# STRATEGI MENINGKATKAN KESADARAN *CYBERSECURITY* PADA PENGGUNA MEDIA SOSIAL DI INDONESIA SEBAGAI PERWUJUDAN *SMART AND GOOD CITIZENSHIP*

Rehan Aditya Saputra
*Pendidikan Pancasila dan Kewarganegaraan, Universitas sebelas Maret*
*rehanaditya06@student.uns.ac.id*

**ABSTRAK**

Penelitian ini bertujuan untuk meningkatkan kesadaran masyarakat, utamanya bagi para pengguna sosial media dalam menghadapi serangan *Cybersecurity* yang terjadi dengan cerdas. Artikel ini dibuat dengan menggunakan metode penelitian studi literatur untuk memberikan landasan teoritis sebagai upaya untuk mendapatkan informasi yang akan dijelaskan pada pembahasan. Dalam hasil ditemukan berbagai macam ancaman dan tantangan yang dihadapi oleh masyarakat atau pengguna sosial media terhadap ancaman dari serangan *cybersecurity* yang mengancam keamanan setiap individu dalam kehidupan berbangsa dan bernegara. Banyak macam ancaman seperti ancaman fisik, logikal, hingga operasional. Dari mulai serangan *malware, cyberbullying*, hingga *cybercrime.* Dalam menghadapi berbagai macam ancaman dan tantangan, masyarakat atau pengguna sosial media dapat melakukan berbagai macam upaya yang bisa dilakukan seperti dengan *capacity building*, meningkatkan kapasitas SDM, pembentukan Undang-Undang tindak pidana siber, melakukan kerja sama dalam keamanan siber, dan pencegahan *malware*. Berbagai upaya tersebut dapat dilakukan dengan memahami nilai-nilai dasar bela negara. Hal ini menjadikan dasar bagi setiap masyarakat atau pengguna sosial media agar mampu menjadi warga negara yang baik dan cerdas dalam menghadapi berbagai macam ancaman dan tantangan yang mengancam keamanan siber.

**Kata kunci** *: Cybersecurity, malware,* warga negara, ancaman, tantangan

***ABSTRACT***

*This research aims to increase public awareness, especially for social media users, in dealing with cyber security attacks that occur intelligently. This article was created using the literature study research method to provide a theoretical basis in an effort to obtain information that will be explained in the discussion. The results found various kinds of threats and challenges faced by society or social media users regarding threats from cybersecurity attacks that threaten the security of every individual in the life of the nation and state. There are many types of threats, such as physical, logical and operational threats. Starting from malware attacks, cyberbullying, to cybercrime. In facing various kinds of threats and challenges, the public or social media users can carry out various kinds of efforts such as capacity building, increasing human resource capacity, establishing cybercrime laws, collaborating in cyber security, and preventing malware. These various efforts can be made by understanding the basic values of defending the country. This provides the basis for every citizen or social media user to be able to become a good and intelligent citizen in facing various threats and challenges that threaten cyber security.*

***Keyword****: Cybersecurity, malware, citizens, threats, challenges*

## PENDAHULUAN

Dalam era digital yang terus berkembang, penggunaan media sosial telah menjadi suatu fenomena yang mendominasi sebagai bentuk interaksi masyarakat di indonesia. Berbagai platform media sosial seperti Facebook, Instagram, Twitter, dan Whatsapp telah menjadi bagian yang tidak dapat terpisahkan dalam kehdiupan sehari-hari banyak individu. Namun seiring dengan adanya perkembangan teknologi serta adanya kemajuan internet yang semakin luas, keamanan informasi pengguna media sosial menjadi semakin rentan terhadap berbagai ancaman terutama ancaman *cyber*.

Kesadaran terhadap *cybersecurity* pada penggunaan media sosial di Indonesia masih menjadi isu yang perlu diperhatikan secara serius. Data-data pribadi dari pengguna seperti informasi kontak hingga suatu hal yang detail dalam kehidupan sehari-hari, dapat dengan mudah dieksploitasi oleh pihak-pihak yang tidak bertanggung jawab apabila hal tersebut tidak dilindungi dengan baik. Hal ini mengakibatkan berbagai konsekuensi buruk diantara lain pencurian identitas, penipuan online dengan berbagi modus, hingga penyebaran informasi palsu yang dapat merugikan individu ataupun suatu kelompok masyarakat.

