INTERNATIONAL JOURNAL OF LAW MANAGEMENT & HUMANITIES

[ISSN 2581-5369]

Volume 4 | Issue 5

2021

Pegasus and its Effects in International Realm

JAI KHURANA[1]

ABSTRACT

There has been evidence of Cyber-attacks from the beginning of the Digital World. Attacks and Cyber-security have grown in their impact and capability at an alarming level respectively. Cyber realm had a tremendous breakthrough in July 2021 when Pegasus Spyware was introduced by the NSO Group, Israel to the world.

Pegasus can have major effects on each and every industry in the world. International Grounds may see major changes depending upon the intentions for usage of the said software. The impact can be boon or bane in the areas ranging from National Security to Human Rights. Trade also may fluctuate depending on the opportunities and threats each country face on hard, soft and structural powers. Major concern arises on the topic of how countries react on facing the said attack on an International level.

There have been speculations on how the spyware can benefit on areas regarding Human Rights. Major opinion states the potential damage Pegasus can cause is tremendous and it needs to be controlled otherwise, it can lead to great chaos.

Keywords: *Pegasus, Cyber Crime, International Relations, Technology, Effects*

I. INTRODUCTION

A smartphone's sole purpose is to provide the owner with the leisure of messaging, connecting, browsing the internet, mobile payments, and e-commerce with peace of security. Every owner's privacy is tried to be kept intact be it a millionaire or a terrorist. Before that a question arises, can it be possible that each digital move can be tracked? Why is there a need for such software in the world? Currently, we are living in a world of gadgets and devices. Let's imagine a situation where every device provides transparent security! All the activities of each human being, people with national or anti-national sentiments can be tracked. Also, functions could be performed from the devices without the owner's knowledge.

Now another question arises, are all Spywares bad? Spywares can be fatal! Agreed, but if they are used effectively, then they can lead to a peaceful and harmonious world.

[1] Author is a student at Vivekananda Institute of Professional Studies, New Delhi, India.

 [ISSN 2581-5369]

Pegasus is built by the NSO Group, an Israeli company in the year 2010 with bonafide intentions to provide it to intelligence agencies to control crime and terrorism.

Pegasus being zero-click spyware can grant control to attackers more than the owner. It can steal everything the device is containing including passwords, contacts, messages, photos, etc. In other words, the attacker can access the phone equal to or greater than the owner. The spyware can function without human interaction as it was required before. A simple initiation from the attacker; be it in a way of a message or call is enough for Pegasus to access the device.

(A) Literature Review

Each International factor is viewed separately here due to difference in the impact each factor experiences due to the aforesaid spyware.

Spyware: Spyware peeks into individual's data and all individual's computer activity — whether authorized or not. However, many trusted computer services and applications use "spyware-like" tracking tools. As such, the spyware definition is reserved mostly for malicious applications nowadays. Malicious spyware is a type of malware specifically installed without individual's informed consent. Step-by-step, spyware will take the following actions on individual's computer or mobile device:

- Infiltrate — via an app install package, malicious website, or file attachment.
- Monitor and capture data — via keystrokes, screen captures, and other tracking codes.
- Send stolen data — to the spyware author, to be used directly or sold to other parties.

In short, spyware communicates personal, confidential information about individual to an attacker. The information gathered might be reported about individual's online browsing habits or purchases, but spyware code can also be modified to record more specific activities.

National Security: An ability of a nation to meet the needs necessary for its self-preservation, self-reproduction, and self-improvement with minimal risk of damage to the basic values of its current state. First, national security is not something that merely affects the well-being of Citizens. Rather, it involves their safety, their security, and their freedoms. It is becoming more commonplace to view perceived social "injustices" as national security problems, but this distorts the very concept. Perceptions of social injustice or inequality are domestic concerns, not national security matters. Making less money than a neighbor is hardly as important to one's life as being safe from incineration in a skyscraper in a terrorist attack.

