making it too painful for the victim. (Jormakka and Mölsä 2005). The finds applied to both offensive and defensive dominance.

2.1.11 Troll Farms

With nation-states adopting new means by which they conduct information warfare, a research group decided to investigate how influential state-sponsored trolls have been used during recent information warfare campaigns. Turning to social media platforms like Twitter and Reddit, the group used a statistical model known as the Hawkes process. The Hawkes process counts a sequence of data points over time to create a model. Modeling trade orders, earthquakes, and even gang violence have used the Hawkes process. The results were based upon data from 1000 Twitter accounts and involved 27,000 tweets attributed to known Russian troll farms over 21 months. What was a bit surprising was that despite all of the effort by the Trolls, the effect was minimal. The significant exception was news published by R.T., the Russian state-sponsored news outlet. (Zannettou et al. 2019). The cost and effort is minimal since the campaigns can be relaunched over and over again with little effort as well as redesigned for different target audiences. This is what will make the tracking of such campaigns and the data gathered so crucial for future research.

2.1.12 Botnets

There are many different techniques to open or steal social media accounts, but how does having a large number accounts help if the dissemination of disinformation is too cumbersome? The answer is a botnet. Bot masters are looking for monetizing their bots via a diversified portfolio of work. The use of botnets for IW campaigns is one area where the strategies of nation states overlap with the civilian world. Botnets are traditionally known for Spam and DDoS attacks. The drive for increased profits have opened up the compromised networks to spreading disinformation via social media on behalf of their clients. The Lithuanian Technical Institute produced an interesting paper on Botnets which charts their beginnings from IRC chat rooms until today. The opinion of the researchers is that people are responsible for protecting their computers much in the way they are responsible for protecting their vehicles. (Juknius and Čenys 2009) In 2010 another researcher from the University of London did another study looking at the dangers of botnets. The researcher, Claire Elliott, confirmed the multiple dangers of a botnet. What makes them dangerous is their flexibility. (Elliott 2010) The botnet can be created under one premise, for example, DDoS attacks, or ransomware. However, once they are established the networks can be hired out to spread whatever the client wants, including misinformation. That makes the defense more tedious since delivering the information can happen immediately and from an overwhelming number of computers. APT groups can turn their botnets into propaganda machines if their employer so wishes. The lasting effects of such campaigns have to be adequately measured. However the turnaround for such networks depending on the client and their vastness make them a real threat.

2.1.13 Next Generation of Cyber-Enabled IW

The process of generating content for mass information warfare campaigns is labor intensive. What will happen when Artificial Intelligence and Machine Learning are more readily available for producing fake news and disinformation? The attackers capabilities are enhanced by technology. AI is not creative by nature and will only produce the average of the data used for training. Producing novel content is not yet a capability. According to a study produced by Conflict Research Centre people that have public facing content like politicians, business people, and celebrities are exceptionally at risk for such AI produced attacks due to the large amount of content available for training the AI. “While in 2019 the process of generating a Deepfake required human intervention, over the next decade this will become a far more automated process”.(Hartmann and Giles 2020) Will this remain a cat and mouse game between technology helping to defend and technology increasing harm? The outlook suggesting raising public awareness about the existence, its methods and indications seems apt.

2.1.14 Future of IW

Looking at the facts about the increase of IW attacks and spread of disinformation is important to the understanding of what is being done and can be done. Several emerging IW techniques using technology will make discerning what is real and what is not more of a challenge. Technologies like OpenAI’s GPT-3 for text has been demonstrated in numerous ways being able to generate content from only a few key words. An demonstration of an app given at Black Hat conference in 2021 that combines keywords given and GPT-3 to produce tweets.

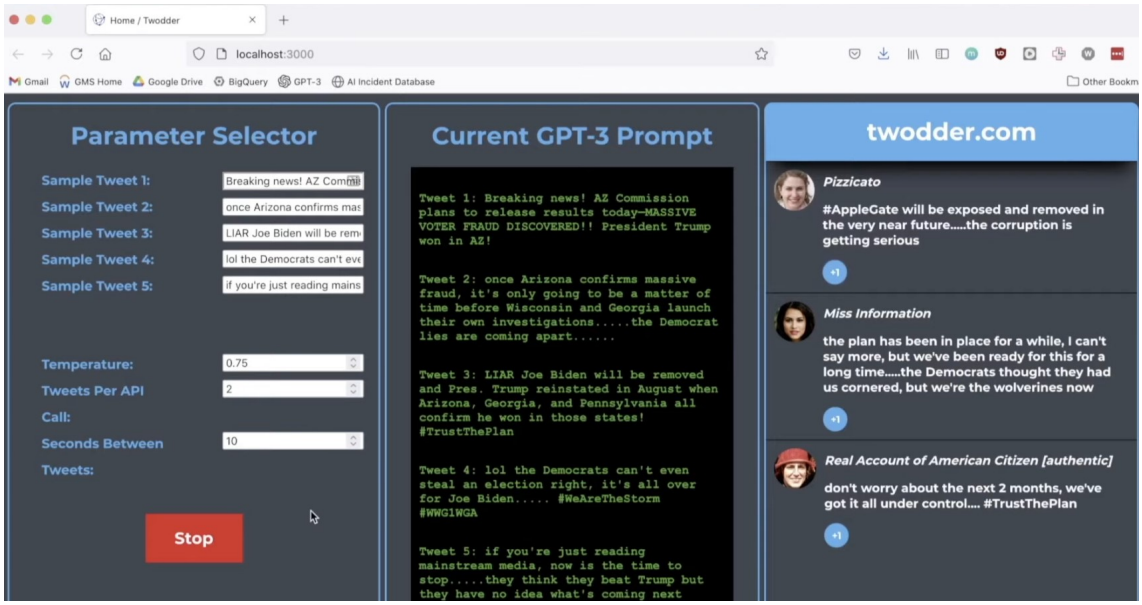

Figure 2.1: Twodder Black Hat demo
(Lohn 2022)

Keywords make the campaigns more specific and more difficult to detect. The capability for individuals to create malicious content at scale is scary enough. What happens when a large group or nation state employs the same technology? Similar techniques can be used when targeting populations. Exploiting tensions, or regional differences can split a nation. A study was conducted using GPT-3 and

several text examples to see how it can be weaponized. The researchers at the Center on Terrorism, Extremism, and Counter-terrorism demonstrated that GPT-3 was able to produce answers to simple questions about conspiracy groups like Qanon, and neo-nazi groups like the Atomwaffen Division. GPT-3 was also able to produce content based on what it knew of these groups. Today OpenAI is limiting access and the way the GPT-3 can be used by the general public. However that will not be the case forever as GPT-4 is already under development. The paper concluded if the terms change "Successful weaponization could include wholesale production of content used to synthetically populate interactive platforms such as forums and message boards, with minimal need for human curation of synthetic content, and testing and full evaluation of such content is recommended"(McGuffie and Newhouse 2020)

2.2 Current Metrics

2.2.1 Global Cyber Security Index

The International Telecommunication Union has 193 member states. They published a report called the Global Cyber Security Index and Cyber Wellness profile in 2015. The profiles outline each countries general wellness based on questionnaires. This report helps give a baseline for each member's development regarding connectivity and expansion of the technological infrastructure. An exciting area of the report are the questions regarding legal structures for protection and criminality. Another interesting area are the questions regarding security policies. With such a large group of members, there is a vast range from technologically underdeveloped nations like Eritrea, where 0,9 percent of the population use the internet, to highly developed like Denmark, where 94 percent of the people use the internet.(Peña-López et al. 2015) In 2021 the ITU released an updated version now called the Cyber Security Index. It is a more comprehensive report that weighs legal structures and protection policies highly. The countries are then ranked by an overall score based on measures taken in areas like Legal, Technical, Organizational, Capacity, and Cooperative. The updated rankings place the U.S. at number 1 and countries like Eritrea and Equatorial Guinea at the bottom of the scale.(Bruggemann et al. 2021)Probably most relevant to this paper was a median increase of 9,5 percent in infrastructure and internet usage from 2018 to 2020.

2.2.2 Cyber Power Index

The Belfer Center at Harvard has put together a Cyber Power Index for 2020. The CPI ranks 30 countries based on their intent and capabilities. These rankings give a different perspective and different rankings compared to the GCI. Countries like the U.S. and U.K. still rank highly on both, but countries like China and Russia make it into the top 5 of the Cyber Power Index with the added dimension of intent.Voo et al. n.d. The intent of countries with high cyber capabilities can expose a significant number of potential victims to information warfare campaigns. The CPI is only ranking 30 of the top nations. However, countries with lower capabilities can still be highly motivated to carry out cyber operations, which means that now a connected individual has the potential to be exposed to I.W. campaigns from 30+ nations. That is a great disparity compared to the bi-polar nature of The Cold War a few decades ago.

2.2.3 Social Side of Cyber Power

The distinction needs to be made that often it is assumed that Cyber Power means that same country would also be strong in conducting social media operations. Drew Herrick authored a paper pointing out the common mistakes made when analyzing social media operations and cyber power. The two do not go hand in hand and according to the author should not. Social media operations are public and provide a two way communication between the attacker and the victim(s). Cyber operations on the other hand want and or need to be stealthy. Most operations do not want their victim to even know they have been there. This difference means that a country that does not rank high on the CPI may still be a strong adversary in the IW and SO-ME operations space. But the reverse is not necessarily true “Policymakers, journalists, and even some academics often treat social media activity as a proxy variable for an actor’s latent technical proficiency and even cyber capability, in other words, its cyber power. Actors that are extremely successful at engaging in social media activities are assumed to be technically proficient and even capable of engaging in cyber operations.” (Herrick 2016)

2.2.4 Patents as Indicator of Cyber Power

Cyber power has traditionally been a difficult metric to accurately measure. Measurement is especially difficult in the realm of IW. Having large pools of technology and teams of hackers does not necessarily translate into IW capabilities as described in the “Social Side of Power”(Herrick 2016). Two researchers from Hungary offer a way to gain some insight into a country’s cyber capabilities. They offer looking at the nations patents as an indicator of its technological position in the world. The methodology analyzed the relative comparative advantage of a country measured by the impact of the patent instead of the number of patents. To accomplish this a 50 year old weighting system proposed by Balassa looked at the number of citations as a proxy of technological impact.(Mora-Apablaza and Navarrete 2022) This study has limitations. The data came only from the US Patent office from 2006-2015. Technology developed before 2008 or after 2015 and filed in the US Patent Office will not be part of the data set. Additionally technology patented in other parts of the world like Japan or the European Patent Office would also be left out of the study.

