NVEO
Natural Volatiles &
Essential Oils

Interrelation Between The Physical World And Cyber Space In The Context Of Unexpected Events: The Study Case Of Indonesia

Richardus Indrajit [1] , Lilly Wasitova[2] , Marsetio[3] , Rudy Gultom[4] , Pujo Widodo[5]

[1,2,3,4,5]Indonesia Defence University, Indonesia.

Abstract

The birth of the cyber world has brought a new color of life in the ecosystem of human life. The two worlds that were originally considered to be independent have converged with each other. Various events in the cyber world are allegedly an extension of what is happening in the physical world. And at the same time events in the physical world have the potential to influence unwanted events in the cyber world. This study aims to examine events in the past that show a relationship between the two worlds. The data used are a number of events that have occurred in Indonesia in the last two decades. The methodology used is through case study analysis. The results show that there are six types of events in the physical world that affect a number of events in the cyber world. On the other hand, there are also six types of events in the cyber world that stimulate unwanted events in the real world. Humans need to understand the causal relationship between the two worlds in order to be able to understand the various phenomena that occur every day.

Keywords: cyber space, physical world, criminal events

Introduction

At the beginning of the birth and use of the internet, a term such as virtual world or cyber world has been introduced to represent it. This virtual world is considered as an arena of interaction between those who have access to use computer systems that are connected in a gigantic network. These historical events indirectly colored the mindset of humans in the early days of the development of the internet, which dichotomies the real world with the virtual world [1].

In the context of this dichotomy, an opinion is formed that there is no clear and unequiv- ocal relationship between these two worlds [2, 3]. Each stands alone and does not affect each other. An example is the opinion that says that wars that occur in the real world will have no effect in cyberspace, and vice versa. Even users or individuals sometimes have "two personalities" that are different when interacting with these two worlds. When in the real world, the person concerned has the data, behavior, and profile as it is; but when enter- ing the virtual world, the person concerned can pretend to be someone else because of the flexibility and possibilities offered.

Email addresses: eko.indrajit@idu.ac.id (Richardus Indrajit), lilly.wasitova@idu.ac.id (Lilly Wasitova), marsetio@idu.ac.id (Marsetio), rudy.gultom@idu.ac.id (Rudy Gultom), pujo.widodo@idu.ac.id (Pujo Widodo)

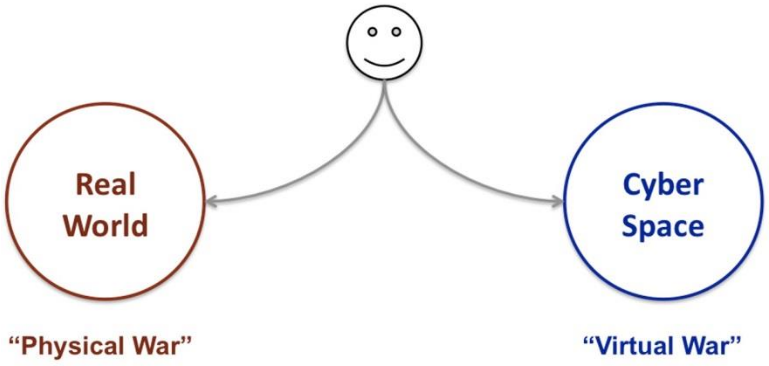

Figure 1: The Two Worlds in Human Ecosystem

Gradually, in accordance with the rapid development of the internet and information technology, which was previously only used for research and education, it began to develop into industry and other aspects of life. Business transactions began to occur, social in- teractions between individuals became more and more symptomatic, the spread of culture intensified, political openness and media freedom dominated daily life, and so on [4, 5]. Sev- eral world research centers have even indicated that there has been a significant decrease in the number of economic transactions that usually occur in the real world — due to shifting to the virtual world which provides a number of benefits such as efficiency and optimiza- tion [6]. For example, in terms of the tendency to buy goods that switch from cash to electronic-based payment models (such as credit cards, debit cards, telephone credit, and so on).