Nuclear Proliferation: Specifically, the spread of nuclear weapons, and, more generally, the spread of nuclear technology and knowledge that might be put to military use. Increasingly,

the prospect of nuclear weapons in the hands of terrorist organizations, such as al-Qaeda, is creating concern. Nuclear proliferation is widely considered to be a problem because of the fear that it will increase the probability of nuclear weapons being used. Some argue that nuclear proliferation could enhance international security by spreading the paralysing effects of deterrence in regions that otherwise have a high probability of recurrent conventional war. Because of the close links between civil and military nuclear technology, many states are able to reduce the time necessary to acquire a nuclear weapon by acquiring a range of nuclear technologies for civil purposes. Several states have already achieved threshold status, in which they either have unannounced nuclear weapon capabilities, or could develop them extremely quickly if necessary.

Human Rights: Human rights are standards that recognize and protect the dignity of all human beings. Human rights govern how individual human beings live in society and with each other, as well as their relationship with the State and the obligations that the State have towards them. Human rights law obliges governments to do some things, and prevents them from doing others. Individuals also have responsibilities: in using their human rights, they must respect the rights of others. No government, group or individual person has the right to do anything that violates another's rights.

International Finance Relations: International finance is that branch of financial economics that deals with the monetary or the macroeconomic inter relations between two or more nation states. This field studies the relationships and dynamics that exist in the global financial systems or the international monetary system such as balance of payments, stock exchanges, exchange rates, foreign direct investment as well as international trade. Multi-national organizations hire the experts in international financial management to study the inter-play between the various elements of international finance and accordingly formulate strategies for international business for their organization. It is also referred to as multinational finance, international monetary economics or international macroeconomics.

International Trade Relations: Foreign trade is exchange of capital, goods, and services across international borders or territories. In most countries, it represents a significant share of gross domestic product (GDP). While international trade has been present throughout much of history, its economic, social, and political importance has been on the rise in recent centuries. All countries need goods and services to satisfy wants of their people. Production of goods and services requires resources. Every country has only limited resources. No country can produce all the goods and services that it requires. It has to buy from other countries what it cannot produce or can produce less than its requirements. Similarly, it sells to other countries the goods

 [ISSN 2581-5369]

which it has in surplus quantities. India too, buys from and sells to other countries various types of goods and services.

(B) Significance of Study

The study of International Relations and its effect in the International Realm can be a learning paradigm in the Technological, Financial and International Institutions to enhance the knowledge on the matter of Pegasus. The project's goal is designed to help even general public on areas of effect of the Spyware. Students may also improve academic competence, develop employability skills, implement a career plan and participate in a career pathway in preparation for growing areas of technology.

(C) Hypothesis

- Do Countries have jurisdiction to try and give orders pertaining to Pegasus in their Hon'ble Courts?
- What are the potential effects of Pegasus on the International Relations?

(D) Research Methodology

The Researcher has followed primary as well as secondary data collection. This research is doctrinal. The researcher has also utilized articles, notes, and other writings to incorporate the various views to present a holistic view.

II. LEGAL GROUNDS HOVER OVER PEGASUS

Pegasus even after being used with bonafide intentions, still needs to stand in front of the legal light. Certain cases go too far and need a proper watch. Even if you have the best of intentions on spying on someone, you may have to face the legalities of the matter.

(A) Which Country's Court May Exercise Jurisdiction Over the Matters Of Pegasus?

Default principles of private International Law or conflict of interest will require courts to look at various factors, such as countries where the parties are based, the country where the subject matter is situated, the country in which the performance is required, etc.

This problem can be avoided by specifying the specific system of laws in matters of dispute for the interpretation of contracts. Apart from Google and Microsoft which have physical offices in multiple countries, it is very difficult for businesses to be sued in every other corner of the world. Thus, it must look forward to restricting legal proceedings to a specific country. This helps companies or tech giants to manage all the legal matters in a very specific way for matters which include them all over the world.

 [ISSN 2581-5369]

In the case of NSO Group, companies terms and conditions explicitly state all the matters in regards to the company be dealt with in Tel Aviv, Israel, until it is mutually agreed upon by both the parties.

(B) Effects of Pegasus in International Trade and Relations

Pegasus can make a major impact on the world, both positive and negative. Being at an international level, it may affect the international relations.

1. National Security

Online attacks like Pegasus have the potential to harm national security. All the information from politicians' phones can be tracked and could be accessed by technologists at NSO or even lead to worse outcomes if it is handled by a person with mala-fide intentions.