2.2.5 Permeation of Smartphones and Internet Access

Statistic websites like Statista have compiled smartphone sales and adoption data showing an increase over the last five years from 2020 to 2025. The number of users of Social Media has also globally increased to 3.78 billion in 2021 from 2.86 billion in 2017. The digital population is also on the rise. More users, more devices, more access, and more time on the internet can mean a larger threat vector for those users and a larger target for the perpetrators.

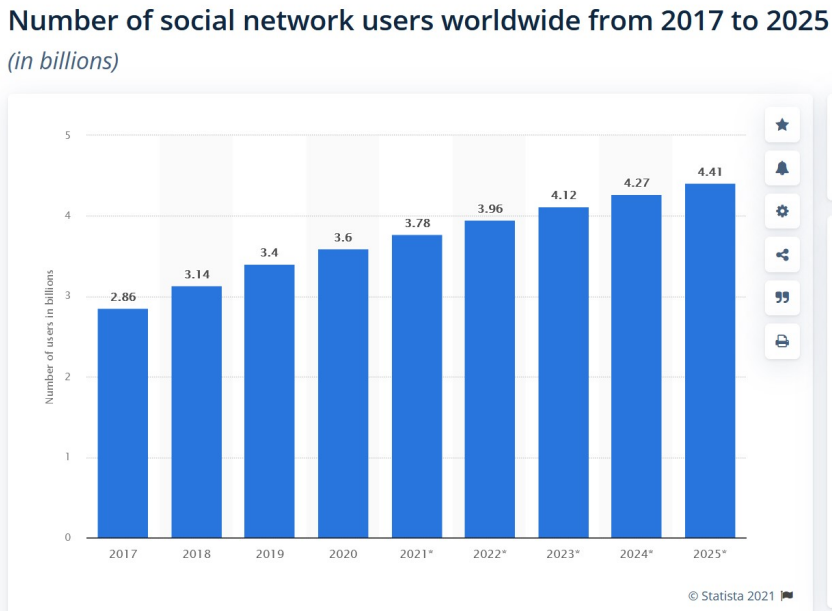

Figure 2.2: Social Network Users Worldwide
(Statista 2021c)

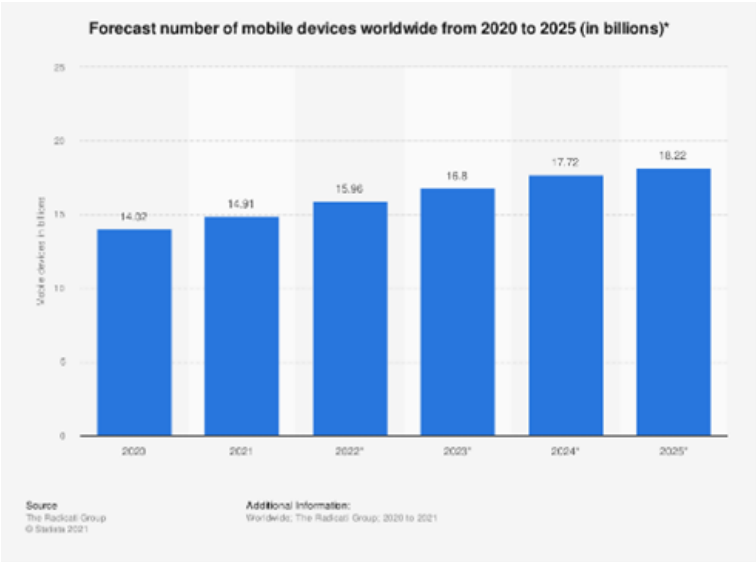

Figure 2.3: Mobile Devices Worldwide
(Statista 2021a)

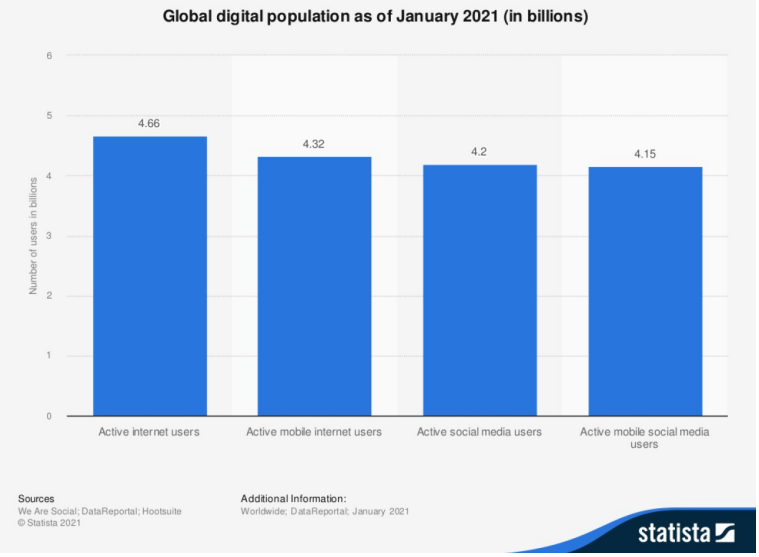

Figure 2.4: Global Digital Population
(Statista 2021b)

2.2.6 Disinformation Campaigns

The democratization of certain technologies allows the world's populations to connect and engage in ways never before experienced in human history. The same democratization also creates an opportunity for state actors and criminal groups alike as the communication horizons open up to the individual, so does their threat landscape. The lines for trustworthy media content are blurrier than ever as "sources" are popping up faster than services or regulators can verify them. Disinformation campaigns now have larger target audiences in addition to a more significant number of sources. According to the creators of the Global Disinformation Index, "Disinformation is the shadowy side to the open internet. It undermines faith in institutions, economies, governments, and even democracy itself" (Srinivasan and Fagan 2019)). Santosh and Fagan created a website that attempts to index as many as 30 of the most popular news sites in each of the ten countries they cover. The website disinformation index.org has several reports from 2019 and 2020 available for further research in specific markets. The information is limited and cumbersome for the average user, so the reports are not user-friendly. Defending against Information Warfare is not an easy task for a military. It is even more arduous for private citizens. The U.S. Military has adapted one of its previous Kill Chain strategies to combat Information Warfare.

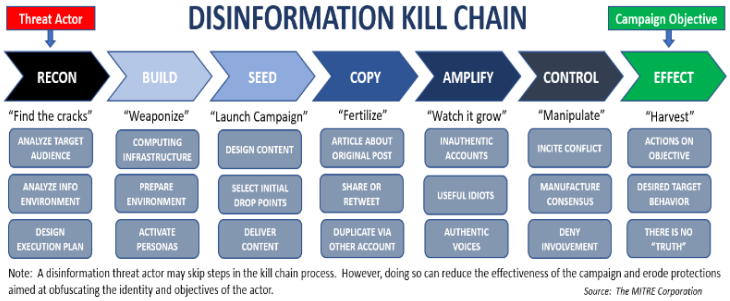

Figure 2.5: Disinformation Kill Chain
exchange (2019)

2.2.7 Private and Nation-State Actors

Going forward how does the average person defend themselves against a nation-state? Rarely in a kinetic situation are citizens asked to protect themselves against a nation-state. However, when the realm of conflict is cyber, citizens are often left to their own devices for defense. The Lithuanian Technical Institute produced an interesting paper on Botnets where The opinion of the researchers is that people are responsible for protecting their computers much in the way they are responsible for protecting their vehicles.(Juknius and Čenys 2009) What if that computer is compromised without their knowing? Most people are not responsible for protecting their car from an attack from abroad, and the lasting ramifications of a car theft are not as severe as a computer with their PII being compromised. The social, political, and ethical roles cybersecurity is playing and will play is the focus of a EU sponsored study examining how the different roles of people, governments, and organizations can influence cybersecurity. Cybersecurity can be at odds with different values and interests. “The provision of cybersecurity depends on numerous values, aims and requirements that are interrelated but also in competition or even conflict with each other.”(Weber 2022) This is concluded that the interests and power to enforce can be very different, so the citizen is in the weakest position and will on most occasions bare the cost of any compromise.

2.3 Characteristics

2.3.1 Individual Differences in Susceptibility to Cybercrime

Research that investigates susceptibility is limited. Especially in the realm of IW. However, some research has been done on susceptibility to cybercrime, and finding correlations if any between gender, IT confidence, and IT negligence. Time on the Internet was the main determinant whether any potential victim would be victim of a cyber crime. What was most interesting with this study was they found that of the subjects interviewed, those with high IT confidence were the most likely to be a victim of a cybercrime. Due mostly to their increased use of IT as a result of their confidence. The two remaining groups low IT confidence, and IT negligence could have represented a greater percentage of victims if they had similar use patterns as the high IT confidence group. While the study focused on susceptibility to cybercrime, there are several findings that can be extrapolated and applied to information warfare susceptibility. “IT skill training is no doubt essential, but greater effort should be expended to enhance users’ sensitivity to cyber threats and build their guardianship to combat such threats.”(Cheng, Chan, and Chau 2020)The need for greater education and limiting exposure to the internet were the recommendations. These translate directly to IW. Greater awareness and less exposure to the internet seem to be the best defense against IW campaigns.

2.3.2 Millennial Skepticism and Susceptibility to Media Persuasion

Millennials, those born between 1980 and 2000, with an age range of 18 to 35 have grown up to be skeptical of traditional corporations and traditional media. They therefore consume a majority of their news from online sources and the largest percentage of that comes from social media. A 2016 study produced a survey to test if there is a disconnect between their distrust of traditional media and their skepticism towards online media. The study was not conclusive, but was also limited by the test demographic. They were not able to get a wide enough age range in their 100 subjects. The study concluded with even though their study did not produce conclusive proof of a disconnect the

importance of further study “Since millennials’ news media consumption habits will ultimately shape the news media of the future, it couldn’t be of greater importance to explore and explain their habits for the purpose of self-correction” (Lee 2016)

2.3.3 Personal Character Impacting Phishing

Personality type combined with IT, and internet experience can indirectly combine to affect a persons susceptibility to phishing campaigns. A study from the Academy of Sciences in Beijing, China studied the answers to a study of 414 Chinese participants. The Big Five personality traits: Openness, Conscientiousness, Extroversion, Agreeableness, Neuroticism were the basis for how mail was processed and how susceptibility for falling for a phishing campaign. The conclusion that susceptibility is a combination of factors but that “a general personality profile for those who may easily fall prey to phishing includes low conscientiousness, low openness and high neuroticism.”(Ge et al. 2021). This directly translates to IW and whom may be susceptible.

