*Doktrina: Journal of Law*, 4 (2) Oktober 2021 ISSN 2620-7141 (Print) ISSN 2620-715X (Online)
DOI: http://dx.doi.org/10.31289/doktrina.v4i2.5793

# *Doktrina: Journal of Law*

*Available online http://ojs.uma.ac.id/index.php/doktrina*

# Penanggulangan Tindak Pidana Siber Dengan Menggunakan Teori Jendela Pecah

## *Cybercrime Prevention by Using the Broken Window Theory*

**Wenggedes Frensh***
Fakultas Hukum Universitas Medan Area, Indonesia
*Coresponding Email: wenggedesfrensh@staff.uma.ac.id
Diterima: September 2021; Disetujui: Oktober 2021; Dipublish: Oktober 2021

## Abstrak

Berkembangnya teknologi informasi dan komunikasi memberikan manfaat positif seperti munculnya *e-learning*, *e-commerce*, *e-banking*, *e-government*, *e-medicine* dan lainnya. Namun teknologi informasi dan komunikasi juga memberikan dampak negatif dengan munculnya tindak pidana siber (*cybercrime*). Pengguna internet di Indonesia awal 2021 mencapai 202, 6 juta jiwa, jumlah ini meningkat 15, 5% atau 27 juta jiwa dibandingkan pada januari 2020. Di Indonesia kasus tindak pidana siber telah ditangani Direktorat Tindak Pidana Siber (Dittipidsiber) Bareskrim Polri sebanyak 4.656 kasus di tahun 2020 sepanjang periode januari sampai November. Penelitian ini bertujuan untuk mengetahui bagaimana penanggulangan tindak pidana siber di ruang siber dengan menggunakan teori jendela pecah (*broken window theory*). Metode penelitian yang digunakan adalah metode penelitian yuridis normatif dengan sumber data sekunder dan dianalisis secara deduktif. Hasil penelitian menunjukkan bahwa penanggulangan tindak pidana siber di ruang siber dapat menggunakan teori jendela pecah (*broken window theory*). Penanggulangan tindak pidana siber dilakukan dengan menjaga ruang siber agar tetap terjaga seperti jendela yang utuh (*window with glass*). Penjagaan ruang siber agar terlindung seperti sebuah jendela dengan kaca yang kuat adalah dengan menjaga ruang siber menggunakan Undang-Undang ITE dan Pornografi yang diterapkan, keamanan siber (*cybersecurity*) yang dijaga setiap pengguna teknologi dan Polisi siber yang melakukan patroli siber (*cyberpatrol*).
**Kata Kunci: Penanggulangan, Tindak Pidana Siber, Jendela Pecah**

## *Abstract*

*The development of information and communication technology provides positive benefits, such as the emergence of e-learning, e-commerce, e-banking, e-government, e-medicine and others. However, information and communication technology also has a negative impact with the emergence of cybercrime. Internet users in Indonesia in early 2021 reached 202.6 million people, this number increased by 15.5% or 27 million people compared to January 2020. This study aims to determine how to tackle cyber crime in cyberspace by using the broken window theory. The research method used is a normative juridical research method with secondary data sources and analyzed deductively. The results of the study indicate that the prevention of cyber crime in cyberspace can use the broken window theory. The prevention of cyber crime is carried out by maintaining cyber space so that it is maintained like a window with glass. Safeguarding cyberspace to be protected like a window with strong glass is to protect cyberspace using the ITE and Pornography Law that applies, cybersecurity which is guarded by every technology user and cyber police who conduct cyber patrols.*

***Keywords: Prevention, Cybercrime, Broken Window***

**How to Cite:** Frensh. W. (2021). Penggulangan Tindak Pidana Siber Dengan Menggunakan Teori Jendela Pecah. Doktrina: Journal of Law. 4 (2): 159-169

**PENDAHULUAN**

Teknologi telah berkembang sangat pesat dan mengambil peranan yang penting dalam kehidupan manusia selama beberapa dekade terakhir. Kurang dari dua dekade yang lalu, kebanyakan orang tidak memiliki telepon seluler untuk mengirimkan pesan. Komputer pribadi juga masih cukup mahal dan secara ekonomis jauh dari jangkauan banyak keluarga. (Thomas and Adam: 2016). Namun saat ini teknologi informasi dan komunikasi seperti telepon seluler dan komputer pribadi telah banyak digunakan untuk memenuhi kehidupan sehari-hari masyarakat.