This phenomenon implies that what is happening in the virtual world cannot be separated from the reality in the real world, given the tendency for the two worlds to overlap, which shows that the slices are getting bigger and bigger [7, 8]. This is further clarified by the fact that those who interact in cyberspace are actually human individuals, using legal means of payment of money, and involving a number of legal agreement documents. With the overlap of the two worlds, it is clear that there will be a fairly close relationship between one world and another [9]. What happens in the virtual world will greatly affect those in the real world, and vice versa. Even in the future, when all individuals are connected and can access the internet, the two worlds will be identically united [10, 11].

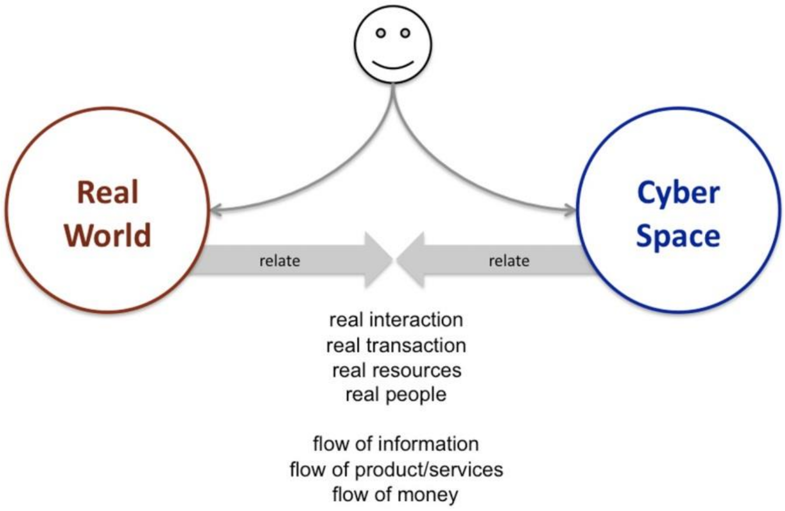

Figure 2: Interdependent Phenomena between The Two Worlds

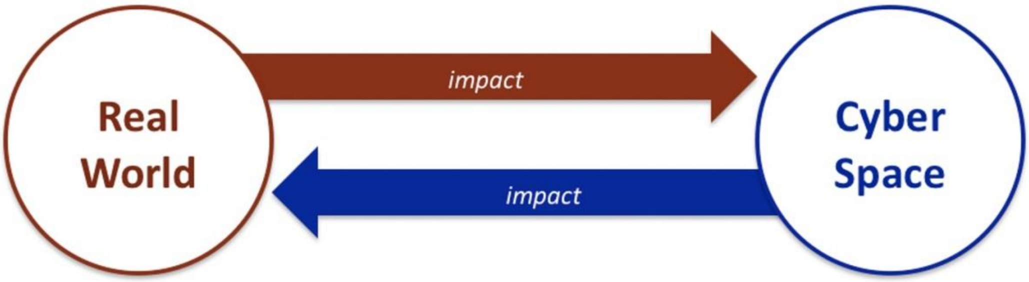

Figure 3: Mutual Impacts between The Two Worlds

Results

Related to the issue of internet security that is being talked about by many people today, there are also a number of presumptions that predict that things that happen in the real world can have an effect in cyberspace and vice versa - especially things related to various internet crime events. The results of an in-depth study of a number of cases in the physical world that affect events in the cyber world show that there are six types of events. The six triggering events relate to: (i) political incidents; (ii) international events; (iii) computer- security publication books; (iv) training modules; (v) pirated software; and (vi) community programs. Meanwhile, six other events in the cyber world that triggered events in the physical world were, among others, due to the existence of: (i) personal blogs; (ii) citizen journalism; (iii) anonymous interactions; (iv) phishing and forgery; (v) propaganda; and (vi) communities review.

Discussion

1.1. The Impacts of Real-World Events on Cyberspace

From various monitoring results of much information security practitioners and the in- ternet, there are a number of events in the real world that directly or indirectly affect various events that take place in cyberspace. The following are some of the types of triggers for these events.