2.3.4 Susceptibility to Online Influence and Victimization

Online susceptibility has several dimensions. Two studies, each tackling one of the dimensions. Online influence and cybercrime victimization and its psychological aftermath. Individual differences were key with both studies. Each person is individually susceptible to different things. The response and psychological aftermath is also individual. The study on victimization demonstrated two things. A positive correlation between IT knowledge and confidence, and an inverse correlation between victimization and trusting people online, perceived control,happiness. These findings indicate that as more people become IT proficient, they will spend more time online and have a greater chance of becoming a victim.(Cheng, Chan, and Chau 2020) The second study put forth a framework to help describe the individual differences so that better mitigation technologies can be developed.(Williams, Beardmore, and Joinson 2017)

2.4 DEFENSE:How Do We Defend Ourselves?

Technology will also need to be one of the saviors, and potentially Machine Learning is one of those technologies that can detect misinformation before it reaches the victim. The offense is several steps ahead of the defense, so more research and development is needed in the areas that will help defend users against Information Warfare. The authors of a study comparing different approaches to disinformation created a framework and common language to fill a gap that is hindering the study of misinfosec.They will expand the MITRE ATT&CK framework to include misinformation and create a similar framework of their own called AMITT.(Gray and Terp 2020) Interdisciplinary cooperation is the way forward.

2.4.1 APT Detection

Three researchers at CNCERT in Beijing, China, produced a paper exploring how the problem of tracking and finding APT group activities can be solved like a mathematical problem. “In this paper, through a deep study of Cyber Kill Chain behaviors, combined with intelligence analysis technology, we transform APT detecting problem to be a measurable mathematical problem through weighted

Bayesian classification with a correction factor to detect APTs and perceive threats."(Wen, Rao, and Yan 2018) The researchers conclude that their experiment did work. This is an area that should have further investigation. As with some previous studies using technology to combat some of the vulnerabilities that using technologies creates makes sense. The individual user does not stand a chance without technological resources to help them navigate the sea of misinformation and information warfare.

2.4.2 Detecting Susceptibility

A framework for detecting susceptibility was lacking in the academic circles when it comes to social engineering. The framework produced by a PhD student at Embry Riddle could be used or modified to include information warfare. The thesis attempts to address the gap left in other frameworks. Previous frameworks do not take into account such factors as national, cultural, organizational, and personality traits of employees. The list of countries used was quite extensive and grouped eventually into two categories. Victim and non-victim countries. The paper concluded that there needs to be more data, and in future research a deeper analysis could be done with less scarce data.(Alneami 2021) Having access to adequate data is a challenge for many research projects.

2.4.3 Phishing Susceptibility Detection through Social Media Analytics

Phishing emails and more specifically spear phishing emails are one of the ways that technology is used to specifically target victims for using their own personal information provided by their activity on social media websites there was a study done by 2 researchers in Canada that took a look at susceptibility detection through social media analytics. They analyzed the idea of coming up with not the detection system itself but more of I high level architecture for reconnaissance tools he came up with a flow control engine data preparation engines and data analysis engines and using those tools and it was possible to in their study evaluate the susceptibility of the person to his spirit fishing campaign based on their online activity. "The preliminary results from a prototype tool show that there is a lot of identifiable information that is easily accessible to the public about individuals that have social media accounts."(Alam and El-Khatib 2016) The tools are not complete, but are the start of what could become tools for people to analyze their publicly available information that is online. The goal of the architecture scheme is to better inform the public of what kind of information a potential attacker could find and use to create spear phishing campaigns. While spear phishing can be separate from information warfare the study uses the same data sets that could be used for either IW or spear phishing.

2.4.4 Detecting Phishing Using Machine Learning

Machine Learning and AI are two technologies that many look to when the speak about the future of things. Especially when it comes to defense, and protection. Combating both Fake News and Phishing websites with machine learning trained expert systems was the goal of a team to use machine learning that makes defensible decisions. A banned tweet for example would have an explanation. One of the fears of AI and ML are their potential bias. When the chain of inputs and decision process is not known they do not gain a lot of trust. When the machine learning makes defensible decisions with an explanation, the bias anxiety is relieved. This is accomplished by the machine learning training the expert system. There are data points that are partially used for further decision making. "The

system incorporates the concepts of partial membership and ambiguity, allowing fact values to be between 0 and 1. Rules, instead of just being logical 'AND' operators, store weighting values that define the contribution of each input fact towards the identified output fact. These weighting values must be between 0 and 1 and sum to 1."(Fitzpatrick, Liang, and Straub 2021) The next question was can it be effective? The study concluded that it was in fact effective at flagging websites as phishing and understanding the nuances of context and emotion when flagging fake news. Machine Learning Expert Systems (MLES) could be used by a wider range of neural networks not only for things like fake news and phishing, but analyzing datasets in general to minimize bias.

2.4.5 Understanding Limits of Auto Fact Check

Automated fact checking is one of the technologies that people at large are hoping will do the heavy lifting for catching fake news before it goes out into social media or into other media outlets there are some interesting different approaches and different techniques to auto fact checking which a research paper put together by Lucas graves for the Reuters institute looks at however the conclusion of the paper quite aptly again looks at the vast amounts of data from the huge amount of sources and it's an overwhelming proposition for any automated system to do an accurate job of catching fake news at scale and while there are various different approaches including identifying uh claims and verifying those claims it's still a problem of too much data too many sources and not enough reliability because it has to be almost perfect if it has a small percentage of failure that still means a large amount of a fake news makes it through the filters so this study is very interesting unfortunately it comes to the same conclusion that we see time again with some of the other studies that or just dealing with so much data that it's the technology for the detection needs to catch up with the scale that it's trying to be used for

2.4.6 Mutual Assured Destruction

Since cyber operations lend themselves to asymmetric warfare, will strategies and comparisons to the Cold War ever be valid? Can there be a mutually assured destruction situation that keeps nations from acting on their intentions? Jeremy Straub and his research team tried to address this question by modeling different modes of cyber warfare to compare against the "strategic bi-polarity" model from the Cold War. The work concluded that it is impossible to foresee a mutually assured destruction situation developing due to the multiplicity of domains, adversaries, and capabilities. Further research of relevant scenarios is planned.(Straub 2019)

2.4.7 Society Wide Combat Disinformation

Combating disinformation will take an entire society and a framework is needed to facilitate the co-operation between public and private organizations. That is what a study sponsored by the DHS set out to accomplish. A response framework was presented with the intention to: Hit the actor, Hit the Technology, Build Resilience, and Share Information. The stakeholders were identified and the need for literacy and transparency were expressed. It is still difficult to map the effect of disinformation campaigns "Disinformation can generate a lot of activity in a very short period of time, but whether this disinformation amounts to little more than noise in the system or represents a genuine threat is often not readily apparent."(exchange 2019) The role increased noise plays is a factor that will be looked at later in this paper.

2.4.8 Hoaxy

A joint research project from Indiana University and China's National University of Defense Technology published a paper introducing an online platform named Hoaxy. Hoaxy was developed to map the spread of rumors, hoaxes, fake news, and conspiracy theories. Terms can be searched for in real-time and the platform predicts the degree of likelihood that a bot network is involved. The plans for the platform will study active spreaders of fake news, which will allow for greater study. (Shao et al. 2016) The visual nature of the information is quite remarkable. Hoaxy provides some great information if the user is willing to search for it. The true benefit will be when the data gained can be used for future filtering of content. The website https://hoaxy.osome.iu.edu/ is currently up and can be accessed with a valid Twitter account.

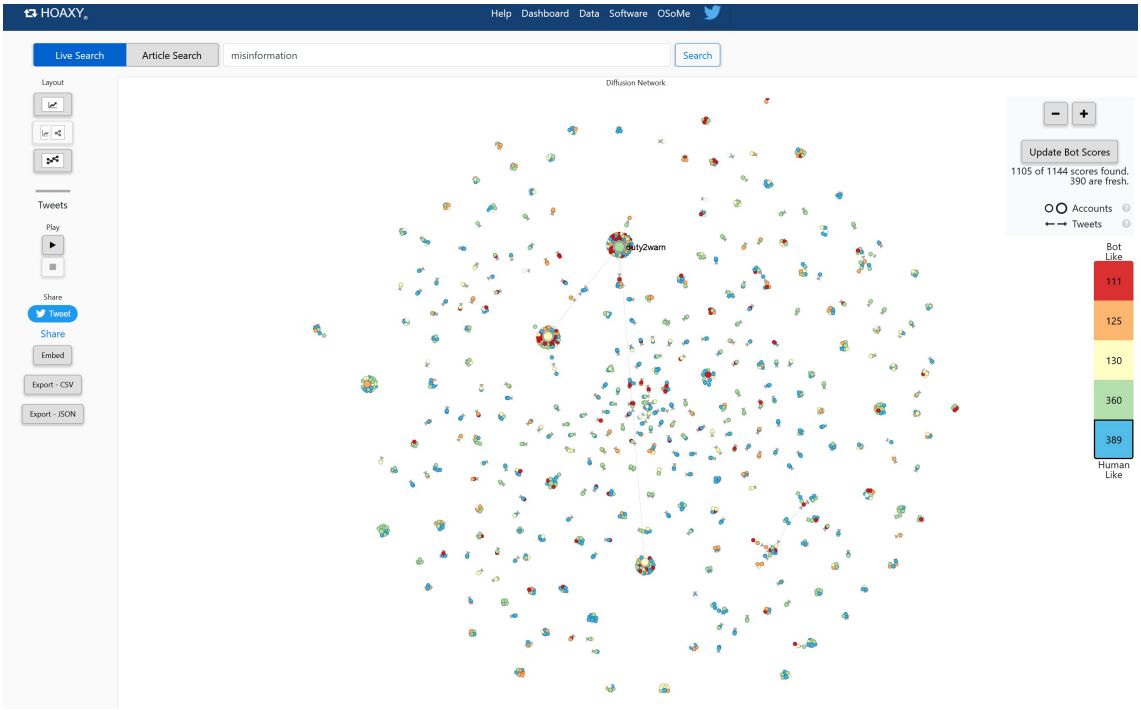

Figure 2.6: Hoaxy screenshot search term = misinformation
(Hoaxy 2021)

2.4.9 GDELT

One of the challenges with understanding IW and its many components and uses is the overwhelming amount of data that crosses the internet every second. What is trustworthy information and what is misinformation or disinformation? The time and resources necessary needed to fact check and confirm is nearly impossible on a human level. Time is against us. By the time something is fact checked and confirmed or denied it is already "old news". Seeing global trends in real time is one of the necessary tools that will allow people to better understand what is real and what is not. The GDELT Project is a real time network diagram and database of global human society for open research.(2022) It is a database supported by Google Jigsaw, which is a division of Google combating censorship and disinformation, that presents in real time global trends in news. It is a searchable database with various dashboards available. Thus allowing research and better understanding of what is happening around the world. This may not be a tool for the average person, however other tools leveraging this data will certainly be able to help people in the future be more selective in what they are accepting as truth. As stated previously the future war is for who controls the narrative. The GDELT Project is one of the tools that can help societies to combat those trying to maintain or gain control of what is true and what is not.