Teknologi informasi dan komunikasi yang digunakan masyarakat terhubung dengan internet. Internet adalah sistem jaringan komputer yang saling terhubung di seluruh dunia dan dapat diakses publik untuk mengirimkan data (Rajmohan Joshi: 2006). Dengan internet semua pengguna teknologi informasi dan komunikasi di seluruh dunia akan dapat saling terhubung dan melakukan komunikasi maupun bertukar informasi.

Di Indonesia, masyarakat yang menggunakan internet cukup tinggi. Masyarakat Indonesia yang menggunakan internet pada awal 2021 mencapai 202, 6 juta jiwa. Jumlah ini meningkat 15,5 % atau 27 juta jiwa jika dibandingkan pada Januari 2020 lalu. Masyarakat Indonesia yang menggunakan internet rata-rata berusia 16 sampai 64 tahun. Internet yang digunakan dihubungkan dengan perangkat elektronik seperti telepon seluler, laptop/PC, tablet, *smartwatch*, dan alat elektronik lainnya. Masyarakat Indonesia rata-rata dapat menghabiskan waktu selama 8 jam 52 menit dalam menggunakan internet. (Galuh: 2021)

Teknologi informasi dan komunikasi terhubung dengan internet memberikan banyak manfaat yang positif bagi kehidupan masyarakat Indonesia, seperti pembelajaran secara elektronik (*e-learning*), perdagangan secara elektronik (*e-commerce*), pelayanan perbankan secara elektronik (*e-banking*), pemberian informasi dan pelayanan dari pemerintah secara elektronik (*e-government*), pengetahuan klinis medis secara elektronik (*e-medicine*) dan layanan elektronik lainnya (Leela and Wendy: 2006).

Teknologi informasi dan komunikasi yang terhubung dengan internet, selain memberikan banyak manfaat bagi kehidupan masyarakat, namun juga memiliki dampak negatif seperti yang disebutkan David Wall, yaitu terjadinya pelanggaran hukum maupun tindak

kejahatan seperti *cyber-trespass*, *cyber deception and theft*, *cyber-porn and obscenity*, dan *cyber-violence* (Thomas and Adam: 2016). Kejahatan yang terjadi di ruang siber disebut dengan Tindak pidana siber (Nash Haynes: 2018).

Di Indonesia, jumlah kasus tindak pidana siber cukup tinggi. Terkait dengan kasus tindak pidana siber, Direktorat Tindak Pidana Siber (Dittipidsiber) Bareskrim Polri telah menangani 4.656 kasus sepanjang periode Januari hingga November 2020. Berdasarkan data Dittipidsiber Bareskrim Polri, tindak pidana siber yang ditangani seperti pencemaran nama baik sebanyak 1.743 kasus, penipuan 1.295 kasus, pornografi 390 kasus, akses ilegal 292 kasus, ujaran kebencian atau SARA 209 kasus, berita bohong/palsu/*hoax* dengan 189 kasus, manipulasi data 160 kasus dan pengancaman 131 kasus (Irwan Suherman: 2020).

Tindak pidana siber (*cybercrime*) sering disebut juga dengan istilah *"old wine in a new bottle"* dan *"new wine in new bottles"* (Thomas Holt, Adam Bossler and Kathryn Seigfried: 2015). Tindak pidana seperti pencurian, pemerasan, penghinaan dan lainnya di ruang siber disebut sebagai *"old wine"*, karena tindak pidana ini dianggap umum dan sering terjadi. Sedangkan *"new wine"* digunakan untuk tindak pidana seperti *malware* yang baru muncul akibat adanya perkembangan teknologi.

