Introduction

Disinformation is defined as false information spread deliberately with intent to deceive, often attracting a large pool of naïve users with timely information. This is not a new phenomenon, but a problem with increased prevalence due to the development of newer communication technology. In most cases, online intruders employ psychological tactics to incite excitement or fear attempting to fool users to download programs or click links to compromised websites. Once the malware is downloaded to individuals’ devices, hackers have unlimited access to all personal information. This is how the rise of fake news contributes to the swelling amount of cyber attack.

Online intruders begin by the widespread information they can access through hacking which they illegally obtain users’ personal information for economic benefits. Advanced technology has only assisted hackers in becoming more elusive. Phishing mail is one of the commonly used ways, comprising about 71 percent of commencement of cyber-attack, according to the research done by Varonis, a software security company. Clickbait is another method in which online intruders mislead users to certain webpages that contain a virus.

Targets of cyber-attacks range from individuals to entire industries and governments. The damage on the governance causes tremendous loss. Business’ lose an average of 2.4 million dollars per malware attack, whereas the average cost of lost or stolen records and accounts per citizen is only about 141 dollar. Moreover, the damage related to cybersecurity is projected to hit annual 6 million dollars by 2021. For
the sake of European nations, it is imperative to address this rise of cyber-attacks by preventing disinformation.

**Background**

Disinformation, or fake news, is present in almost every online article, ranging from blatant falsifications to minor exaggerations in news reporting. However, when it comes to disinformation targeting specific groups of readers with the purpose of hacktivism, the issue is particularly urgent in Europe. In particular, the EU parliamentary elections of May 2019 evoked a flood of concerns regarding potential foreign influence.

In the fight to strengthen national cybersecurity, there has been a variety of responses. Many nations have placed the responsibility of preventing the spread of fake news on technology and media companies. For instance, the Italian government has required Facebook to monitor any false materials related to Italian democracy. Hence, Facebook created a new fact-checking program that can identify and debunk misleading articles by flagging newly uploaded false articles as a related article to false information, thus notifying users that the content of the article has been disputed by fact-checkers.

On the other hand, French and German governments attempted to create an ambitious set of laws aimed towards the elimination of disinformation among social network platforms. Specifically, the German government has recently proposed a solution last year which called on major social media platforms to eliminate unlawful online content within 24 hours since it was uploaded. Yet, this set of laws has evoked great concern about conditions that constitute fake news and safeguards for freedom of expression. Lastly other European nations chose to build governmental task force units to strengthen cybersecurity itself rather than to set up disinformation regulations on citizens. The United Kingdom and the Czech Republic are examples of those countries. The Czech Republic has comprised a 20-person unit of the Interior Ministry that monitors any potential threats of the disinformation campaign. Moreover, the government emphasized conversation than regulation, which means it has put tremendous effort to approach to citizens by teaching them how to avoid from the risk of disinformation threats and cyber
threats via their social media accounts. However, the public still gives more attention to seemingly tempting fake news than the truth approved by the government.

The worldwide number of cyber attacks is on the uprise. Even ransomware attacks, a type of malware attack which is designed to block access to a computer system until a sum of money is paid, is growing more than 350 percent everywhere according to the research done by Varonis. Indeed, the issue of disinformation that contributes to the rise of cyber attack is abysmal. Unfortunately, the full scope of the problem remains largely unclear, making effective recourse difficult to achieve.

**Problems Raised**

*Malware attack*

Proliferating malware throughout millions of private business and governmental devices has been the most commonly used way of attacking and destroying computer systems and networks. There are numerous types of malware including ransomware, adware, crimeware, spyware, stealware and so on. Once any of these specific kinds of malware is downloaded, it can greatly influence your device by stealing sensitive information, allowing unauthorized access to system resources, disrupting operations, and even creating problems with the network. The incognizant act of opening up malware that is dressed up as a program – an advertisement or a link – can lead to a chain of disastrous consequences. Particularly, malware attacks often leads to concerns of data theft, the act of stealing computer-based information from an unknowing victim with the intent of compromising privacy or obtaining confidential information. If this was an act of organized crime targeting a specific individual, the possible exploitation of financial and technical documentation could be tremendous. Moreover, the US Securities and Exchange Commission’s survey concluded that small and midsize business companies are principal targets for groups of online intruders. However, Victims fail to sense the urgency of the problem as only
29 percent of small businesses seek for improvements in their security measures. Thus, in this case, the group of hackers can actively destroy innocent users' computers and trade sensitive information for economic, social, or even political purposes. In line with EU data protection law, governments should do their utmost to protect an individuals’ rights.

**Extended roles of social media companies**

Europol, the EU’s law enforcement intelligence agency, has even announced that the EU Council has adopted the EU Law Enforcement Emergency Response Protocol. This ensures that EU will respond to cross-border cyber more efficiently by cooperating with other local agencies across the border and sharing all the information about those threats. Despite the strengthened governmental law enforcement, the amount of cyber attack in the form of disinformation online is still inconceivable. Hence, most EU governments have the tendency to pawn off the responsibility of preventing the spread of fake news on major social media and technology companies. In the case of Europe, numerous vendors such as Cloudflare, Google, Microsoft, and Symantec have come up with free services. According to Europol, Microsoft even expanded its AccountGuard in order to build up better protection against cyber crimes hidden behind junk news. The company has interfered in elections in the U.S. and Europe. In other words, the burden of handling cyber crimes has passed along to private business companies causing various problems including economic loss. As governments tend to avoid their duties, global technology companies are currently suffering from the dilemma of the likelihood of cyber attacks while still risking themselves against online intruders.