2.4.10 Information Literacy

It is often said that we are analog citizens living in a digital world. The shift to a digital world has been happening at a pace that most people have difficulty keeping up with. The rate at which fake news and misinformation is created and disseminated overwhelms most consumers and even the technology charged with filtering/protecting users. Going back to the roots with literacy as a key tool to have in each individuals tool chest. IT Literacy, Information Literacy, Media Literacy, and even Digital Media Literacy are names for a similar strategy:education. Educating the people on how better to filter sources as opposed to the approach used today "post-truth". "The over consumption of information fuelled by the internet has produced a so-called "post-truth" society in which people consume information that reaffirms their pre-existing beliefs and ideologies rather than attempting the difficult task of identifying the truth."(De Paor and Heravi 2020). The question of who will be the best for education is answered by two researchers from Ireland. They wrote a paper for the Journal of Academic Librarianship to introduce the idea that Librarians who have traditionally been the gatekeepers and fact-checkers before the digital age. They are trained in information science and their roles from traditional librarianship to educator is needed in order to combat the overwhelming amount of fake news, misinformation, and disinformation.

2.4.11 Increased Noise

The overwhelming sentiment is that misinformation and fake news are a scourge and need to be stopped. While this may be true, is there evidence that hearts and minds have been changing as quickly and dramatically as suspected? Not everyone agrees. Researchers at the Institut Montaigne in France have looked at foreign information operations targeting France. The researchers agree that the number of countries involved with information operations has only increased and the tactics have changed as well. Their key question is "Have we made too big a deal out of disinformation? The paradox is that most of us are entirely convinced that content has the power to tell us what to buy or who to vote for, but scientists have not yet determined what impact content truly has on how

opinions are formed."(Lenoir 2021) The volume of information and disinformation could mean that a bigger threat is "post-truth" bias. People choosing media and sources that confirm what they already believe to be true. It is less daunting than the task of wading through the sea of disinformation floating around on the web today. "Addressing disinformation in 2022 will require both stopping the spread of foreign information that aims to voluntarily deceit, and reducing hasty conclusions in public debates that portray disinformation as the cause of social tensions."(Lenoir 2021)

2.4.12 Limited Reach of Fake News

A group of Italian researchers took a look at the spread of fake news on Twitter during the 2019 European elections they took a look at approximately 400,000 tweets between 863 different accounts over a three day period from May 26-29, 2019. The accounts were chosen because they were conversing about different issues of the European Parliament election.(Cinelli et al. 2020)They did not find through their quantitative analysis that there was any connection between disinformation organizations and the spreading of these tweets so this was an interesting look at how a tweets in a smaller group 400,000 is quite a lot but when you have a continent of 300 million people over a three day period it's just a very small percentage and it was for three days between the 23rd and 26th of may 2019 So what this speaks to is the amount of data that it makes any of this so difficult the amount of data to look at and analyze and the computing power and the analytical power and the time it's just overwhelming it's overwhelming for researchers it's overwhelming for computers and even when there's programs written to do a lot of the analysis four or automated that probably is one of the reasons we do not see nearly as much research about the actual effects of some of these it IW campaigns that compared to the research done on the potential dangers of IW campaigns.

3

Analysis/Implementation

3.1 Analysis

The methodology for this paper consists of four stages. The first stage is a systematic collection of existing research. Keywords were identified like technology, information warfare, and susceptibility. Finding existing research with the key words as the subject matter was instrumental to starting the project. Research papers often included other key words that were added to the list and explored. Research topics were expanded in order to get a broader perspective of information warfare and the available research. There is a plethora of research regarding the looming dangers of information warfare. However, success of campaigns and attribution research is understandably difficult to find. Many of the campaigns and suspected campaigns do not have a body that takes credit. The world wide web is indeed a web in which the perpetrators weave their own sticky web of content producers and network of sharing and spreading. Therefore the research gathered for this paper mainly focuses on the methodologies and the metrics for prediction of susceptibility. It is out of the scope of this paper to include research of or statistics about successful campaigns. The second stage of the research was to conduct a literature review. The number of sources is extensive for the length of the project, however information warfare is a broad subject and focusing the project on the technology side allowed for narrowing the scope to a manageable level to complete withing the allotted time. The literature review demonstrates a sample of the most relevant research that was found. The literature includes methodologies and strategy. Date was not a determining factor when collecting literature sources. Many of the early research source contained predictions which did come true with regards to hybrid mixing between traditional and information warfare used by modern armies. The research that predated the early 2000s did not predict the powerful force of social media, which was very interesting to see that it has surprised all of us. The third stage was the analysis. The analysis method

used was a hybrid approach. A majority of the research is qualitative in nature. Giving background information without hard statistics. This part of the research formed the basis for answering the question whether or not a society is more susceptible to information warfare. The answer however needed to be quantitative. After understanding the nature of the answers statistical data was gathered and compiled with the end goal of a metric that would allow for not only comparison between nations, but expansion of data points and tracking over time. The fourth stage was the creation of the metrics and weighting. This project had limited scope and a limited time for completion. Therefore the number of countries and data points was also limited. Four countries were chosen: Norway,South Africa, Argentina, Colombia. Four data points were also chosen: Overall trust in news, Trust in Social Media for news, Percent of news from Social Media, and Education rankings 2021. The countries were chosen to specifically demonstrate differences between the criteria and show that a ranking with value could be created. In order to give value to be ranked a weighting system was developed with points given per block of percentage. Education ranking was given a score based on ranking. Countries in top 20 were given 1 point, top 21-40 given two points and so on.

3.2 Implementation

To get to the final metric a few steps of distillation were necessary in order to compile the data for ranking. Data of internet usage worldwide was collected. Education rankings, and Global censorship by country. The countries where a full picture of data could be displayed were chosen and then from that group a final group of four countries was used to display the range of scores possible.

Individuals using the internet worldwide 2019, by region	
Developed	87%
Europe	83%
The Americas	77%
CIS*	73%
World	51%
Arab States	55%
Asia and Pacific	45%
Developing	44%
Africa	29%
Least Developed Countries (LDCs)	19%
Land Locked Developing Countries (LLDCs)	27%
Small Island Developing States (SIDS)	52%

Figure 3.1: Regional Internet Use
(Statista 2021d)

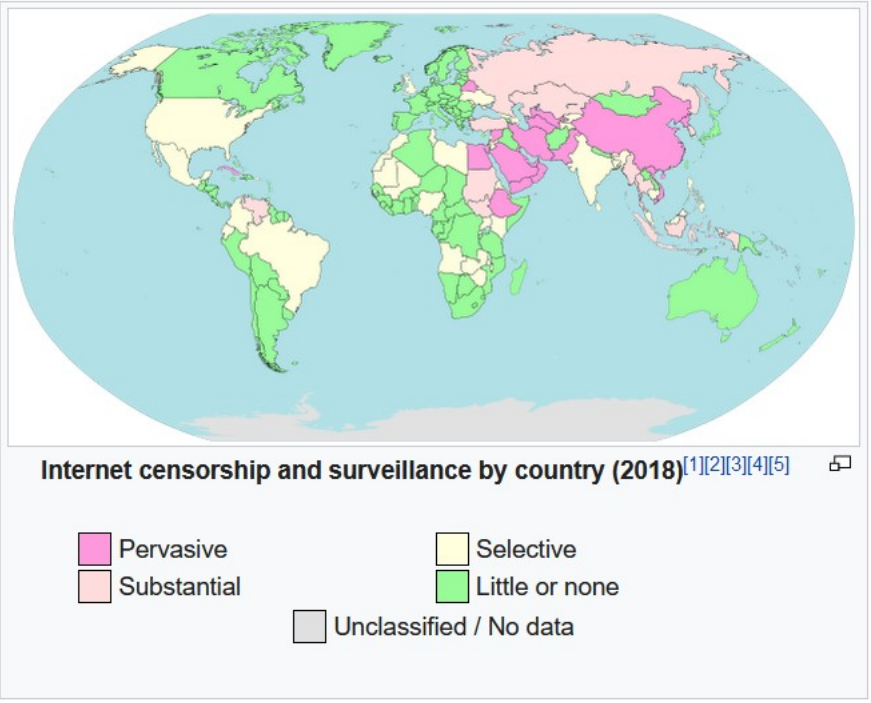

Figure 3.2: Global Net Censorship
(Jeffrey Ogden 2018)

Country	Facebook Users	Population 2021	Percent of population using Facebook	Education ranking 2021	% news from social media
Taiwan	19,190,000	23,855,010	80.44%	17	54
Malaysia	25,520,000	32,776,194	77.86%	42	72
Singapore	4,470,000	5,896,686	75.81%	1	57
United Stat	240,000,000	332,915,073	72.09%	20	42
Hong Kong	5,361,000	7,552,810	70.98%	6	61
Chile	13,000,000	19,212,361	67.66%	43	69
Argentina	30,000,000	45,605,826	65.78%	52	66
Thailand	46,000,000	69,950,850	65.76%	77	78
Brazil	139,000,000	213,993,437	64.96%	91	63
Philippines	71,760,000	111,046,913	64.62%	86	72
United King	44,000,000	68,207,116	64.51%	16	41
Denmark	3,700,000	5,813,298	63.65%	3	46
Norway	3,400,000	5,465,630	62.21%	10	44
Sweden	6,300,000	10,160,169	62.01%	14	47
Canada	23,000,000	38,067,903	60.42%	5	55
Peru	20,000,000	33,359,418	59.95%	66	70
Mexico	78,000,000	130,262,216	59.88%	72	67
Slovakia	3,200,000	5,460,721	58.60%	49	56
Australia	15,000,000	25,788,215	58.17%	9	47
Netherlanc	9,800,000	17,173,099	57.07%	7	37
Portugal	5,800,000	10,167,925	57.04%	39	55
Colombia	29,000,000	51,265,844	56.57%	73	70

Figure 3.3: Prosperity Index Statistics
(*Legatum Prosperity Index* 2021)(*Trust:NewsSoMe* 2021)

4

Results

The research suggests that there is an ever present danger that is only increasing with time. The solutions suggested are limited and currently do not help the masses beyond education. There are many frameworks, and mathematical models suggested. How can the average user relate? As the public becomes more aware of IW and its potential sources and motives the tactics and technology used will only keep getting more precise. The battle for the definition of reality will push the demand for greater tools for manipulation. Hopefully the tools for defense will keep pace. Where does that leave us? With the research pointing towards to potential danger and a limited amount of research demonstrating correlation between IW campaigns and direct outcomes. A metric was created in order to take some of the basic metrics and score them in order to give a rating. A rating that could be used for ranking or comparison. These rankings could then over time be compared against different years to establish trends. The results would suggest that with a lower score a country is less likely to be susceptible to information warfare. Norway for example had a total score of 9 where South Africa had 16. Therefore based on the table is suggested that South Africa is more susceptible to information warfare than Norway. Two key points being percent of news from social media and education ranking. They are dramatically different comparing Norway with an education ranking of 10 and South Africa with an education ranking of 108. In addition Norway receives 10% of its news from social media where South Africa receives 61%. These two factors alone can explain much of the great disparity between the two nations.

