Implications of the WannnaCry Ransomware Attack on Personal Security: Analysis of Human Security Concepts

Nasywa Tsabita Amelia
Universitas Darussalam Gontor
nasywatsabitaamelia57@student.hi.unida.gontor.ac.id

ABSTRACT

The 2017 WannaCry ransomware assault exposed fundamental flaws in increasingly complicated cybersecurity that harm individuals and organizations worldwide. The impact and losses caused by this incident are highly distressing. The hack locked data on unprotected systems, demanded a Bitcoin ransom, and caused financial losses and disruptions to critical services like as health care. Indonesia, as the afflicted country, is among those working together to solve this problem. This article will examine the implications of a WannaCry assault on personal security by studying the idea of human security. Using the framework of the human security concept, this article seeks to investigate how the attack affects persons' well-being and emphasizes the significance of proactive and collaborative cybersecurity measures. This ransomware attack is believed to have been carried out by a group of hackers called Lazaras Group who are purportedly associated with North Korea. The findings emphasize the importance of regular system updates, backups, and strong security policies in keeping with current and future advances to ensure personal security in the digital era.

Keywords: *Human Security Concept; Personal Security; WannaCry Ransomware.*

INTRODUCTION

Globalization is an indication of the world's rapid development and the start of the digitization era in many facets of human life. Through gadgets, information can be easily conveyed and spread to the public. As a result of this process, digitization has emerged, bringing forth different breakthroughs in communication technology, computer networks, and the internet (Fauziyah et al., 2022). From all this practicity and convenience, there are consequences that users must inevitably bear. User data and information are required to support communication and verification processes during usage. Although privacy security systems are in place, it is not uncommon for undesirable incidents to occur, such as the leakage of users' personal data, which is then misused by irresponsible parties.

In May 2017, the world was shocked by the WannaCry ransomware attack, which spread rapidly and infected over 300,000 computers in more than 150 countries (Cloudflare, 2017). WannaCry is a type of malware that encrypts data on infected computers and demands a ransom payment in Bitcoin to restore access to that data. This attack exploits a vulnerability in the Windows operating system, known as EternalBlue, which was previously discovered by the United States National Security Agency (NSA) and later leaked to the public by the hacker group Shadow Brokers (Informatika, 2023). In addition to causing enormous financial losses, the WannaCry attack interrupted major global

enterprises, transportation, and healthcare systems. For instance, due to an unreliable computer system, the National Health Service (NHS) in England was compelled to postpone surgeries and medical appointments. This incident highlights how susceptible people and organizations are to pervasive and sophisticated cyberthreats (Hern, 2017).

This article aims to explore the impact of the WannaCry attack on personal security through the lens of human security. Human security includes various dimensions, such as economic, health, and personal security. Analyzing this attack within the human security framework allows for a more nuanced understanding of how cyber threats impact individual well-being and underscores the necessity for comprehensive and collaborative cybersecurity strategies. Personal security, as a critical aspect of human security, involves safeguarding individuals from physical and psychological threats. In the context of the WannaCry attack, personal security is compromised through potential data loss, disruptions to essential healthcare services, and financial losses incurred by individuals and organizations. This analysis will help identify steps that can be taken to enhance protection against future cyberattacks and ensure that personal security is maintained in this increasingly interconnected digital era.

METHODS

This study utilizes a qualitative research methodology, with a descriptive analytical approach at the explanatory level. In examining the selected research topic on the WannaCry malware attack, the researcher offers a more thoroughly descriptive explanation (Rusandi & Rusli, 2014). In conducting this study, the author utilizes reading proficiency to gather information from diverse sources related to the topic. By employing a literature review or library research method, the author identifies relevant scholarly works and studies that serve as references from prior research. These sources include books, academic journals, official reports, articles, news, and other pertinent studies. John W. Creswell defines qualitative research as an approach that seeks to explore and comprehend the meanings that people assign to social and human issues (Murdiyanto, 2020). This qualitative research follows a procedure that involves collecting specific data to obtain more accurate results.

RESULT AND DISCUSSION

Human Security Concept

Security is a fundamental necessity for every individual worldwide, driving the continuous pursuit to attain it. Within the realm of international relations, the concept of security has experienced substantial changes. This is not only because it relates to a fundamental aspect of human existence but also due to the evolving nature of interactions among individuals (Perwita, 2008). The urgency of security became prominent when the world faced conflicts and wars that threatened human safety. Traditionally, the concept of security was limited to the state and its military power, primarily focused on self-defense. However, this notion has evolved alongside the advancement of modern security studies, now recognized under the framework of non-

traditional security (NTS) (Trihartono et al., 2020). Issues and actors within Non-Traditional Security (NTS) are not limited to states alone, they increasingly involve non-state actors, particularly communities, both as groups and as individuals.