Tindak pidana siber memiliki karakteristik khusus, karna tindak pidana ini memanfaatkan teknologi informasi dan komunikasi sebagai instrumen (alat yang digunakan) untuk melakukan tindak pidana. Selain itu tindak pidana siber terjadi bukan diruang yang dapat disentuh, melainkan tindak pidana ini terjadi di ruang siber yang berada di dalam jaringan menghubungkan berbagai perangkat teknologi informasi dan komunikasi.

Karakteristik khusus tindak pidana siber membuat tindak pidana ini dalam upaya penanggulangannya juga harus menggunakan pendekatan dan cara yang khusus. Dalam upaya penanggulangan kejahatan terdapat teori jendela pecah (*broken window theory*) dari George Kelling dan James Wilson. Teori jendela pecah menjelaskan,Jika sebuah jendela di gedung rusak dan dibiarkan tidak diperbaiki, maka semua jendela lainnya akan segera rusak. Satu jendela pecah yang tidak diperbaiki merupakan tanda tidak ada yang peduli, sehingga akan menyebabkan lebih banyak lagi jendela yang akan dipecahkan (George Kelling and James Wilson: 1982) .

Berdasarkan uraian diatas, maka penelitian ini bertujuan untuk mengetahui bagaimana upaya penanggulangan tindak pidana siber di ruang siber, dengan menggunakan teori jendela pecah (*broken window theory*).

## METODE PENELITIAN

Jenis penelitian yang digunakan adalah jenis penelitian normatif. Penelitian ini bersifat deskriptif analitis. Sumber data penelitian diperoleh melalui data sekunder yang terdiri dari bahan hukum primer. Analisa data yang digunakan yaitu analisa data kualitatif, yang akan dikelola untuk menjawab permasalahan dalam penelitian ini.

## HASIL DAN PEMBAHASAN

### Penanggulangan Tindak Pidana Siber di ruang siber dengan menggunakan Teori *Broken Window*

Kelling dan Coles adalah dua kriminolog yang memiliki Teori *Broken Window*. Teori *Broken Window* adalah teori kriminologi yang bertujuan untuk melakukan penanggulangan kejahatan. Kelling dan Coles menyimpulkan bahwa kriminalitas terjadi sebagai akibat dari adanya ketidakteraturan. Semua bermula dari adanya jendela yang kacanya pecah di suatu pemukiman. Jendela yang pecah (*broken window*) yang didiamkan oleh pemiliknya akan mendorong pelaku kriminal lain untuk memecahkan kaca jendela lainnya. (Rhenald Kasali : 2007).

Berdasarkan penjelasan teori *broken window* dari Kelling dan Coles, maka penanggulangan kejahatan harus dilakukan dengan cara seperti menjaga sebuah rumah agar tetap memiliki jendela dengan kaca yang utuh (tidak pecah). Jika sebuah rumah memiliki jendela yang tidak pecah, maka rumah tersebut dalam keadaan terjaga. Tetapi jika rumah memiliki jendela yang pecah, maka akan membuat orang lain masuk kerumah dan menganggap rumah tidak dijagah oleh penghuninya.

Dalam kehidupan sehari-hari masyarakat memiliki rumah ataupun tempat persingahan. Rumah menjadi tempat untuk menyimpan barang-barang berharga. Rumah akan ditutup rapat dengan menggunakan pintu maupun jendela agar tidak sembarang orang dapat memasuki rumah tersebut. Maka rumah yang terjaga dengan ditutup dengan pintu maupun jendela akan menggambarkan kondisi rumah yang terjaga dan akan dihindari pelaku kejahatan.

Teknologi informasi dan komunikasi yang terhubung dengan internet akan membentuk sebuah ruang yang disebut

dengan *cyberspace* (Andrew Murray: 2019). Istilah *cyberspace* pertama kali digunakan William Gibson pada tahun 1982. *Cyberspace* digambarkan Gibson sebagai halusinasi konsensual yang dialami setiap hari oleh miliaran operator sah yang masuk melalui komputer (Adam Segal: 2016). Berdasarkan penjelasan Gibson maka dapat dilihat bahwa *cyberspace* merupakan ruang yang menghubungkan pengguna teknologi informasi dan komunikasi dengan pengguna lainnya.