The research used for this paper demonstrate the various complexities of digital life and information warfare. Displaying the data in a format that individuals can understand clearly was the goal. Further contribution to the existing complexities was not the goal of the metric.

Country	Overall trust in news	points	Trust in Social Media for news	points	Percent of news from Social Media	points	Education ranking 2021	points	Total
Norway	57%	6	18%	2	10%	1	10	1	**9**
South Africa	52%	6	29%	3	61%	7	108	6	**16**
Argentina	36%	4	28%	3	66%	7	52	3	**14**
Colombia	40%	4	42%	5	70%	7	70	4	**16**

Lower score will result in higher resiliance

Figure 4.1: Country to country comparison

News	Percentile	Points		Education	Range	Points
Key	0-10%	1		Key	top 20	1
	11-20%	2			from 20-40	2
	21-30%	3			from40-60	3
	31-40	4			from 60-80	4
	41-50	5			from 80-100	5
	51-60	6			from 101-120	6
	61-70	7			from 121 -130	7
	71-80	8			from 131-140	8
	81-90	9			from 140-160	9
	91-100	10			from 160-180	10
					from 181	11

Figure 4.2: Comparison key

5

Conclusion

5.1 Introduction

This aim of this paper was to examine the effects of information technology on susceptibility to information warfare campaigns and create an analysis tool for predicting a nations susceptibility. The area is new and there is much research that has yet to be done. There are several remaining questions when it comes to technologies role in information warfare. Not all nations are forthcoming with their plans or capabilities. Making data gathering difficult. Attribution is difficult, which makes data collection on the perpetrators more difficult. Since attribution is difficult and penalties are few the incentive is greater, because it is harder to get caught. Without international treaties there will be few international repercussions. Cyber operations will continue to play a greater role in a nations military defense strategy and are often regarded as less lethal and far lower cost, when compared to modern day kinetic warfare. The question of how lethal is IW? is a point that is actively debated. While cyber operations are currently regarded as less lethal than kinetic, they are hard to defend against, hard to quantify their effectiveness, and the time frame between deployment and payoff can be long. Nation-states can use the very devices and technology that everyday citizens use to communicate as a way in to their lives via disinformation campaigns and false information websites. Social media allows for large campaigns to spread faster and touch more individuals than ever before. Campaigns that are deemed less effective can be relaunched time and again for little or no cost. As one may use a reminder in their calendar to set the alarm for an appointment or send a critical email, similar automation for tweets, blog entries, and viral news stories can be created. The Cambridge Analytica scandal showed that micro-targeting is real and based on just a handful of data points. These same data points can be bought on the open market and used by bad actors, both foreign and domestic, to precisely target information warfare campaigns.

So what can be done to defend against the myriad of disinformation? Technology, ironically enough, may be able to help. As some articles suggest, the defender is often four steps behind the offender, and a technological solution will be needed to combat Information Warfare. Using Machine Learning for vetting news stories in real-time before they spread false information could be a partial answer. Some of the Global indexes for Disinformation will have a big enough pool of data and sources to be an effective website or app that citizens can use to check sources of stories spreading on social media. Something needs to be done as the bad guys are turning an old playbook into a new strategy and using criminal groups to help spread their word. Botnets will, unfortunately, be used to conduct automated attacks via social media outlets more and more. The tools to combat their disinformation spreading will need to be equally as vast. Again it is difficult to gauge the effectiveness of the campaigns. When the data is available, it will hopefully be anecdotal to demonstrate that the measures were well deserved. Maybe the best defense people have right now against such campaigns is their short attention spans and lack of motivation due to an overwhelming amount of information consumed and presented every day. In April 2022 “A court in Moscow has ordered Google to pay an 11 million ruble ($134,500) fine over materials about Russia’s ongoing unprovoked invasion of Ukraine on YouTube.”(2022) This is a recent example of the Russian government controlling the narrative about the invasion of Ukraine using censorship as its tactic of information warfare.

5.2 Summary of Research

The bulk of the research explores the dangers of information warfare both real and perceived. The majority of the research that I came across specifically targeted military and more governmental a large portion of that research it is American based done by American think tanks American universities or military organizations did find quite a bit of European and even some Asian based research on information warfare I think the reason a majority of the research pertains to the militaries there possibly the ones that are paying for the studies compared to just people is idle curiosity to find out how effective programs really are and there seems to be a lack of research on how effective any of these campaigns are I found only one significant study done in Australia by the military by a woman in the military for her masters program other than that there was just math with some mathematical models lot of ideas and and structures but nothing concrete to show that a campaign a had effect be uh there are course news stories and anecdotal stories but actual academic research I was not able to find very much

5.3 Research Objectives

The objective with this paper was to look at the research that has been conducted and try and quantify the effect that technology will have on a society and their susceptibility to information warfare. Looking at the technology being used it quickly became apparent that there is a consensus regarding the danger posed by information warfare. Everyone should prepare for this danger. More smartphones with more Internet access and more apps open up the door for greater communication between people not only in local communities but across the world. The spread of fake news, disinformation, misinformation happen much faster and at greater scale. How does this contribute to making a society more vulnerable? More susceptible? What factors would be key in determining the answers? With so many different types of strategies and different motivations the objective really tried to focus on

how can we look at a society that is adopting these technologies like smartphones and why it makes people vulnerable? People regardless of where they live, what language they speak, education level or economic status are all more or less given the same tools. We all have Facebook. We all have YouTube. We all have Whats App or Instagram or a local version of those apps depending on what country the person is living in and taking that forward to look at what are those factors and then taking those factors and trying to put some numbers around them quantify them. Quantification is important for future studies that can take the data and make it even more granular by adding more data and better criteria. Weighting the criteria so that some of the factors like education level or belief in social media news or access to social media news access to it regular media news and so on and then weigh them out to come up with the score at the end. The score can be compared country to country and could potentially be extrapolated. These metrics can be tracked over time to see if the society is becoming more susceptible or less susceptible as time goes on as more defenses are added and as people's education levels are increased. This is the main objective of this paper

5.4 Research Contribution

The research contribution of this paper is developing a metric that could allow for comparison either between two or more countries for a given year, or look for trends over multiple years. Either for a single country or multiple countries. The metric would be able to be used in future research and to be expanded further with more criteria and taken onto a larger and larger scales both geographically and with greater populations. I chose to test the metric with multiple countries in order to demonstrate the differences in scoring. Countries that may have similar metrics in some categories could end up with a completely different result after scoring all categories. The goal is to do that this is a starting point for future research that could continue looking at how is society may be more susceptible then another one but also in addition how can these metrics be tracked and expanded so that overtime you could see if a society was becoming more susceptible or less susceptible to information warfare campaigns. Having tangible data would be necessary to create legislatively protective measures. Currently there is no international legislation that governs the rules of cyber or information warfare. Paris Call for Trust and Security in Cyberspace, put forth by France's president Emmanuel Macron in 2018, is maybe the closest potential agreement that asks nations to honor nine points of self governance.(2018) This idea should be taken further by organizations like the UN. Having statistical data for the effectiveness of IW campaigns can bolster the need for drafting such legislation. The starting point for discussion and understanding with the ability for broadening and expansion is the real research contribution of the project.

5.5 Future Work

With a longer time frame to continue this project it could be expanded in several dimensions in order to create trend data. The number of nations could be expanded which would possibly show trends over geographic regions allowing for a different type of comparison than just country to country. Geographic trends could then open up for more questions regarding culture, internet access, government type and do those criteria play a role in a society's susceptibility? The criteria used in this project could be expanded as data becomes available including average internet and average social media use per day. As well as government type, freedom of press and or speech, and economics as a start.

The more criteria included will give a more granular insight. All of this data becomes more valuable when the same is plotted over many years. It would be important for the success of the project to be able to produce trend data. That data can then be analyzed further. There is great potential for future development and better understanding of how societies are affected by information warfare. Considering the difficulty of attribution and the lack of criminal prosecution there is little data to suggest that the trend of using technology to propagate information warfare will decrease in the years ahead. Therefore it would be important to gain as much insight as possible into how or if society's susceptibilities are changing over time. Those changes can be plotted against any existing data of efforts to combat information warfare for example education. If trends start to show and for example a country changes its trust in social media or percent of news from social media finding the answer as to why could be another exciting extension of the project. An increase of IW activity could possibly affect those numbers in either a positive or negative way. There are several interesting directions for the project to develop given the appropriate time and resources.

Bibliography

(2018). URL: https://pariscall.international/en/principles.

(2022). URL: https://www.gdeltproject.org/data.html.

(2022). URL: https://www.rferl.org/a/russia-google-fines-ukraine-war/31814512.html.

Adamsky, Dmitry (2015). *Cross-domain coercion: the current Russian art of strategy*. IFRI Security Studies Center.

Alam, Safwan and Khalil El-Khatib (2016). "Phishing susceptibility detection through social media analytics". In: *Proceedings of the 9th International Conference on Security of Information and Networks*, pp. 61–64.

Alneami, Hashim H (2021). "A Framework to Detect the Susceptibility of Employees to Social Engineering Attacks". In.

Bradshaw, Samantha and Philip N Howard (2019). "The global disinformation order: 2019 global inventory of organised social media manipulation". In.

Brooker, Cassandra (2021). "The Effectiveness of Influence Activities in Information Warfare". In: *Australian Army Research Centre*.

Bruggemann, Rainer et al. (2021). "Global Cyber security Index (GCI) and the Role of its 5 Pillars". In: *Social Indicators Research*, pp. 1–19.