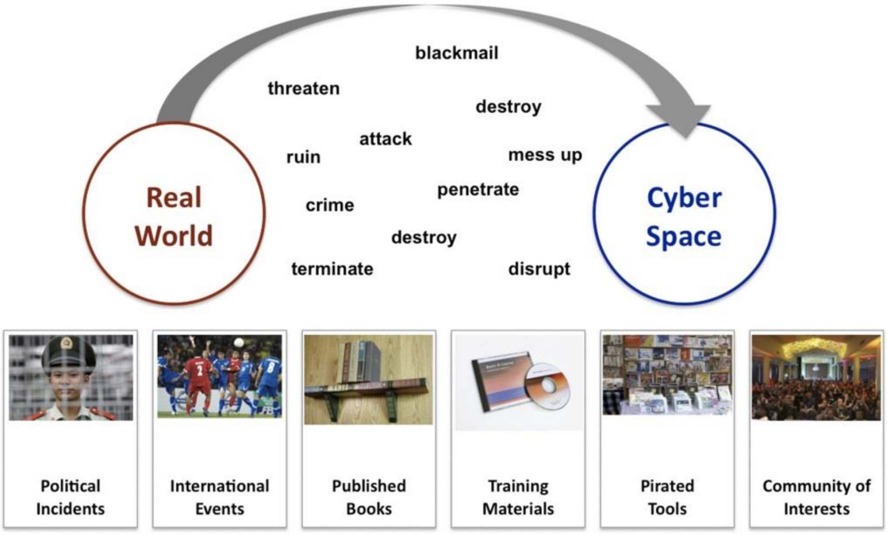

Figure 4: Cases on How Real World Events Bring Impacts to the Cyber Space

The first is the acts of attacks which were triggered by political events. An example was a political tension that raised between Indonesia and Malaysia in the case of the seizure of the Ambalat Straight. Right after the declaration of conflict, several web defacement attacks were launched between Indonesian and Malaysian underground hackers. Various sites with Indonesia internet domain addresses were hacked by the Malaysian side, and vice versa. The same thing happened between Indonesia and Australia whenever there was one or two political news that brought tension in bilateral relations between the two countries concerned [6]. The same phenomena had happened also in cyberspace when there is a feud between China and Tibet, Malaysia and Singapore, Russia and Georgia, and so on.

The second is the situations related to the hosting of various international scale events, such as the Olympics, Sea Games, Asian Games, and World Cup. The intense competition between a number of countries brought tension among their spectators. Look at the example when there was a football cup final between two countries. The hackers who support a country’s football team are not reluctant to attack the website of the country that is their opponent. The incident of the beating of an Indonesian karate referee by a number of Malaysian athletes also triggered a massive cyber attack that was difficult to control. It should be noted that not only sporting events, but large international gatherings such as the United Nations, G8, OPEC, and G20 could invite hackers to launch severe attacks in cyberspace.

The third is triggered by the examples of attacks procedures that were introduced to the public through publications or training modules. It turns out that the trend of types of attacks in cyberspace – such as SQL Injection, Web Defacement, Botnets, DOS/DDOS Attacks, and so on – is closely related to publications related to the hacking process which are sold freely in the market. Most of the training modules for instance are accompanied by case examples or exercises involving certain hacking activities [3, 5]. The readers who were the students simply followed step-to-step activities as instructed by the book. They did not suspect that the activities they carried out were basically a system penetration process that violated the law because it was without permission.

The fourth is due to the training activities demonstrated by the instructors. For ex- ample, it is very difficult to understand the theory of internet security without providing and conducting a number of examples of vulnerability analysis or penetration testing. Some of the instructors were not using virtual environment due to many excuses. It caused the students to conduct their learning activities in real cyber space environment. The adage of attacking is the best way of defending giving birth to various cases of attacks on real sites that cause damage.

The fifth is triggered by the existing pirating software or tools that could be easily downloaded from the internet. These programs that were sold freely at low prices not only gave users the freedom to carry out various types of attacks in cyberspace, but from day to day also offer conveniences in using them (user-friendly). For those who have a hobby of pursuing the world of internet security, these supporting software were very useful because they provide a variety of tricks, facilities, features, and very diverse capabilities [9, 12, 13]. The sixth that often triggers action and events in cyberspace was the activity of un- derground communities that often hold competitions to break into certain sites. Hackerscommunity who usually meet in a number of places exchange ideas and related information about various vulnerabilities of the world’s leading sites [14]. When they meet, it is often seen that there are a number of hackers who show off their skills by breaking into various sites that are known to be difficult to penetrate.