**International Actions**

**EU Law Enforcement and Emergency Response Protocol**

The large-scale cyber attacks crippling individuals, businesses, and even further society are less inconceivable as Wil van Gemert, Deputy Executive Director of Operations at Europol, has mentioned that it is critical to increase cyber preparedness in order to protect citizens from much more sophisticated
attmepts of cyber crimes. This EU Protocol is adopted by the EU Council and takes important parts in Europol's European Cybercrime Centre (EC3) as well as the EU Blueprint for Coordinated Response to Large-Scale Cross-Border Cybersecurity Incidents and Crises. This EU wide-resource is a big step forward in supporting the EU law enforcement authorities with not only providing an immediate response to major cross-border cyber-attacks, securing and timely sharing critical information, but also helping effective coordination of the international aspects for addressing increasing sophistication of nation-state and cybercriminal-sponsored attacks. The protocol follows the major stakeholder process which is consisted of seven stages from the early detection to the closure of emergency response protocol.

**EU joint and coordinated action against disinformation**

The EU joint and coordinated action against disinformation is another robust framework that the European Commission has enacted, in cooperation with the European Parliament, the EU Council, the European Economic and Social Committee, and the Committee of the regions. Member states have put effort to tackle the spread of disinformation via this joint since March 2015. In 2015, the European External Action Service (EEAS) has launched a new task force called East StartCom against disinformation. With this starting action, the EU council has made great achievements throughout 2018. They first have come up with a variety of measures securing free and fair European elections and then the code of practice which was the set of measures to fight against disinformation. Followed by the launch of Observatory for Disinformation and Social Media Analysis,
action plans, and a series of meetings, this joint and coordinated action has been shown to the public with far-reaching progress. The EU has built up ways to identify and counter disinformation via the Strategic Communication Task forces and the EU Hybrid Fusion Cell in the European External Action Service. Furthermore, the exchange of information between member states and the EU institutions has been much timely and practical by the newly set up system called Rapid Alert System. Governments have put much effort into addressing the issue of corruption within political communications and manipulated information by working with online platform industries. Lastly, the Commission was successful in stimulating international institutions and organizations to face the consequential matters of disinformation on a global scale, and be more engaged in increasing the awareness and resilience to fake news.

Key Players

**Moldova**

Among European nations, Moldova appeared to have the lowest level of disinformation resilience. The vulnerability of Moldovans against misleading news was shown to be relatively high compared to other European countries by a larger population exposure to fake news, and the poor quality of systemic responses. The government has repeatedly emphasized their progress toward the fight against propaganda, however, it will need to come up with clear policy measures to properly address the problem. Its previous decisions in solving the lack of political will to supplement the requirements of the ‘Broadcasting Code’ has allowed Russian control over its media market. Russian control has even manipulated citizens’ opinions about national governance. Furthermore, the Moldovan government is having a dilemma due to the fact that its implementation of more active policies might go against the freedom of the press.

**Europol**

Europol, the European Union Agency for Law Enforcement Cooperation or formerly known as the European Police Office and Europol Drugs Unit, is the law enforcement agency of the European Union. It was formed in order to handle criminal intelligence via cooperation between all authorities of EU member states. This agency has greatly contributed to strengthening the cybersecurity of European nations against the spread of disinformation followed by cyber attacks. The EU protocol received pledges
alliance from every member state because of Europol. It has succeeded in raising global awareness to the issue of fake news and poor cybersecurity, and has devised new measures to combat cyber crimes throughout the continent.

**Possible Solutions**

*Law enforcement*

The methods hackers utilize to approach innocent individuals with the danger of cyber attacks which vary widely are increasingly sophisticated, while national cybersecurity has not made any step forward. The root cause of the increase in fake news with a higher likelihood of cyber attacks is the existing groups of online intruders. Hence, strengthening cybersecurity policies and enforcing punishments on those hackers will be effective in reducing the number of victims of such crimes. For instance, governments can raise awareness of media policies such as "The law on the press" in order to cover the dissemination of fake news. Governments can also cooperate with other law enforcement agencies to enhance cyber detection.

*Security testing for companies*

Another common target of cyber attack is small businesses and organizations that are not aware of their risk to serious cyber attacks. Despite the rising trend of such companies and organizations that are harmed by unauthorized access to their data, 41 percent of their sensitive information is known to be protected with poor cybersecurity. In addition, 65 percent of such organizations are not aware of the extreme risk of clicking suspicious emails and advertisements. Thus, it is essential for those
companies and organizations to regularly go through security testing and fix flaws beforehand in order to prevent the loss of confidential information supported by governmental funding.

**Glossary**

**Disinformation**
False information spread deliberately to deceive / deliberately misleading or biased information; manipulated narrative or facts; propaganda.

**Fake news**
False stories that appear to be news, spread on the internet or using other media, usually created to influence political views or as a joke, also known as junk news or pseudo-news.

**Phishing**
The fraudulent practice of sending emails purporting to be from reputable companies in order to induce individuals to reveal personal information, such as passwords and credit card numbers.

**Malware**
Software that is specifically designed to disrupt, damage, or gain unauthorized access to a computer system.

**Cyber attack**
An attempt by hackers to damage or destroy a computer network or system / an illegal attempt to harm someone’s computer system or the information in it, using the internet.
Sources