Selain itu, tren penggunaan media sosial yang terus meningkat juga menunjukan bahwa banyak individu, mulai dari anak-anak, remaja, hingga dewasa terpapar potensi bahaya *cyber* yang dapat merusak citra diri serta reputasinya secara online. Pemahaman terkait praktik *cybersecurity* yang masih kurang juga menjadi faktor utama dalam meningkatnya resiko keamanan bagi pengguna media sosial di Indonesia.

Berdasarkan data Laporan Tahunan Keamanan *Cyber* Nasional, jumlah kasus terhadap individu dan etintas di Indonesia meningkat dalam beberapa tahun terakhir. Berbagai macam serangan seperti *phising, malware,* dan *cyberbullying* menjadi ancaman yang nyata bagi para pengguna media sosial utamanya bagi pengguna yang kurang memiliki kesadaran *cybersecurity* yang memadai.

Dalam konteks global, Indonesia termasuk dalam daftar negara dengan tingkat keamanan siber yang perlu diperhatikan. Menurut laporan *Cybersecurity ventures*, Indonesia menduduki peringkat ke-10 sebagai negara dengan jumlah siber terbanyak di dunia. Hal ini menunjukkan urgensi terkait bagaimana meningkatkan kesadaran *cybersecurity* pada pengguna media sosial di Indonesia agar dapat merespons dan mengurangi resiko yang dapat mengancam keamanan digital pada masyarakat.

Sehingga, dengan memperhatikan kondisi yang telah dijelaskan, pengembangan strategi yang efektif untuk meningkatkan keadaran cybersecurity pada pengguna media sosial di Indonesia menajdi sangat penting. Pendidikan dan sosialisasi tentang bagaimana praktik *cybersecurity* yang aman, peningkatan pemahaman tentang resiko *cyber*, serta penguatan kesadaran akan pentingnya perlindungan data pribadi setiap indovidu merupakan langkah awal yang perlu dilakukan untuk menciptakan lingkungan digital yang aman bagi semua.

## METODE

Penelitian ini menggunakan pendekatan studi literatur untuk mengumpulkan informasi yang relevan dan terkini mengenai *cybersecurity*, media sosial, dan praktik *smart and good citizenship*. Studi literatur memberikan landasan teoritis yang kuat dalam mendukung pembahasan mengenai strategi meningkatkan kesadaran *cybersecurity* pada pengguna media sosial di Indonesia.

## HASIL

### 1. Ancaman Cybersecurity

Bersumber dari [1] banyak macam ancaman yang dihadapi dalam *cybersecurity* diantaranya :

a. Ancaman Fisik
   Berupa adanya potensi kerusakan pada bagian fisik dari infrastruktur TI, seperti contoh pencurian perangkat keras, pusat data, serta fasilitas lainnya yang mengancam gangguan pada operasional, hilangnya data, hingga gangguan layanan

b. Ancaman Logikal
Serangan yang terjadi pada infrastruktur teknologi informasi melalui *malware. Malware* ini adalah sebutan bagi perangkat lunak yang berbahaya, seperti virus, worm dan trojan. Karena virus yang menempel pada suatu file dan dapat menyebar saat digunakan, worm menybear melalui jaringan dan trojan menyamar yang kemudian mengeksploitasi sistem.

c. Ancaman Operasional
Ancaman operasional ini muncul dari faktor-faktor internal dalam sebuah kelompok masyarakat. Kesalahan yang dilakukan manusia seperti konfigurasi sistem yang salah atau penghapusan data yang tidak disengaja, akan mengakibatkan kerugian. Maka perlu dilakukan pelatihan rutin kepada anggota untuk mencegah terjadinya hal tersebut.

**2. Tantangan *Cybersecurity* pada Pengguna Sosial Media di Indonesia**

Menurut Hasyim Gautama, terdapat sejumlah permasalahan terkait dengan strategi penguatan *cybersecurity* di lingkup nasional diantaranya 1) lemahnya pemahaman penyelenggara negara dalam security terkait dengan dunia cyber yang memerlukan adanya pembatasan penggunaan layanan yang letak keberadaan servernya di luar negeri dan perlu adanya *secured system*, 2) Legalitas penanganan penyerangan di dunia siber, 3) Pola kejadian cyber crime sangat cepat sehingga mengakibatkan hal ini sulit untuk ditangani, 4) Tata kelola kelembagaan cyber security nasional yang masih terbatas, 5) Rendahnya *awareness* atau kesadaran akan adanya ancaman *cyber attack* internasional yang melumpuhkn infrastruktur vital suatu negara, 6) Masih lemahnya industri nasional yang memproduksi dan mengembangkan perangkat keras atau hardware terkait dengan teknologi informasi yang merupakan celah yang dapat memperkuat maupun memperlemah keamanan dalam dunia siber. (4).