1.2. The Impacts of Events in Cyberspace on the Real World

The opposite phenomenon where events in the cyber world trigger problems in the cyber world as well. The following are a number of cases that were found as evidence of the said statement.

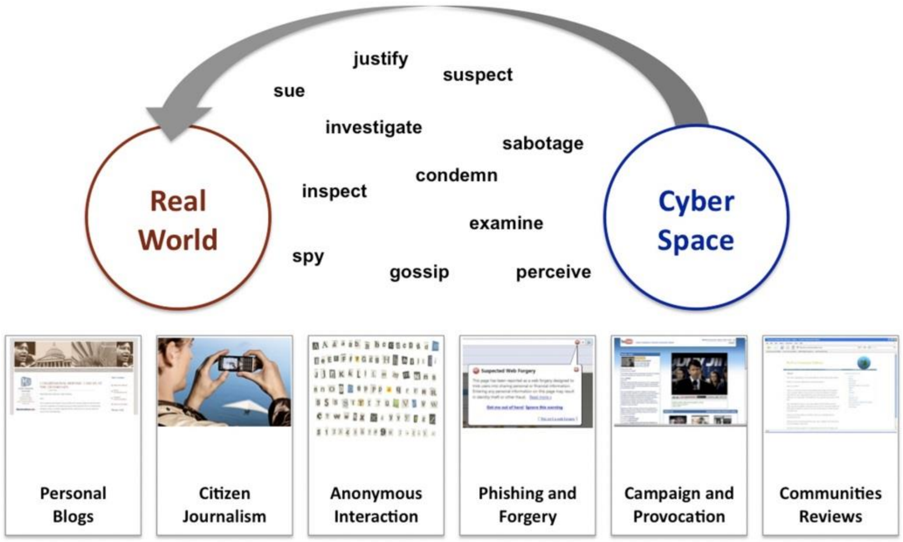

Figure 5: Cases on How Cyber Space Events Bring Impacts to the Real World Cyber Space

The first that what happens the most is the impact of someone’s blog message. The contents of a blog are more of an experience and personal view of individuals or certain events or events based on certain feelings, perceptions, or assumptions. Not infrequently found in the blog mentions clearly and unequivocally the names of individual actors related to the content of the existing story. In this context, it turns out that not all individuals in the real world are ready to deal with such a "democratic opinion" nature. Many of them continue with the demands of "defamation" from those whose names are mentioned in a number of personal blogs that traveled around the cyberspace [12, 15]. By using various types of articles in the cyberlaw, the person concerned is trying to criminalize the blog writer.

The second is a phenomenon triggered by the development of the citizen journalism community. By using various electronic gadgets such as digital cameras, cell phones, personal digital assistants, and so on — a layman can become a journalist because of his ability to cover news wherever he is involved. Look at how the channels of communication between television and radio are opened with these individuals as is done by the world’s leading news agencies CNN and YouTube. Not infrequently an individual in carrying out his daily activities encounters interesting events such as: a member of parliament who is scolding a restaurant waiter, or a former official who is cursing a security guard, or an artist who is annoyed with a seller, or a public figure who was meeting with a notorious conglomerate, and so on. The incident was easily recorded and covered by using a mobile phone or digital device that was brought and then uploaded to the internet to be accessed and enjoyed by the public [12]. Of course the person concerned with various pretexts denied that he was in the recording and turned to the dispute and sued the "amateur journalist".

The third is the number of circulating dark e-mails or “canned e-mails” which contain threats, accusations, discrimination, or other things that are scary or discredit a person or institution in cyberspace. Although the identity of the sender is not clear, but if the content of the threat is related to terrorism, for example, or those who are threatened are important figures such as government officials, regardless of whether the content of the threat is true or not, its existence should be taken seriously. For example, the case of the circulation of the wills of the Bali bombers that threatened the safety of the President of the Republic of Indonesia which immediately received serious responses from the police, intelligence, and all law enforcement and internet security practitioners in the country.

The fourth is the occurrence of various types of crimes or forgeries that are committed to identity fraud or phishing against the customers of certain companies, especially banks. The most widely used technique is using email and SMS media. Under the guise of pretending that the person in question is a legitimate party, customers are asked to take remittances or notify certain keywords which lead to the disappearance of the victim's financial as- sets [10]. This incident in the virtual world really has an impact on the real world because the perpetrator knows exactly the weaknesses or limitations of knowledge of the potential victims.