*Cyberspace* sebagai ruang yang menghubungkan pengguna teknologi informasi dan komunikasi ini disebut juga dengan istilah ruang siber. Kelling dan Coles dalam teori *broken window* telah menjelaskan bahwa kriminalitas terjadi akibat adanya ketidakteraturan dan semua bermula dari adanya jendela kaca yang pecah di suatu pemukiman atau rumah. Sehingga kaca yang utuh pada jendela sangat penting. Dalam ruang siber terdapat banyak ruang-ruang siber yang dimasuki oleh pengguna internet (netizen). Maka setiap ruang yang ada didalam ruang siber dapat disebut sebagai jendela dengan kaca (*window with glass*) berdasarkan teori broken window.

Di ruang siber terdapat kejahatan yang disebut dengan *cybercrime*. Mark Jhonson menjelaskan *cybercrime* adalah kejahatan apa pun yang melibatkan penggunaan komputer yang terhubung ke internet atau setiap jaringan yang sama (Mark Jhonson: 2016). *Cybercrime* ini disebut juga dengan istilah Tindak Pidana Siber.

**Penanggulangan Tindak Pidana Siber dengan menjaga Ruang Siber Menggunakan Undang-Undang ITE dan Pornografi**

Dalam upaya penanggulangan dan penindakan terhadap tindak pidana siber di Indonesia terdapat Undang-Undang No. 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik dan Undang-Undang No. 44 Tahun 2008 tentang Pornografi. Dengan adanya UU ITE dan Pornografi maka akan membuat pengguna internet (*netizen*) menghindari untuk melakukan tindak pidana siber di ruang siber.

Dalam Undang-Undang No. 19 Tahun 2016 perubahan atas Undang-Undang No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik pada Pasal 27 ayat (1) mengatur tentang pelanggaran kesusilaan di ruang siber, Pasal 27 ayat (2) perjudian di ruang siber, Pasal 27 ayat (3) penghinaan dan/atau pencemaran nama baik di ruang siber, Pasal 27 ayat (4) pemerasan dan/atau pengancaman di

ruang siber, Pasal 28 ayat (1) menyebarkan berita bohong dan menyesatkan yang mengakibatkan kerugian konsumen di ruang siber, Pasal 28 ayat (2) menimbulkan rasa kebencian atau permusuhan individu dan/atau kelompok masyarakat tertentu berdasarkan atas suku, agama, ras, dan antargolongan (SARA) di ruang siber dan Pasal 29 perundungan di ruang siber (*cyberbullying*).

Dalam Undang-Undang No. 44 Tahun 2008 tentang Pornografi terdapat pasal-pasal yang mengatur larangan pornografi di ruang siber antara lain :

Dilarang memproduksi, membuat, memperbanyak, menggandakan, menyebarluaskan, menyiarkan, mengimpor, mengekspor, menawarkan, memperjualbelikan, menyewakan, atau menyediakan pornografi di ruang siber (Pasal 4 ayat 1).

Dilarang menyediakan jasa pornografi di ruang siber (Pasal 4 ayat 2).

Dilarang meminjamkan atau mengunduh pornografi di ruang siber (Pasal 5).

Dilarang memperdengarkan, mempertontonkan, memanfaatkan, memiliki, atau menyimpan produk pornografi di ruang siber (Pasal 6).

Dilarang mendanai atau memfasilitasi pornografi di ruang siber (Pasal 7).

Dilarang menjadi objek atau model yang mengandung muatan pornografi diruang siber (Pasal 8).

Dilarang menjadikan orang lain sebagai objek atau model yang mengandung muatan pornografi di ruang siber (Pasal 9).

Dilarang mempertontonkan diri atau orang lain dalam pertunjukan atau di muka umum yang menggambarkan ketelanjangan, eksploitasi seksual, persenggaman, atau yang bermuatan pornografi lainnya (Pasal 10).