The development of security studies has led to the emergence of several new concepts, one of which is human security. The concept of human security was formally introduced by the United Nations Development Program (UNDP) in its *Human Development Report 1994*. However, similar ideas were presented years earlier by academics participating in the World Order Models Project (WOMP) and the Club of Rome during the 1960s and 1970s. These gatherings were organized to discuss global issues, one of which focused on individual safety, security, and well-being. The Canadian government also adopted the concept of human security and incorporated it as a foreign policy priority, leading to the establishment of the Human Security Network to promote a shared coalition (Kusuma, 2022).

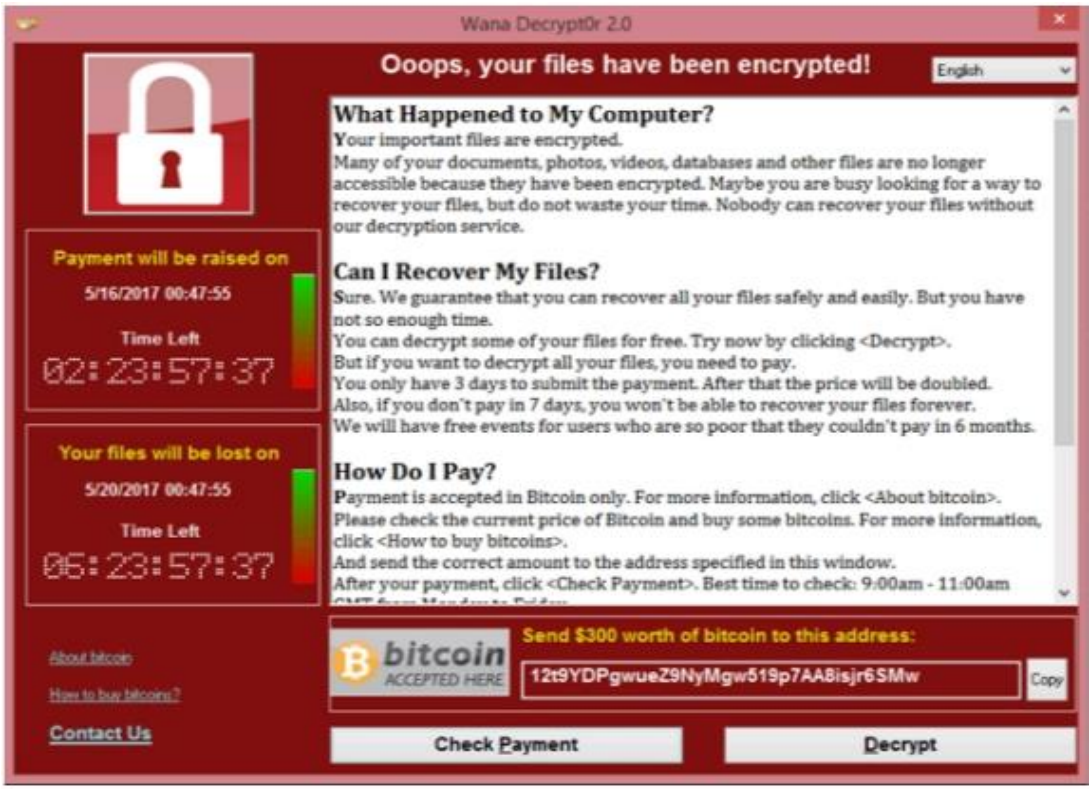
The UNDP, in its report, describes the concept of human security as 'freedom from fear', 'freedom from want', and 'freedom to live in dignity'. This concept covers several aspects, including economic security, food security, health security, environmental security, personal security, community security, and political security. According to the report, human security involves *"first, safety from chronic threats such as hunger, disease, and repression. And, second, ... protection from sudden and hurtful disruptions in the patterns of daily life, whether in homes, in jobs, or in communities."* (UNDP, 1994). According to the Commission on Human Security, human security is defined as *"safety for people from both violent and non-violent threats. It is a condition or state of being characterized by freedom from pervasive threats to people's rights, their safety, or even their lives".* Both explanations conclude that individuals must be in a safe environment where they are free from hunger, malnutrition, disease, and repression. Furthermore, people must be protected from unexpected disruptions or turmoil that could endanger their well-being in everyday life, whether at home, at work, or within their community (Mumtazinur & Wahyuni, 2021).