Economic institutions, medical pieces of equipment, or power infrastructures could be hacked as a way of stealing or extorting additional resources. It may also be used to advance an ideological agenda. The complex coordinated attack is a major threat as banking and financial systems are increasingly digitized and connected to the internet, thus their information can also be accessed via illicit means. There are also fears that illicitly acquired information could be publicized. Major chaos can also happen throughout metropolitan areas due to fear among people and them withdrawing their every resource connected with the internet including banking and e-commerce thus even affecting the economy.

2. Nuclear Proliferation

The potentially most hazardous way to escalate nuclear proliferation would emerge from the early utilization of digital weapons (here Pegasus) in an extraordinary force emergency to paralyze the vital command, control, and communications capabilities of a nation, large numbers of which serve nuclear powers. In the "confusion of international conflict" that would normally result from such an experience, the beneficiary of such an assault may fear more follow-up dynamic assaults, perhaps including the utilization of nuclear weapons, and, dreading the deficiency of its armory, dispatch its weapons right away. This may happen, for instance, in a conflict between NATO and Russian powers in the east and focal Europe or between the U.S. also, Chinese powers in the Asia-Pacific locale.

The vulnerability of nuclear weapons being hacked has given countries the incentive to build more powerful nuclear weapons. Pegasus has the potential to disarm the country from its weapons. Simultaneously, attention to the danger of a Pegasus attack boosts the need to build

 [ISSN 2581-5369]

the assurance of nuclear powers related organizations from demonstrations of unlawful obstruction, paying little heed to their source, which adds to keeping up with security.

Policies of different countries in respect to cyber-attacks and nuclear relations

- US: US Nuclear doctrine which was developed under the Trump Administration gives the president the option to revert to attack by nuclear weapons. The policy expanded the grounds of use of nuclear weapons in the times of "significant non-nuclear strategic attacks," including "attacks on the U.S., allied, or partner civilian population or infrastructure." This may include cyber-attacks on the U.S.[2]

- China: Due to China's No First Use Policy maintained by Beijing, the link between cyber threats and nuclear use in public Chinese documents is quite challenging. Nevertheless, China has given statements comparing the consequences of cyber attacks to be equivalent to nuclear bombs[3]. Research on the entanglement between non-nuclear and nuclear weapons-related systems suggests that China is still considering strict policies and grounds over the 'cyber issues'.

- France: French "fundamental heed" that are protected by nuclear weapons are intentionally ambiguous and not exhaustive, but Paris pays great attention to the cyber domain. Principles of the Paris Call for Trust and Security in Cyberspace state the link between nuclear threats and cyber threats.[4]

- UK: UK officials acknowledge the threat to NC3 and nuclear weapons systems; nothing suggests that such attacks might be considered among "the most extreme threats" to be responded with nuclear weapons. However, London, without any doubt, will be interested in reducing the risks of nuclear use as a result of cyber interference.

On the other hand, cyber-attacks like Pegasus can make countries reconsider their nuclear policies as having more bombs can make a country more prone to getting targeted for cyber-attacks and can ultimately lead to the country's loss.

3. Human Rights

For a long time, Amnesty International has cautioned of the threats to human rights presented by the surveillance industry for the most part, and the particular instances of unlawful

[2]*Nuclear Posture Review*, US DEPT OF DEFENCE (Feb 2, 2018), https://media.defense.gov/2018/Feb/02/2001872886/-1/-1/1/2018-NUCLEAR-POSTURE-REVIEW-FINAL-REPORT.PDF

[3] Ander Browne, *China: Cyberattacks Are Like Nuclear Bombs*, WALL STREET JOURNAL (Apr 22, 2013, 10:48 P.M. ET), https://www.wsj.com/articles/SB10001424127887323551004578438842382520654.

[4]*The 9 principles*, PARISCALL (Dec 11, 2018), https://pariscall.international/en/principles

designated observations worked with by NSO Group explicitly.

States have restricting commitments under international human rights law to shield human rights from maltreatment by outsiders, including privately owned businesses that work outside their boundaries.

As per international lawful guidelines, an organization might be complicit in human rights infringement if it meets two fundamental standards: that through its business exercises it helped in the commission of the infringement and that the organization knew or ought to have realized that its demonstrations would help in advancing the infringement.