Dilarang melibatkan anak dalam kegiatan dan/atau sebagai objek pornografi di ruang siber (Pasal 11).

Dilarang mengajak, membujuk, memanfaatkan, membiarkan, menyalahgunakan kekuasaan, atau memaksa anak dalam menggunakan produk atau jasa pornografi (Pasal 12).

Dengan adanya Undang-Undang ITE dan Undang-Undang Pornografi, maka setiap pengguna internet (*netizen*) yang melakukan tindak pidana siber akan mendapatkan sanksi pidana sesuai dengan ketentuan aturan yang berlaku. Bagi pengguna internet yang telah mengetahui Undang-Undang ITE dan Undang-Undang

Pornografi, akan menghindari untuk melakukan tindak pidana siber.

Undang-Undang ITE dan Undang-Undang Pornografi sebagai regulasi peraturan perundang-undangan yang mengatur tentang tindak pidana siber, akan menjadi *"window with glass"*. Artinya Undang-Undang ITE dan Undang-Undang Pornografi menjaga agar pengguna internet tidak sembarangan melakukan tindak pidana siber saat berada di ruang siber.

Jika dalam ruang siber tidak terdapat Undang-Undang ITE dan Undang-Undang Pornografi, maka pengguna internet akan menganggap ruang siber bebas dalam melakukan tindakan melanggar hukum maupun perbuatan pidana. Hal ini yang akan menyebabkan terjadinya "broken window", dimana tidak adanya undang-undang yang memberikan perlindungan bagi pengguna internet. Sehingga pengguna internet akan melakukan tindakan melanggar hukum maupun tindak pidana di ruang siber.

**Penanggulangan Tindak Pidana Siber dengan menjaga Ruang Siber Menggunakan Keamanan Siber (*Cyber Security*)**

Tindak pidana siber merupakan salah satu ancaman paling berbahaya bagi perkembangan negara dan berdampak serius terhadap setiap aspek pertumbuhan suatu negara. Entitas pemerintah (*government entities*), organisasi nirlaba (*non-profit organizations*), perusahaan swasta (*private companies*), dan warga negara (*citizens*) adalah target potensial dari sindikat penjahat siber (Madhu Tyagi: 2017).

Penanggulangan tindak pidana siber adalah aspek paling penting. Keamanan siber (*cybersecurity*) adalah pertahanan terbaik dalam menanggulangi tindak pidana siber. Setiap pengguna teknologi informasi dan komunikasi harus menyadari risiko ancaman di ruang siber (Madhu Tyagi: 2017).

Madhu Tyagi menjelaskan terdapat beberapa langkah sederhana yang penting diperhatikan dalam menjaga dasar keamanan siber (*cybersecurity*), yaitu sebagai berikut (Madhu Tyagi: 2017) :

Mengatur kata sandi yang kuat dan mengubahnya secara teratur (*Set strong passwords and changed regularly*).

Secara teratur memperbaruhi komputasi (*patch*) untuk semua komputer (*Regular and updated patches for all computers*).

Menyadari potensi ancaman dalam jaringan (*online*), misalnya tidak mengklik tautan atau membuka lampiran dari email

yang tidak diketahui (*Making sure aware of the potential threats online, not clicking links or opening attachment from unknow emails*).

Memiliki sistem cadangan reguler untuk semua data dan sistem (*Having a regular back-up system in place for all data and system*).

Memiliki proses dalam jaringan (*online*) dan ruang siber yang jelas, konsisten, dan diperbarui (*Having clear, consistent and updated online and cyber processes*).

Memahami kerentanan dan melakukan perbaikan rutin (*Understanding what your vulnerabilities are and making regular improvements*).

Mengatur *Firewall*. *Firewall* adalah lapisan perlindungan penting pertama terhadap serangan di ruang siber. *Firewall* menawarkan perlindungan yang kuat terhadap virus dan malware untuk seluruh jaringan (*Manage Firewall. This is the first crucial layer of protection against cyber-attacks. It offers powerful protection against viruses and malware for your whole network*).