In her work, Sharbanou defines security in a clear and straightforward manner as the *'absence of insecurity and threats'*, security is achieved when an individual is free from anxiety and any circumstances that could lead them to feel threatened. The notion of freedom from anxiety pertains to a condition where there is no fear—whether it is physical, psychological, or emotional. This concept of human security began to emerge and gain relevance in the post-Cold War era. The global dynamics underwent considerable changes after the Cold War. New actors, such as international organizations, investment corporations, and NGOs, are increasingly playing pivotal roles in international relations. Even though the risk of major global conflicts has lessened, new threats have emerged, including internal conflicts, terrorism, extreme poverty, and diseases like HIV/AIDS. These threats are transboundary and interconnected, with far-reaching impacts on societies worldwide. This concept stems from many case studies demonstrating that states often serve as sources of insecurity for their citizens. Not only do they fail to safeguard their citizens, but they sometimes even endanger their lives.

Concurrently, the world has observed numerous instances of international interventions in Bosnia, Kosovo, East Timor, and Afghanistan. While the conflicts in these locations appear to be resolved, the underlying issues have not been sufficiently addressed through long-term rehabilitation and peacebuilding measures (Tadjbakhsh, 2005).

WannaCry Ransomware Attack Chronology

Ransomware is a type of malware that employs cryptographic techniques to hijack files and user data, demanding a ransom in cryptocurrency for their release. As a subset of malicious software, malware is intended to gather and exploit personal information. It works by obstructing system processes and encrypting data, thereby compromising its security. WannaCry is identified as 'crypto-ransomware,' which targets file systems to encrypt user data and demands Bitcoin for decryption (Mubarak et al., 2024). The WannaCry ransomware, also known as Wanna Decryptor, locks all files on the affected computer system, leaving the victim with only two files, one with instructions for payment and the other being the Wanna Decryptor itself. Consequently, the victim is left with few options but to comply with the attacker's demands by paying the ransom or risking the permanent loss of their data due to the virus (Ramadhan, 2023).



(Source: https://tif.uad.ac.id/yuk-mengenal-ransomware-wannacry/)

On May 12, 2017, the WannaCry ransomware attack was launched indiscriminately, affecting tens of thousands of computers worldwide (Eraspace, 2023). Specifically, 75 thousand computers spread across 99 countries were affected by this attack (BBC, 2017). Additionally, 200,000 organizations in 150 countries were also impacted. The estimated financial damage caused by the WannaCry ransomware attack is around 53

trillion rupiah (Cloudflare, 2017; Simbolon, 2021). At the same time, Spain, the United Kingdom, France, Germany, and Indonesia are affected. Specifically, the attack impacted two hospitals, Rumah Sakit Harapan Kita and Rumah Sakit Dharmais (Kartopati, 2017). In subsequent days, Russia and Turkey also suffered from the attack. WannaCry exploited vulnerabilities in the Server Message Block (SMB) protocol in the Windows operating system, known as EternalBlue. The vulnerability primarily affected Windows users who had not updated their operating systems since April 2017. The attack affected 0.1% of Windows XP users and 98% of Windows 7 users (Informatika, 2023).

The EternalBlue exploit system was originally developed by the United States National Security Agency (NSA), but it was subsequently leaked to the public by the hacking group known as the Shadow Brokers (Tribune, 2024). On May 14, 2017, Marcus Hutchins, a cybersecurity researcher, discovered a kill switch for the ransomware. This kill switch involved a domain that, when registered, could stop the ransomware's propagation. Follow-up investigations indicated that a hacker group called the Lazarus Group, associated with North Korea, was probably responsible for the attacks. In 2018, the U.S. Department of Justice indicted two North Korean individuals for their participation in the attacks.

The Budapest Convention on Cybercrime

The Budapest Convention on Cybercrime 2001 represents the first international treaty established by the United Nations to address cybercrime and the digital realm. The convention aims to: 1) Harmonizing national laws, where the convention provides a framework for countries to align their legislation on cybercrime, thus creating a consistent legal basis for addressing cyberattacks; 2) Advancing investigative techniques by encouraging the development and application of cutting-edge methods to detect and prosecute cybercriminals; and 3) Strengthening international cooperation, particularly concerning attacks involving multiple countries, to identify attack patterns and expedite prevention efforts. The convention also includes guidelines for the collection and preservation of electronic evidence for judicial use. Sponsored by the Council of Europe on November 23, 2001, it became effective on July 1, 2004 (Agung et al., 2022).