Cheng, Cecilia, Linus Chan, and Chor-lam Chau (2020). "Individual differences in susceptibility to cybercrime victimization and its psychological aftermath". In: *Computers in Human Behavior* 108, p. 106311.

Cinelli, Matteo et al. (2020). "The limited reach of fake news on Twitter during 2019 European elections". In: *PloS one* 15.6, e0234689.

De Paor, Saoirse and Bahareh Heravi (2020). "Information literacy and fake news: How the field of librarianship can help combat the epidemic of fake news". In: *The Journal of Academic Librarianship* 46.5, p. 102218.

Devries, Anita D (1997). *Information Warfare and Its Impact on National Security.* Tech. rep. NAVAL WAR COLL NEWPORT RI.

Egloff, Florian J and James Shires (2021). "The better angels of our digital nature? Offensive cyber capabilities and state violence". In: *European Journal of International Security*, pp. 1–20.

Elliott, Claire (2010). "Botnets: To what extent are they a threat to information security?" In: *Information security technical report* 15.3, pp. 79–103.

exchange, Public private analytic (2019). *Combating Targeted Disinformation Campaigns*. Analytic Exchange Program, pp. 1–28.

Fitzpatrick, Benjamin, Xinyu Sherwin Liang, and Jeremy Straub (2021). *Fake News and Phishing Detection Using a Machine Learning Trained Expert System*. URL: https://arxiv.org/abs/2108.08264.

Ge, Yan et al. (2021). "How personal characteristics impact phishing susceptibility: The mediating role of mail processing". In: *Applied Ergonomics* 97, p. 103526.

Gray, John F and Sara-Jayne Terp (2020). "European Journal of International Security". In: pp. 1–10.

Hartmann, Kim and Keir Giles (2020). "The next generation of cyber-enabled information warfare". In: *2020 12th International Conference on Cyber Conflict (CyCon)*. Vol. 1300. IEEE, pp. 233–250.

Herrick, Drew (2016). "The social side of 'cyber power'? Social media and cyber operations". In: *2016 8th International Conference on Cyber Conflict (CyCon)*. IEEE, pp. 99–111.

Hoaxy (2021). *Hoaxy Live Search*. URL: https://hoaxy.osome.iu.edu/#query=misinformation&sort=mixed&type=Twitter&lang=. (accessed: 16-October-2021).

Jeffrey Ogden CC0, via Wikimedia Commons (2018). *Internet Censorship and Surveillance*. [Online; accessed 22-Dec-2021]. URL: https://commons.wikimedia.org/wiki/%20File:InternetCensorshipandSurveil svg.

Jormakka, Jorma and Jarmo VE Mölsä (2005). "Modelling information warfare as a game". In: *Journal of information warfare* 4.2, pp. 12–25.

Juknius, Jonas and Antanas Čenys (2009). "Intelligent botnet attacks in modern Information warfare". In: *Proceedings of 15th International Conference on Information and Software Technologies*, pp. 39–42.

Lee, Olivia K (2016). "Millennial skepticism and susceptibility to media persuasion". In.

Legatum Prosperity Index (2021). URL: https://www.prosperity.com/rankings?pinned=&filter=. (accessed on 12-November-2021).

Lenoir, Théophile (2021). *The Noise Around Disinformation*. URL: https://www.institutmontaigne.org/en/blog/noise-around-disinformation.

Libicki, Martin C (2020). "The convergence of information warfare". In: *Information warfare in the age of cyber conflict*. Routledge, pp. 15–26.

Lohn, Andrew (2022). *Disinformation At Scale: Using GPT-3 Maliciously for Information Operations*. URL: https://www.youtube.com/watch?v=cWf2uMh-skY&t=608s.

Ma, Zhanshan, Axel W Krings, and Frederick T Sheldon (2009). "An outline of the three-layer survivability analysis architecture for strategic information warfare research". In: *Proceedings of the 5th Annual Workshop on Cyber Security and Information Intelligence Research: Cyber Security and Information Intelligence Challenges and Strategies*, pp. 1–7.

McGuffie, Kris and Alex Newhouse (2020). "The radicalization risks of GPT-3 and advanced neural language models". In: *arXiv preprint arXiv:2009.06807*.

Mora-Apablaza, Loreto and Carlos Navarrete (2022). "Patents as indicators of the technological position of countries on a global level?" In: *Scientometrics*, pp. 1–14.

Paul, Christopher and Miriam Matthews (2021). *The Russian 'Firehose of Falsehood' Propaganda Model*. Santa Monica, CA: RAND Corporation. DOI: 10.7249/CPA614-4.

Peña-López, Ismael et al. (2015). "Global cyber security index & cyber wellness profiles". In.

Saling, Lauren L et al. (2021). "No one is immune to misinformation: An investigation of misinformation sharing by subscribers to a fact-checking newsletter". In: *Plos one* 16.8, e0255702.

Shao, Chengcheng et al. (2016). "Hoaxy: A platform for tracking online misinformation". In: *Proceedings of the 25th international conference companion on world wide web*, pp. 745–750.

Srinivasan, Santhosh and Craig Fagan (2019). *Rating the disinformation risks of news domains: Global Disinformation Index.*

Statista (2021a). *Forecast number of mobile devices worldwide from 2020 to 2025 (in billions)**. URL: https://www.statista.com/statistics/245501/multiple-mobile-device-ownership-worldwide/. (accessed: 10-October-2021).

– (2021b). *Global digital population as of January 2021*. URL: https://www.statista.com/statistics/617136/digital-population-worldwide/. (accessed: 10-October-2021).

– (2021c). *Number of social network users worldwide from 2017 to 2025*. URL: https://www.statista.com/statistics/278414/number-of-worldwide-social-network-users/. (accessed: 10-October-2021).

– (2021d). *Percentage of individuals using the internet worldwide in 2019, by region*. URL: https://www.statista.com/statistics/333879/individuals-using-the-internet-worldwide-region/. (accessed: 19-October-2021).

Straub, Jeremy (2019). "Mutual assured destruction in information, influence and cyber warfare: Comparing, contrasting and combining relevant scenarios". In: *Technology in Society* 59, p. 101177.

Studies, Naval, National Research Council, et al. (1997). *Technology for the United States Navy and Marine Corps, 2000-2035: Becoming a 21st-Century Force: Volume 3: Technology*. National Academies Press.

Trust:NewsSoMe (2021). URL: https://reutersinstitute.politics.ox.ac.uk/digital-news-report/2021/interactive. (accessed on 12-November-2021).

Voo, Julia et al. (n.d.). "Re-conceptualizing Cyber Power". In: ().

Weber, Karsten (2022). "CYBERSECURITY AND ETHICAL, SOCIAL, AND POLITICAL CONSIDERATIONS: WHEN CYBERSECURITY FOR ALL IS NOT ON THE TABLE". In: *Humanities and Social Sciences* 29.1, pp. 87–95.

Wen, Senhao, Yu Rao, and Hanbing Yan (2018). "Information Protecting against APT Based on the Study of Cyber Kill Chain with Weighted Bayesian Classification with Correction Factor". In: *Proceedings of the 7th International Conference on Informatics, Environment, Energy and Applications*, pp. 231–235.

Wikipedia (2021). *Information warfareWikipedia, The Free Encyclopedia*. [Online; accessed 11-October-2021]. URL: https://en.wikipedia.org/wiki/Information_warfare.

Williams, Emma J, Amy Beardmore, and Adam N Joinson (2017). "Individual differences in susceptibility to online influence: A theoretical review". In: *Computers in Human Behavior* 72, pp. 412–421.

Zannettou, Savvas et al. (2019). "Disinformation warfare: Understanding state-sponsored trolls on Twitter and their influence on the web". In: *Companion proceedings of the 2019 world wide web conference*, pp. 218–226.

A

Appendix

A.1 Short Paper

How adopting technology makes a society more susceptible to information warfare

1st Travis Clark
Noroff Universtity College
Kristiansand, Norway
tlcnor@gmail.com

***Abstract*—The military has been the primary user of information warfare in the past. Modern technology has allowed the private sector and criminal groups to join the fight for information and its control. The methodologies used by both nation-state actors and civilian groups are similar. This paper will explore the methods and what factors may cause a nation to become susceptible to information warfare from both sides.**

***Index Terms*—information warfare, methods, technology, military strategy, susceptibility**

I. Introduction

Information warfare traditionally has been a realm of operation reserved for the military. The fast pace of technology and growing global inter-connectivity has made information itself one of the most valuable global commodities. Competition for such a valuable commodity means information warfare tactics are no longer reserved for nation-states and military forces of the world. There is an emerging civilian side to information warfare, not only on the victim's side but also on the attacker's side. Information is the current frontier of commerce and an emerging stage of warfare. The information security industry knows the CIA as acronym for confidentiality, integrity, and availability. Confidentiality and availability have always been part of the attack strategy. Integrity has come under attack especially as technology makes it easier to create fake versions of voice and video. Attacking the integrity of information makes it harder to know what is real and who would have changed the data. Lack of attribution and a collective disagreement about the proper response for information warfare or cyber-attacks means most governments and criminal groups go unpunished. [1] Lawmakers may someday see the disruption of these three attributes of information by an enemy or criminal as an act of information warfare.Future global agreements and treaties will need to establish rules of engagement regarding cyber activities. Today, large social media platforms, mobile device makers, and data brokers collectively provide an abundance of information. Information that nation states, military, and private sectors all draw from to use to curate campaigns at a much lower cost than kinetic warfare. Facebook alone creates an abundance of data, having a larger online population than India and China combined, with roughly 2,9 billion users. [2] Corporations are seeing an increase in cyber and information warfare attacks from competitors and governments. Intellectual property and personal information give geopolitical advantages that traditional military and information warfare campaigns could not provide. Ethics is the only boundary left, stopping only the most egregious of attacks. Balkin describes, "it is not an exaggeration.to say that modern states are informational states that recognize and solve problems of governance by collecting, analyzing, and distributing information." [3] Information warfare comes in different forms and has various applications depending on the goal and target of the campaign. This paper will examine existing models for information warfare and how they apply to both military and private sector campaigns. An analysis of who is vulnerable and a presentation of the different models will be given.