The fifth is an action in the real world that starts from the discourse that occurs in the real world through e-mail, websites, mailing lists, newsgroups, social networking applications, chat rooms, and so on that have campaigned or persuasive nuances to take certain actions - both positive nor negative. Regardless of whether it is true or not, the existence of this chain email has sparked the anger of those who feel offended and intend to conduct massive demonstrations in the real world. Or a mailing list that advises its members to do certain things, such as: not participating in elections or becoming abstentions, boycotting foreign products, being hostile to certain organizations, and so on. Of course, all forms of appeal in this virtual world more or less have an effect on daily life.

The sixth are real-world events as a result of various assessments made by a number of individuals or communities on certain things — goods, services, products, individuals, organizations, and so on – which have a fairly broad impact in the real world. Look at how a customer who is disappointed with the quality of the product he bought then reveals all his worries in cyberspace. Or a tourist who had a bad experience while in a certain tourist area who advised others not to go there. Or how a group of people who have felt aggrieved by the services of a certain bank tell their personal experiences which can result in a rush from customers who are still active customers at the bank concerned, and so on. If in the past experiences like this could be isolated from the news, then with the internet, the public can also find out about them in a very short time.

Conclusion

The whole phenomenon above implies the need for continuous and unending efforts to educate and increase the insight of the community and the community regarding the importance of being careful and paying attention to ethics when interacting in the real world and in the real world. If an unwanted event occurs in the real world, all parties must be prepared if it will and will certainly spread to cyberspace — so that all data and information assets on the internet must be kept safe. Likewise, those who think that they can communicate freely and without limits on the internet should also be careful because if the person concerned commits certain actions that can harm others and the mechanism has been regulated in the applicable law, then civil and criminal penalties in the real world can be imposed.

REFERENCES

1. B. Valeriano, R. C. Maness (2015). [link].

   URL https://doi.org/10.1093/acprof:oso/9780190204792.001.0001
2. H. Rishikof (2022). [link].

   URL http://www.jstor.org/stable/10.2307/48642044?refreqid=search-gateway
3. L. Ayala, Threats and attack detection, Cyber-Physical Attack Recovery Procedures (2016) 15–26.
4. S. H. Sadeghi, Cyber space and real space, Studies in Systems, Decision and Control (2018) 23–37.
5. D. Halder, Assistance for cyber-crime victimisation, Cyber Victimology (2021) 57–72.
6. Emerging issue in cyber crime: Case study cyber crime in Indonesia, International Journal of Science and Research (IJSR) 5 (11) (2016) 511–514.

7. M. Kumazaki, H. Hasegawa, Y. Yamaguchi, H. Shimada, H. Takakura, Cyber Attack Stage Trac- ing System based on attack scenario comparison, Proceedings of the 8th International Conference on Information Systems Security and Privacy (2022).

8. K. B. Alexander, J. N. Jaffer, J. S. Brunet (2017). [link].

   URL http://www.jstor.org/stable/10.2307/26267398?refreqid=search-gateway

9. M. C. Libicki (2017). [link].

   URL http://www.jstor.org/stable/10.2307/26271590?refreqid=search-gateway

10. M. Chaturvedi, A. Unal, P. Aggarwal, S. Bahl, S. Malik, International cooperation in cyber space to combat cyber crime and terrorism, IEEE Conference on Norbert Wiener in the 21st Century (21CW (2014).

11. T. Welsh, Management of a cyber attack, Cyber Security Practitioner’s Guide (2020) 51–80.

12. E. Ignatuschtschenko (2021). [link].

    URL https://doi.org/10.1093/oxfordhb/9780198800682.013.7

13. D. Halder (2021). [link].

    URL https://doi.org/10.4324/9781315155685

14. H. Koppisetty, K. Potdar, S. Jain, Cyber-crime, forensics and use of data mining in Cyber Space: A survey, International Conference on Smart Systems and Inventive Technology (ICSSIT (2019).

15. E. Ignatuschtschenko (2021). [link].

    URL https://doi.org/10.1093/oxfordhb/9780198800682.013.7