This convention offers a framework for countries to standardize the enforcement of laws related to cybercrime and legislative measures, and has been endorsed by more than 70 nations globally. It encompasses various classifications of offenses within its scope (Fadhillah et al., 2023):

1. Violations of confidentiality, integrity, availability of data, and computer systems. This includes violations such as unauthorized access, eavesdropping, data disruption, system interference, and misuse of technology.
2. Computer-related violations. Refers to the production, distribution, and ownership of computer tools intended for illicit purposes.
3. Violations concerning copyright and related rights. This involves illegal technological circumvention and online piracy.

4. Content-specific violations are restricted to offenses related to child pornography.
5. Additional Responsibilities and Sanctions. This includes the responsibility of companies for violations committed on behalf of a corporate entity.

According to Articles 2 through 6 of the Budapest Convention, which pertain to the measures that should be implemented at the national level, states have the authority to respond to incidents related to the WannaCry cyberattack, as this incident falls under violations of these specific articles (Convention on Cybercrime, 2001). This is where the Budapest Convention plays a crucial role. The WannaCry attack, which did not target a single country but rather multiple nations globally, necessitates coordination for resolving the issue and prosecuting the perpetrators. The subsequent coordination led to the discovery that the ransomware attack was orchestrated by a group of hackers known as the Lazarus Group, suspected to be based in North Korea. It was previously known that the Lazarus Group was also behind the hacking attack on Sony Pictures at the end of 2014 (Uchull, 2017).

The WannaCry Attack's Effect on Personal Security

The WannaCry ransomware attack has shown to negatively affect personal security. There is little to gain from this ransomware attack, except for the financial profits the perpetrators obtain through ransom payments or the potential exposure of victims' personal data to anyone for any purpose. Furthermore, the damage inflicted on victims generally manifests as financial losses that must be borne by each individual. The personal data and information of the victims are no longer under the original owners' privacy rights but rather become a liability that could threaten their safety and well-being. Apart from the substantial ransoms required for the return of personal information, victims must also prepare for the potential consequences if such data and information are misused.

In the case of several hospitals impacted by these attacks, all data concerning their patients became inaccessible, leading to an inability to provide appropriate and timely medical care. This situation even caused scheduled surgeries to be postponed. Consequently, patients not only lost their right to adequate and appropriate treatment but also faced potential dangers to their safety if not promptly addressed and treated. According to the notion that security implies freedom from fear or harm, these ransomware attacks evidently place these patients in a state of insecurity, where their personal security is significantly compromised.

CONCLUSION

It is undeniable that digitalization drives individuals to keep pace with its advancements. Nevertheless, caution and vigilance are necessary in every aspect of its use. Apart from the risk of personal data breaches, other personal security concerns, such as stalking, have become increasingly common through digital intermediaries and social media. The

worst-case scenarios involving the misuse of personal data represent a significant threat for those who decide to engage in the digital realm. The WannaCry ransomware incident serves as a reminder that navigating cyberspace requires more than mere willingness; it also necessitates proper education and heightened cyber awareness. Additionally, preventive measures, such as cybersecurity regulations, are essential to safeguard users from potential cyber threats in this digital age.

REFERENCES

Agung, A., Hafrida, & Erwin. (2022). Pencegahan Kejahatan Terhadap Cybercrime. *PAMPAS : Journal Of Criminal*, *3*(2), 212–222.

BBC. (2017). *Massive ransomware infection hits computers in 99 countries*. BBC News. https://www.bbc.com/news/technology-39901382

Cloudflare. (2017). *What was the WannaCry ransomware attack?* Cloudflare. https://www.cloudflare.com/learning/security/ransomware/wannacry ransomware/

Convention on Cybercrime, 25 (2001).

Eraspace. (2023). *Ransomware Wannacry , Cyber Attack yang Gemparkan Dunia di 2017*. Eraspace. https://eraspace.com/artikel/post/ransomware-wannacry-cyber-attack-yang-gemparkan-dunia-di-2017 5/7

Fadhillah, S. A., Matakupan, M. S. A., & Mingga, B. W. B. (2023). Peran Interpol dalam Penyelesaian Kasus Kejahatan Siber Berdasarkan Konvensi Budapest On Cybercrimes. *Journal on Education*, *05*(04), 16553–16564. http://jonedu.org/index.php/joe

Fauziyah, N., Ramadhini, A., Wardhana, K. E., & Hudayat, A. F. S. (2022). Penggunaan Aplikasi Tiktok Sebagai Media Pembelajaran Untuk Meningkatkan Minat Belajar Peserta Didik di Era Globalisasi Digital. *Jurnal Tarbiyah & Ilmu Keguruan (JTIK) Borneo*, *3*(3), 181–193.