Companies like NSO Group have violated the norms of Human rights with impunity and still selling the Pegasus software for profits. States worldwide have allowed NSO's software to flourish without even considering the amount of loss human rights may face.

4. International Organizations

The discussion of security and peace (supra) mentions the threats a country can face in soft, hard and technological factors. In such a scenario, International Organizations also get affected and have to manage foreign aid for the country in dire need of the very same.

In addition to, out of many other functions, International Organizations also need to settle disputes which may arise at International levels. An act of trans-national crime like Pegasus may disrupt peace between two countries and can cause frustrated relations. Recent concerns between America and Russia[5] may provide an idea of what all can happen due to cyber-attacks.

International organizations like United Nations Organizations (UNO) and European Union (EU) are some of the organizations that condemn the act of Pegasus software. UN High Commissioner Michelle Bachelet's statement[6] clearly stated the disagreement from the UN in regards to Pegasus being used to spy on other beings in the name of surveillance for national security. European Commission president Ursula von der Leyen shared the same opinion by mentioning the importance of free press and freedom of speech.[7]

[5] David Sanger, Nicole Perlorth, *US aid agency system used to carry out cyberattacks by Russia: Microsoft*, BUSINESS STANDARD (May 29, 2021, 01:19 IST), https://www.business-standard.com/article/international/us-aid-agency-system-used-to-carry-out-cyberattacks-by-russia-121052800365_1.html

[6] Snigdha Choudhary, *Pegasus row: United Nations to European Union, here is how the world reacted*, INDIATODAY (Jul 23, 2021, 14:19 IST), https://www.indiatoday.in/world/story/pegasus-row-united-nations-european-union-amnesty-how-world-reacted-1831705-2021-07-23

[7] *Ibid* (www.indiatoday.in)

 [ISSN 2581-5369]

5. Globalization

With increasing connectedness and interdependence of world cultures and economies, globalization, in the long run, has led to a rise in cyber-crime including both a new range of criminal forms such as data theft and web-based scams and the reinvigoration of many traditional types of crime; identity theft, money laundering, and tax evasion, etc.

Due to the activities of NSO Group, Israel might get an advantage in the face of globalization as it may sell Pegasus to more than half a world until stopped by Israel's policies. The technology is in demand and is asked for by both developed and developing nations.

However, other commodities might not be brought up into the International market as before as the countries are still dealing with the greater issue of Corona-Virus. The private sector may even share the same opinion for avoiding the spotlight to prevent their classified information to be shared with technologists or the Government of the state.

6. Economic Development

Economic development takes a great negative toll due to normal cyber-attacks; Spyware like Pegasus can even lead to more harm. Any entity targeted by the spyware can lead to loss of reputation and authenticity. Chances are Intellectual Property of an organization like a patent can also be tracked down and misused.

Valuable data of sensitive business information can also be compromised and loss of such data harms the organization as it can be used by the competitors. Businesses can also get disrupted and loss of sales could also happen as businesses won't be willing to give full services in the fear of their data being stolen and in such scenarios, customers cannot get the services thus leading to loss to the organization in a very short period. Also, there is an imminent danger of loss of equipment and fluctuation in stock prices.

7. International Financial Relations

In April 2020, the Financial Stability Board (FSB) warned that "a major cyber incident, if not properly contained, could seriously disrupt financial systems, including critical financial infrastructure, leading to broader financial stability implications."[8] Due to unprecedented digital transformation due to the COVID-19 pandemic, every minor and major work has been transformed and shifted to online services. Banks have also thrown the weight behind digital currencies and modernizing payment systems.

[8]*Effective practices for Cyber incident and response recovery,* FSB (Oct19, 2020), https://www.fsb.org/2020/10/effective-practices-for-cyber-incident-response-and-recovery-final-report/

 [ISSN 2581-5369]

In such situations, Pegasus can derail innovations and undermine trust when all over the world's economy has taken a major hit. Financial Markets all over the globe can also face losses as companies may not be able to perform at their very best.