II. Related Work

Since the 90s, non-military groups have been increasing their use of technology for the purpose of information warfare. Thanks to technology and the wide adoption globally of smartphones,information warfare need not be limited to military use. [4] Winn Schwartau defined information warfare by dividing it first into 3 classes: Personal, Corporate, and Global. Class 1 Information warfare is an attack against an individual's electronic privacy: Digital records, files, or other portions of a person's electronic essence. Class 2 Information Warfare however, is about more than the acquisition of information: it's also about the use of information -real or ersatz. Class 3 Information Warfare Is waged against industries, political spheres of influence, global economic forces, or even against entire countries. It is the use of technology against technology; it is about secrets and the theft of secrets. [5] What they did not predict in the earlier examinations was the smartphone and explosion of social media. The wide adoption of both have sped up the timeline for all three classes. Information and its protection have now become geopolitical. [6] Companies, private citizens, and militaries alike handle the protection and defense of their information from an unprecedented number of attack vectors. The democratization of technology has simultaneously increased the number of attack vectors along with the possibilities for interaction, as the development is often beyond purview of governments. The future ramifications of technologies outpacing governments' ability to stay on top and fully understand the rapid development remain to be seen. [7]

Nations are choosing bytes over bullets. "Almost every nation in the world now has a cyber exploitation program." Robert Joyce, Cyber security director for the NSA, said at the Aspen Cyber Summit that the vast majority of those are

used for espionage and intelligence purposes," Joyce also said "There is interest in dabbling in offensive cyber and outcomes". [8] In modern times, all information is valuable. Traditionally, militaries would have engaged in information warfare to keep their battle plans secure and try to get the enemies' battle plans. Today, the goals can be motivated by both geopolitics and economics. With fewer nations using military forces to wage a conventional war, a more hybrid approach is increasingly more common. The cost of entry for cyber capabilities is far lower than traditional weapons. A small group can have a far greater reach of their information warfare campaigns using cyber. Something that would be unthinkable a few decades ago. Technology presents an equal opportunity for both military and civilian. Information warfare plays a more significant role in nation-states trying to defend their nations' information while trying to get another nation's information.

Dr.Martin Libicki wrote a paper in 1995 titled "What is information warfare?" [9], where he already defined seven forms of information warfare as:

- Command and Control Warfare (C2W)
- Intelligent-Based Warfare (IBW)
- Electronic Warfare (EW)
- Psychological Warfare (PW)
- Economic Information Warfare (EIW)
- Hackers Warfare (HW)
- Cyber Warfare (CW)

These forms are important when trying to explore the different methods of information warfare, especially within of the context of Schwartau's definition. Combining the seven forms from Dr.Libicki with the three classes from Schwartau allows for granular classification of methodologies. Certain groups either nation states or civilian each have certain expertise or motivations that make one type of attack more attractive than another. Attribution is difficult with cyber attacks in general. Information warfare attacks using cyber maybe even more difficult. Not only are the operational security tactics one part, but the motivation behind the attack is another. Trying to attribute the attacks can be risky as many researchers and journalists have seen the tactics turned toward them during their investigations. [10]

III. Data Gathering/Analysis

I divided the gathered data into two groups, military and civilian. The tactics can overlap between the two groups since they are often using similar playbooks and technologies. The analysis of the different tactics remains with the primary use group. Which factors will play a key role in the attack? Can the motivations be discerned? These are some of the key questions for the different methodologies and attributions. **MILITARY SECTOR** The strategies used for military and nation-state are motivated by gaining control or maintaining control of an adversary's information. Techniques involving misinformation and disinformation are for gaining political will or influencing political outcomes. Capturing or interrupting and adversaries' military strategy as well as influencing future strategical decisions are both optimum goals for military based information warfare. In more recent years some militaries have added economic gain to their motivations. Stealing of crypto currency and or intellectutal property are two of the most popular targets.

Gamification Gamification of information warfare is a method for researching and understanding the potential outcomes of information warfare campaigns. The researchers understood, from the results, that the correct balance of pain is needed for a campaign to succeed. Too much pain causes resistance. Just enough and for not too long of a period will get the best results. The OODA loop-based models were put into four categories: Terrorism- which focused on domination Evildoer–which focused on reduced domination Vandal -which focused on short-duration domination Rebel–which focused on rebellion leading to domination The study concluded that when the pain level of the victim goes too high, they will rebel. Dominance is maintained by not making the victim realize too much pain. [11] Walking this fine line of dominance without too much pain can be a challenge with cyber. Attacks can come fast and from so many different angles it can overwhelm. Cyber has given nation-states access to networks of "warriors" for hire that would not usually be an option for traditional military operations. Criminal groups can offer their services to governments that will pay. These programs can run in parallel with state-sponsored activities. Both groups have different objectives and have different degrees of deniability. For some criminal groups it is a win/win situation as an employee of the government by day they are allowed to operate by night without repercussion for their criminal activities. [12]

Hybrid Approach The Hybrid Approach is the meeting of cyber with traditional warfare. Military forces see the value in adding cyber because of its far-reaching effect at a comparatively low cost. Information warfare is being used to disrupt before traditional troop movements. Controlling information or overloading a group with information results in confusion about what is happening. This can give a crucial window to a military with little organized resistance. [13]

Convergence Nation-states waging a more hybrid type of warfare is only natural, according to Dr. Martin Libicki. Dr. Libicki has held many institutional positions within American academia and defense. In his 2017 article entitled "The Convergence of Information Warfare," He further explains that as technology trends rise and other countries exploit those trends, then it is "far less plausible to imagine a cyber-attack. campaign unaccompanied by other elements of information warfare—in large part because almost all situations where cyber-attacks are useful are those which offer no good reason not to use other elements of information warfare." [14] **Troll farms** conduct information warfare campaigns via social media. For little cost, messages are generated and posted, thus trolling the followers. Political or financial motivations can spill over to botnets. Criminal groups controlling a botnet and working with governments can offer their services for payment or exemption from prosecution/extradition. Employment of

botnets to further a troll farms reach is another tactic. Most of the algorithms on social media platforms reward the activities of engagement such as likes with posts being promoted in the feeds of followers and potential followers. [15] The future will only be more challenging for individuals to discern what is real and what is not accurate. Deep-fake audio and deep-fake video will be easier and cheaper to create. The technology will move into the smartphone app market making it available to most of the over four billion users worldwide. Artificial Intelligence companies like Open AI create text-based AI that can have a conversation and create text based on a subject. While not perfect today, GPT3 will create simple messages in great quantity that can be perfect for such platforms as Twitter and Facebook. The next generation GPT4 will be even better. [16] The size of a nation's military budget means a military or nation-state can be the sponsor or first adopter of much of the technology developed by the private sector. As a first adopter, there is a time advantage to be gained, which could mean the difference between success or failure of a mission.

CIVILIAN SECTOR

The civilian attacks can be similar to military and have been adding stochastic terrorism as well for political and economic gain. **Stochastic Terrorism** is defined as the incitement of violence through public demonizing of a group or individual. [17] Platforms allowing people to make such inciting claims are now available to everyone with internet access. The broad audience also allows for plausible deniability if an unpredictable follower acts on the demonizing. The unpredictability and difficulty with attribution have made it an attractive mode of operation for political figures as well as media personalities alike. **Troll Farms** With nation-states adopting new means by which they conduct information warfare, a research group investigated how influential state-sponsored trolls have been during recent information warfare campaigns. Turning to social media platforms like Twitter and Reddit, the group used a statistical model known as the Hawkes process. The Hawkes process counts a sequence of data points over time to create a model. Modeling trade orders, earthquakes, and even gang violence have used the Hawkes process. The results based upon data from 1000 Twitter accounts and involved 27,000 tweets attributed to known Russian troll farms over 21 months. What was surprising was that despite all the effort by the Trolls, the effect was minimal. The significant exception was news published by RT, the Russian state-sponsored news outlet. [18] This minimal effect should not deter the troll farms since the cost is also minimal and older campaigns can be given new life quite quickly. Pictures, memes, and posts are often seen recirculating with some minor adjustments or updates over time. Sometimes just re-branded for a different purpose.

DEFENSE Some might say that the offensive side has all the advantages right now. Defense is several steps behind, but what is being done to close the gap? **APT detection** Three researchers at CNCERT in Beijing, China, produced a paper exploring how the problem of tracking and finding APT group activities can be solved as a mathematical problem. "In this paper, through a deep study of Cyber Kill Chain behaviors, combined with intelligence analysis technology, we transform APT detecting problem to be a measurable mathematical problem through weighted Bayesian classification with a correction factor to detect APTs and perceive threats." [19] The researchers concluded that their experiment worked. This is an area that should have further investigation. As, with some previous studies using technology to combat some vulnerabilities that using technologies creates makes sense. The individual user does not stand a chance without technological resources to help them navigate the sea of misinformation and information warfare. A joint research project from Indiana University and China's National University of Defense Technology published a paper introducing an online platform named Hoaxy. Hoaxy was developed to map the spread of rumors, hoaxes, fake news, and conspiracy theories. Terms can be searched for in real time and the platform predicts the likelihood of involvement from a bot network. The plans for the platform will study active spreaders of fake news, which will allow for greater study by others. [20] The visual nature of the information is quite remarkable. Hoaxy provides some great information if the user will search for it. The true benefit will be when the data gained is used to filter future content. The website https://hoaxy.osome.iu.edu/ is currently up and can be accessed with a valid Twitter account. One of the best defenses against all of the technological avenues for attack is increasing information literacy. Forbes author and GDELT project founder Kaleev Leetharu describes how teaching people to be information literate is the only way to combat "fake news" as technology will not do it alone. " the only way to truly begin to combat the spread of digital falsehoods is to understand that they represent a societal rather than a technological issue and to return to the early days of the Web when we taught society to question what they read online." [21]

IV. Results

Most nations have increased their use of mobile devices and social media. Studies show that traditional media outlets are losing out to online and social media-derived news sources. Technology will make it more challenging in the future for users to understand what is real and what is fake. Nation-states, militaries, and private sector groups are taking advantage of the user-created data pool for information warfare. They will continue to increase their efforts in the future until the ethical standards for cyber-attacks change. Who is susceptible? Everyone, as the attacks can come from anyone, from anywhere, at anytime. Investing in education teaching information literacy may be one of the best ways to combat modern information warfare. Technology companies like to push the idea that there is a technological solution for every problem, yet this seems to be as much a people problem as it is a technology problem. Further examination of these factors are needed, however preliminary analysis of not only having access to the internet, but what type of access will play a role. Is the access highly censored or not? Freedom of the press and multiple

news sources? Restrictions cause choke points and while choke points are good for defending a network, they are not good for the free flow of information and access to the truth instead of a narrative. Figure 4 demonstrates the varying levels of internet censorship globally.