Simulasi dan pelatihan phishing (pengelabuan). Ini akan memberi analisis tentang kerentanan dan pengguna terhadap email phishing dan menawarkan pelatihan penting tentang keamanan informasi (*Phishing simulation and Training. This provides with analytics on the vulnerability and users to phishing emails and offers essential training on information security*).

Pemantauan keamanan siber (*cybersecurity monitoring*). *Cybersecurity monitoring* ini bertindak seperti sebuah alarm yang memberikan peringatan terhadap lalu lintas diruang siber yang tidak bersahabat atau serangan terhadap jaringan *firewall* (*Cyber security monitoring. This act like a burglar alarm for possible hostile traffic or attacks that have dodged the network firewall*).

Menjaga keamanan siber (*cybersecurity*) seperti tahapan yang disebutkan Tyagi, merupakan upaya yang dapat dilakukan pengguna internet untuk menghindari diri menjadi korban tindak pidana siber. Dengan memperkuat keamanan siber dari teknologi informasi dan komunikasi yang digunakan, maka akan membuat pengguna internet dapat dengan nyaman dan aman berada diruang siber.

Keamanan siber seperti membuat kata sandi yang kuat (*set strong passwords*), memperbarui komputasi (*patch*) pada komputer, tidak sembarang membuka tautan (*links*) yang tidak diketahui, memiliki sistem cadangan

reguler pada data, memiliki proses dalam jaringan (*onlin*e) yang jelas, memahami kerentanan, melakukan perbaikan rutin, mengatur *firewall*, memahami kerentanan terhadap *email phishing*, dan memiliki pemantauan keamanan siber (*cybersecurity monitoring*), merupakan penjagaan diruang siber agar pengguna internet terhindar dari ancaman siber yang akan berujung menjadi korban tindak pidana siber.

Dengan adanya keamanan siber yang telah dilakukan pengguna internet saat berada di ruang siber, maka ini akan memberikan perlindungan. Perlindungan kemanan siber ini akan menjadi *"window with glass"* yang dimana penjahat siber (*cybercriminal*) dalam melakukan tindakannya tentunya tidak dapat melakukan tindak pidana siber secara langsung, dikarenakan teknologi informasi dan komunikasi maupun jaringan yang digunakan telah mendapatkan perlindungan (*protection*).

Sinchul Back dan Jennifer LaPrade menjelaskan dalam keamanan siber terdapat hubungan antara faktor manusia (*human*), teknologi (*technology*), dan tindak pidana siber (*cybercrime*). Berdasarkan laporan *European Cyber Security Perspective* 2019 menyatakan bahwa teknologi mutakhir tidak bisa menjadi satu-satunya solusi untuk memitigasi risiko keaman siber, faktanya elemen manusia juga merupakan komponen yang sangat krusial untuk mengganggu ancaman siber (Sinchul Back and Jennifer La Prade: 2019)

**Penanggulangan Tindak Pidana Siber dengan menjaga Ruang Siber Menggunakan Patroli Siber (*Cyber Patrol*)**

Badan Reserse Kriminal atau Bareskrim Polri memiliki polisi siber untuk melakukan penanggulangan dan penindakan terhadap tindak pidana siber. Polisi siber Polri memiliki tujuan agar ruang siber dapat berjalan bersih, sehat dan produktif. Polisi siber Polri juga memiliki tujuan untuk mengurangi konten-konten *hoax* dan negatif yang ada di media sosial. Melalui polisi siber Polri, Kepolisian akan memberikan edukasi dan memberitauhkan bahwa apa yang ditulis ada melanggar pidana, memberitauhkan agar jangan ditulis kembali dan segera dihapus (Hendrik Khoirul Muhid: 2021).