8. International Trade Relations

International Trade Relations may see a rise in the Pegasus era. With the World Bank's forecast of the recession of the world GDP by 5.2% in the pandemic in 2020[9]; countries were/ are more focused on the bigger fish than Pegasus. In such situations, developing countries might take help from the developed countries and international institutions for resources to research and find the solution to the threat of spyware and further strengthen their cybersecurity. If any of the countries could be able to find a solution to the problem then the same would be used worldwide; again rising International Financial Relations.

(C) What Can Be Done?

- Unanimous Implementation of defensive technologies and basic security measures should be done as soon as possible. This responsibility majorly lies on companies and consumers.
- Need for an increased International Law enforcement cooperation. This includes both nation's law enforcement agencies and private sector
- The Government of the country which released Pegasus spyware i.e. Israel must come under pressure from the international community to change their export policies restricting NSO Group to sell worldwide until all the basic laws and regulations are settled.
- Without dedicated action, the global financial system will only become more vulnerable as innovation, competition, and the pandemic further fuel the digital revolution. The financial system does not lack funds or the ability to execute technical issues, it only needs to organize the system's protection across governments, financial authorities, and industries and leverage the resources effectively.
- There is no uniform system to deal with matters like Pegasus spyware. Each country has its regulations that clash in the international purview ultimately weakening International

[9] *COVID-19 to Plunge Global Economy into Worst Recession since World War II*, WORLD BANK (Jun 8, 2020), https://www.worldbank.org/en/news/press-release/2020/06/08/covid-19-to-plunge-global-economy-into-worst-recession-since-world-war-ii

 [ISSN 2581-5369]

law. Thus, there should be understanding and clarity among countries about roles and responsibilities.

- Countries do need to work and collaborate. Pegasus has a great potential to harm humanity all over the world thus contributed effort can lead to better outcomes.
- More people should be trained in the cyber domain to tackle such issues. People who may have lost jobs or earning members of their family can enjoy preference under the same.

III. CONCLUSION

Pegasus can act revolutionary in both positive and negative aspects. If it is used under the guidelines issued and followed under international law, then it can curb major criminal threats over the world. On the other side, if the necessary is not taken into control then the situation can escalate and worsen up quickly.

Laws in the area of international cybercrime still need major amendments and regulations. Firstly, as major cyber-attack sources or targets are democratic countries; democratic countries should strengthen their laws, restricting people from misuse technology as they wish. Secondly, a multi-lateral initiative to impose strengthened controls with transparent human rights assessments on items with surveillance capabilities must be reached as soon as possible.

*****

 [ISSN 2581-5369]

IV. REFERENCES

- *Nuclear Posture Review*, US DEPT OF DEFENCE (Feb 2, 2018), https://media.defense.gov/2018/Feb/02/2001872886/-1/-1/1/2018-NUCLEAR-POSTURE-REVIEW-FINAL-REPORT.PDF
- Ander Browne, *China: Cyberattacks Are Like Nuclear Bombs*, WALL STREET JOURNAL (Apr 22, 2013, 10:48 P.M. ET), https://www.wsj.com/articles/SB10001424127887323551004578438842382520654.
- *The 9 principles*, PARISCALL (Dec 11, 2018), https://pariscall.international/en/principles
- David Sanger, Nicole Perlorth, *US aid agency system used to carry out cyberattacks by Russia: Microsoft*, BUSINESS STANDARD (May 29, 2021, 01:19 IST), https://www.business-standard.com/article/international/us-aid-agency-system-used-to-carry-out-cyberattacks-by-russia-121052800365_1.html
- Snigdha Choudhary, *Pegasus row: United Nations to European Union, here is how the world reacted,* INDIATODAY (Jul 23, 2021, 14:19 IST), https://www.indiatoday.in/world/story/pegasus-row-united-nations-european-union-amnesty-how-world-reacted-1831705-2021-07-23
- *Effective practices for Cyber incident and response recovery,* FSB (Oct19, 2020), https://www.fsb.org/2020/10/effective-practices-for-cyber-incident-response-and-recovery-final-report/
- *COVID-19 to Plunge Global Economy into Worst Recession since World War II*, WORLD BANK (Jun 8, 2020), https://www.worldbank.org/en/news/press-release/2020/06/08/covid-19-to-plunge-global-economy-into-worst-recession-since-world-war-ii

*****

 [ISSN 2581-5369]