V. Conclusion and Future Work

Information warfare will only continue to be a larger part of our daily interaction with the internet as the focus goes away from only military to both military and private sector. As technology is adopted by people and the complexity of the technology used to defend systems increases, attackers know it is often easiest to go after the users and not the system itself. This paper has demonstrated that the cost of engagement is decreasing and that more and more players are using information warfare to conduct their campaigns. The offense has an advantage in technology and methods. Future work will include a deeper examination of the methods used for information warfare campaigns and if there are any geographic or geopolitical differences in their success or failure. A graph or chart showing the differences will visually represent the results of the examination.

VI. Metrics

Several metrics have been created by different research and professional organizations. Different indexes depicting the different levels of cyber capabilities, as well as legislative statistics give way for different ranking systems. The two largest are the Global Cyber Security Index and Cyber Power Index.

A. Global Cyber Security Index

The International Telecommunication Union has 193 member states. They published a report called the Global Cyber Security Index and Cyber Wellness profile in 2015. The profiles outline each country's general wellness based on questionnaires. This report helps give a baseline for each member's development regarding connectivity and expansion of the technological infrastructure. An exciting area of the report are the questions regarding legal structures for protection and criminality. Another interesting area is the questions regarding security policies. With such a large group of members, there is a vast range from technologically underdeveloped nations like Eritrea, where 0,9 percent of the population use the internet, to highly developed like Denmark, where 94 percent of the people use the internet. [22] In 2021, the ITU released an updated version, now called the Cyber Security Index. It is a more comprehensive report that weighs legal structures and protection policies highly. An overall score based on measures taken in areas like Legal, Technical, Organizational, Capacity, and Cooperative then ranked the countries. The updated rankings place the U.S. at number 1 and countries like Eritrea and Equatorial Guinea at the bottom of the scale. [20] Probably most relevant to this paper was a median increase of 9,5 percent in infrastructure and internet usage from 2018 to 2020.

1) Cyber Power Index: The Belfer Center at Harvard has put together a Cyber Power Index for 2020. The CPI ranks 30 countries based on their intent and capabilities. These rankings give a different perspective and different rankings compared to the GCI. Countries like the U.S. and U.K. still rank high on both, but countries like China and Russia make it into the top 5 of the Cyber Power Index with the added dimension of intent. [23] The intent of countries with high cyber capabilities can expose a significant number of potential victims to information warfare campaigns. The CPI is only ranking 30 of the top nations. However, countries with lower capabilities can still be highly motivated to carry out cyber operations, so now a connected individual has the potential to be exposed to information warfare campaigns from 30+ nations. That is a great disparity compared to the bi-polar nature of The Cold War a few decades ago. Since cyber operations lend themselves to asymmetric warfare, will strategies and comparisons to the Cold War ever be valid? Can there be a cyber version of mutually assured destruction situation that keep nations from acting on their intentions? Jeremy Straub and his research team tried to address this question by modeling different modes of cyber warfare to compare against the "strategic bi-polarity" model from the Cold War. The work concluded that it is impossible to foresee a mutually assured destruction situation developing because of the multiplicity of domains, adversaries, and capabilities. Further research of relevant scenarios is planned. [24]

VII. Figures and Tables

Individuals using the internet worldwide 2019, by region	
Developed	87%
Europe	83%
The Americas	77%
CIS*	73%
World	51%
Arab States	55%
Asia and Pacific	45%
Developing	44%
Africa	29%
Least Developed Countries (LDCs)	19%
Land Locked Developing Countries (LLDCs)	27%
Small Island Developing States (SIDS)	52%

Fig. 1. Global permeation of internet 2019 [25]

Worldwide digital population as of January 2021	
Global digital population as of January 2021 (in billions)	
Active internet users	4.66
Active mobile internet users	4.32
Active social media users	4.2
Active mobile social media users	4.15

Fig. 2. World Digital Population 2021 [26]

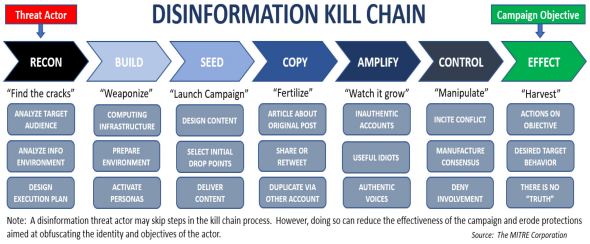

Fig. 3. Disinformation Kill Chain [27]

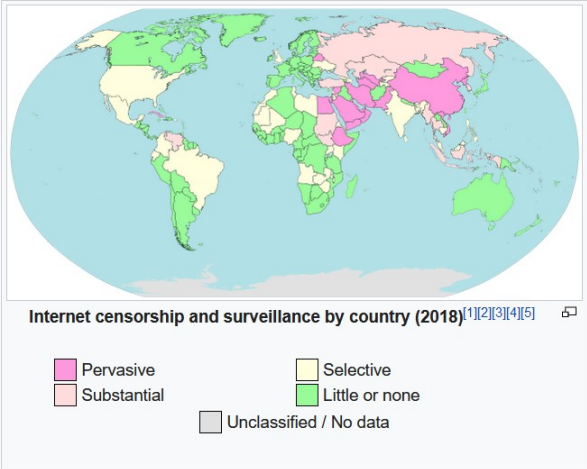

Fig. 4. Internet censorship by country 2018 [28]

REFERENCES

[1] F. J. Egloff and J. Shires, "The better angels of our digital nature? offensive cyber capabilities and state violence," *European Journal of International Security*, pp. 1–20, 2021.

[2] Statista. Number of monthly active facebook users worldwide as of 2nd quarter 2021. [Online]. Available: https://www.statista.com/statistics/264810/number-of-monthly-active-facebook-users-worldwide/

[3] J. M. Balkin, "The first amendment is an information policy," *Hofstra L. Rev.*, vol. 41, p. 1, 2012.

[4] H. Crawford, Blaise Cronin, "Information warfare: Its application in military and civilian contexts," *The Information Society*, vol. 15, no. 4, pp. 257–263, 1999.

[5] W. Schwartau, *Information warfare: Chaos on the electronic superhighway*. Thunder's Mouth Press New York, 1994.

[6] E. Rosenbach and K. Mansted, *The geopolitics of information*. Belfer Center for Science and International Affairs, 2019.

[7] C. Kavanagh, *New tech, new threats, and new governance challenges: an opportunity to craft smarter responses?* Carnegie Endowment for International Peace., 2019.

[8] T. A. Institute. Fireside chat: The next generation of threats. Youtube. [Online]. Available: https://https://www.youtube.com/watch?v=aOz4rN98fhs

[9] M. C. Libicki, *What is information warfare?* NATIONAL DEFENSE UNIV WASHINGTON DC INST FOR NATIONAL STRATEGIC STUDIES, 1995.

[10] H. Carr, "The power of non-attribution in modern information warfare," *Three Swords Magazine*, pp. 42–45, 2018.

[11] J. Jormakka and J. V. Mölsä, "Modelling information warfare as a game," *Journal of information warfare*, vol. 4, no. 2, pp. 12–25, 2005.

[12] S. Zannettou, T. Caulfield, E. De Cristofaro, M. Sirivianos, G. Stringhini, and J. Blackburn, "Disinformation warfare: Understanding state-sponsored trolls on twitter and their influence on the web," in *Companion proceedings of the 2019 worldwide web conference*, 2019, pp. 218–226.

[13] D. Adamsky, *Cross-domain coercion: the current Russian art of strategy*. IFRI Security Studies Center, 2015.

[14] M. C. Libicki, "The convergence of information warfare," in *Information warfare in the age of cyber conflict*. Routledge, 2020, pp. 15–26.

[15] S. Zannettou, T. Caulfield, E. De Cristofaro, M. Sirivianos, G. Stringhini, and J. Blackburn, "Disinformation warfare: Understanding state-sponsored trolls on twitter and their influence on the web," in *Companion proceedings of the 2019 world wide web conference*, 2019, pp. 218–226.

[16] K. McGuffie and A. Newhouse, "The radicalization risks of gpt-3 and advanced neural language models," *arXiv preprint arXiv:2009.06807*, 2020.

[17] M. Amman and J. R. Meloy, "Stochastic terrorism," *Perspectives on Terrorism*, vol. 15, no. 5, pp. 2–13, 2021.

[18] C. Elliott, "Botnets: To what extent are they a threat to information security?" *Information security technical report*, vol. 15, no. 3, pp. 79–103, 2010.

[19] S. Wen, Y. Rao, and H. Yan, "Information protecting against apt based on the study of cyber kill chain with weighted bayesian classification with correction factor," in *Proceedings of the 7th International Conference on Informatics, Environment, Energy and Applications*, 2018, pp. 231–235.

[20] C. Shao, G. L. Ciampaglia, A. Flammini, and F. Menczer, "Hoaxy: A platform for tracking online misinformation," in *Proceedings of the 25th international conference companion on world wide web*, 2016, pp. 745–750.

[21] K. Leetaru, "A reminder that 'fake news' is an information literacy problem - not a technology problem," 2019. [Online]. Available: https://www.forbes.com/sites/kalevleetaru/2019/07/07/a-reminder-that-fake-news-is-an-information-literacy-problem-not-a-technology-problem/?sh=97a52ca6a6f2

[22] R. Bruggemann, P. Koppatz, M. Scholl, and R. Schuktomow, "Global cybersecurity index (gci) and the role of its 5 pillars," *Social Indicators Research*, pp. 1–19, 2021.

[23] ——, "Global cybersecurity index (gci) and the role of its 5 pillars," *Social Indicators Research*, pp. 1–19, 2021.

[24] J. Straub, "Mutual assured destruction in information, influence and cyber warfare: Comparing, contrasting and combining relevant scenarios," *Technology in Society*, vol. 59, p. 101177, 2019.

[25] Statista. Percentage of individuals using the internet worldwide in 2019, by region. [Online]. Available: https://www.statista.com/statistics/333879/individuals-using-the-internet-worldwide-region/

[26] ——. Global digital population as of january 2021. [Online]. Available: https://www.statista.com/statistics/617136/digital-population-worldwide/

[27] e. a. Paul M, "Combating targeted disinformation campaigns," *AEP2019*, p. 1–28, 2019.

[28] v. W. C. Jeffrey Ogden (W163), CC0, "Internet censorship and surveillance," 2018, [Online; accessed 22-Dec-2021]. [Online]. Available: https://commons.wikimedia.org/wiki/File:InternetCensorshipandSurveillanceWorldMap.svg

Word count metrics

NUC Bachelor Project Word Count:
Total Sum count: 11265 Words in text: 11040 Words in headers: 188 Words outside text (captions, etc.): 37 Number of headers: 62 Number of floats/tables/figures: 10 Number of math inlines: 0 Number of math displayed: 0
NOTE: References are excluded.