Hern, A. (2017). *NHS could have avoided WannaCry hack with ' basic IT security ', says report*. The Guardian. https://www.theguardian.com/technology/2017/oct/27/nhs-could-have-avoided-wannacry-hack-basic-it-security-national-audit-office

Informatika, P. S. (2023). *Yuk Mengenal Ransomware Wannacry*. Universitas Ahmad Dahlan. https://tif.uad.ac.id/yuk-mengenal-ransomware-wannacry/

Kartopati, L. (2017). *Mengenal WannaCry , Ransomware yang Serang Dunia*. CNN Indonesia. https://www.cnnindonesia.com/teknologi/20170513185820-192-214636/mengenal-wannacry-ransomware-yang-serang-dunia

Kusuma, A. S. (2022). *HUMAN SECURITY DALAM HUBUNGAN INTERNASIONAL : SEBUAH PENGANTAR* (Issue March).

Mubarak, A. S., Insirat, M. N., & Lutfiya, M. N. (2024). Ransomware: Evolution, Classification, Attack Phase, Detection and Prevention. *SNESTIK: Seminar Nasional Teknik Elektro, Sistem Informasi, Dan Teknik Informatika*, 1–6. https://doi.org/10.31284/p.snestik.2024.5588

Mumtazinur, & Wahyuni, Y. S. (2021). Keamanan Individu (Personal Security) dan Qanun Hukum Keluarga: Tinjauan Konsep Keamanan Manusia (Human Security). *El-Usrah:*

Jurnal Hukum Keluarga, *4*(1), 76–89.

Murdiyanto, E. (2020). *Metode penelitian kualitatif* (1st ed.). Lembaga Penelitian dan Pengabdian Pada Masyarakat UPN "Veteran" Yogyakarta Press.

Perwita, A. A. B. (2008). *DINAMIKA KEAMANAN DALAM HUBUNGAN INTERNASIONAL DAN IMPLIKASINYA BAG I INDONESIA*. UNIVERSITAS KATOLIK PARAHYANGAN JI.

Ramadhan, G. (2023). Perlidungan Hukum Bagi Korban Ransomware Wannacry Tindak Pidana Ransomware. *Das Sollen: Jurnal Kajian Kontemporer Hukum Dan Masyarakat*, *1*(2), 1–17. https://doi.org/10.11111/dassollen.xxxxxxx

Rusandi, & Rusli, M. (2014). Merancang Penelitian Kualitatif Dasar / Deskriptif dan Studi Kasus. *Jurnal Studi Makassar*, 1–13. http://jurnal.staiddimakassar.ac.id/index.php/aujpsi

Simbolon, R. S. (2021). *WANNACRY : CYBER TERRORIST*. KSM Defensia UPN Veteran Yogyakarta. https://ksmdefensiaupnvy.wixsite.com/home/post/wannacry-cyber-terrorist

Tadjbakhsh, S. (2005). Human Security: Concepts and Implications with an Application to Post-Intervention Challenges in Afghanistan. *Les Étudesdu CERI*, *117–118*, 1–331. https://doi.org/10.1177/0094306117744805l

Tribune, T. E. (2024). *Shadow Brokers threaten to release Windows 10 hacking tools*. The Express Tribune. https://tribune.com.pk/story/1423609/shadow-brokers-threaten-release-windows-10-hacking-tools/

Trihartono, A., Indriastuti, S., & Nisya, C. (2020). *Keamanan dan Sekuritisasi dalam Hubungan Internasional* (1st ed., Issue 8). Redaksi Melvana.

Uchull, J. (2017). *WH : Kim Jong Un behind massive WannaCry malware attack*. The Hill. https://thehill.com/policy/cybersecurity/365580-wh-kim-jong-un-ordered-release-of-disastrous-wannacry-malware/

UNDP. (1994). Human Development Report: New Dimension Of Human Security (1994). In *United Nations Development Programme 1994*. http://hdr.undp.org/sites/default/files/reports/255/hdr_1994_en_complete_nostats.pdf