Adam Bossler dan Thomas Holt menjelaskan polisi siber memiliki sedikit informasi tentang bagaimana manajemen untuk menangani tindak pidana siber. Polisi siber masih menganggap bahwa strategi terbaik untuk penanggulangan

tindak pidana siber adalah dengan memperbaiki sistem hukum dan masyarakat yang lebih berhati-hati saat berada diruang siber (Adam Bossler and Thomas Holt: 2012)

## SIMPULAN

Berdasarkan uraian di atas, maka hasil penelitian menunjukkan bahwa dalam upaya penanggulangan tindak pidana siber di ruang siber dapat dilakukan dengan menggunakan teori jendela pecah (*broken window theory*). Penanggulangan dengan teori jendela pecah dilakukan dengan menjaga ruang siber agar tetap terjaga seperti jendela yang utuh (*window with glass*). Penjagaan ruang siber agar terlindung seperti sebuah jendela dengan kaca yang kuat adalah dengan menjaga ruang siber menggunakan Undang-Undang ITE dan Pornografi yang diterapkan, Keamanan Siber (*Cyber Security*) yang dijaga setiap pengguna teknologi dan Polisi Siber yang melakukan Patroli Siber (*Cyber Patrol*).

## DAFTAR PUSTAKA


Adam M. Bossler and Thomas J. Holt. (2012). Patrol Officers Perceived Role in Responding to Cybercrime, Policing An International Journal of Police Strategies and Management, 35 (1), 165-181.

Adam Segal. (2016). The Hacked World Order: How Nations Fight, Trade, Maneuver, and Manipulate in The Digital Age, New York : PublicAffairs

Andrew Murray. (2019). Information Technology Law, United Kingdom : Oxford University Press

Kompas.com. 2016. Jumlah Pengguna Internet Indonesia 2021 Tembus 202 Juta. Diakses dari Tekno.kompas.com/read/jumlah-pengguna-internet-indonesia-2021-tembus-202-juta

Leela Damodaran and Wendy Olphert. (2006). Informating Digital Futures : Strategies for Citizen Engagement. Dordrecht : Springer

Madhu Tyagi. (2017). Security Against Cybercrime: Prevention and Detect, Mumbai : Horizon Books

Mark Johnson. (2016). Cybercrime, Security and Digital Intelligence, New York : Routledge

Metro.tempo.co. 2021. Polisi Virtual atau Polisi Siber Begini Cara Kerjanya. Diakses dari metro.tempo.co/read/polisi-virtual-atau-polisi-siber-begini-cara-kerjanya.

Theatlantic.com. 1982. Broken Windows : The Police and Neighborhood Safety. Diakses dari theatlantic.com/magazine/broken-windows.

PikiranRakyat.com. 2020. Januari-November 2020 Terjadi 4.250 Kejahatan Siber, Polisi: Diperkirakan Akan Terus Meningkat. Diakses dari pikiran rakyat.com/nasional/januari-november-2020-terjadi-4250-kejahatan-siber-polisi-diperkirakan-akan-terus-meningkat.

Rajmohan Joshi. (2006). Encyclopaedia of Journalism and Mass Communication, Delhi : Isha Books

Rhenald Kasali. (2007). Re-Code Your Change DNA: Membebaskan Belenggu-Belenggu Untuk Meraih Keberanian Dan Keberhasilan Dalam Pembaharuan, Jakarta : Gramedia Pustaka Utama

Sinchul Back and Jennifer LaPrade. (2019). The Future of Cybercrime Prevention Strategies: Human Factors and A Holistic Approach to Cyber Intelligence, International Journal of Cybersecurity Intelligence & Cybercrime, 2 (2), 1-4.

Thomas J. Holt and Adam M. Bossler. (2016). Cybercrime In Progress : Theory and Prevention of Technology- Enabled Offenses, New York : Routledge

Thomas J. Holt, Adam M. Bossler and Kathryn C. Seigfried. (2015). Cybercrime And Digital Forensics An Introduction, New York : Routledge

Nash Haynes. (2018). Cybercrime, United Kingdom : ED-Tech Press

Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik.

Undang-Undang Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik.

Undang-Undang Nomor 44 Tahun 2008 Tentang Pornografi.