Menurut BSSN (Badan Siber dan Sandi Negara) dalam [2] menyatakan bahwa di Indonesia sepanjang bulan Januari sampai Oktober tahun 2023, sudah terjadi 361 juta anomali traffic yang terjadi. Data tersebut diperoleh melalui *National Security Operations Center* atau NSOC di BSSN. Anomali traffic tersebut terdapat 3 kategori teratas diantaranya *malware* sebanyak 42,79%, kedua *trojan activity* sebesar 35,40%, dan yang ketiga adalah information leak sebesar 9,35%. Menurut Achmadi (BSSN) menjelaskan bahwa pola kedepannya akan masih sama, yaitu ancaman berupa *Ransomware dan juga Advanced Persistent Threat* atau APT.

Ransomware adalah salah satu jenis *malware* (*malicious software* atau perangkat lunak jahat). Sementara APT merujuk para serangan siber yang canggih dan terstruktur. Dari serangan ini berdampak pada kerugian-kerugian. Kerugian itu antara lain reputasi yang hilang, hilangnya keuangan, hak property intellectual dicuri dan menurunnya kepercayaan publik. *Malware* juga merupakan ancaman yang serius bagi pengguna media sosial, karena malware dapat disebarkan melalui tautan berbahaya atau file yang dikirimkan melalui pesan langsung atau komentar. Hal ini apabila pengguna tidak waspada dapat dengan mudah terinfeksi dan mengalami kerugian seperti kehilangan data penting atau bahkan yang lebih berbahaya adalah kehilangan kontrol atas akun sosial media mereka.

Selain itu tantangan yang dihadapi oleh pengguna sosial media adalah penyebaran informasi palsu atau hoaks. Dalam lingkungan media sosial yang cepat dan mudah tersebar, informasi yang tidak valid ataupun disengaja dapat dengan mudah viral dan memengaruhi persepsi publik, sehingga para pengguna harus lebih kritis dalam memverifikasi informasi sebelum menyebarkannya sebagai upaya pencegahan tersebarnya berita palsu atau informasi yang tidak benar. Menyadari tantangan ini pengguna media sosial perlu meningatkan kesadaran akan keamanan siber dan mengambil langkah-langkah yang tepat sebagai bentuk tindakan preventif terhadap tantangan yang terjadi.

Kemudian apabila berbicara mengenai tantangan dalam penguatan *cyber security* yang dihadapi oleh pemerintah dalam menghadapi *cyber crime* diantaranya adalah tidak cukupnya tenaga ahli teknologi dan ahli teknis keamanan untuk merancang dan melaksanakan *cyber security*. Sehingga akibat dari hal tersebut adalah membuat

negara dengan strategi ketahanan *cyber security* yang lemah dapat menganggu *cybersecurity* negara-negara lainnya. Penggunaan alat anonimisasi misalnya untuk memblokir *chain currencies* atau enkripsi, dalam kejahatan yang menggunakan internet semakin mempersulit pembuatan kebijakan.

Munculnya teknologi dan sistem baru dari waktu ke waktu memerlukan pemutakhiran sistem pengawasan yang dilakukan secara berkala. Bentuk *cybercryme* baru seperti ransomware, pencurian identitas, pendekatan seksual *(grooming)* dan pelecehan seksual melalui ranah siber.

**3. Sikap Warga Negara**

Sikap warga negara dalam menghadapi serangan *cybersecurity* menjadi suatu hal yang sangat penting, karena apabila warga negara atau masyarakat acuh terhadap apa yang sedang terjadi utamanya di era digital *society 5.0* ini, maka akan berimplikasi terhadap keamanan dan kenyamanan dalam hidup berbangsa dan bernegara. Dalam [3] pelaksanaan untuk menjaga keamanan dari serangan *Cybersecurity* sebagai wujud *smart and good citizenship* dapat dilakukan dengan memahami nilai dasar bela negara, diantaranya :

1) **Cinta Tanah Air**
   Perasaan cinta tanah air ini tumbuh melalui hati yang paling dalam dari setiap warga negara terhadap NKRI yang beredasarkan Pancasila serta UUD NRI 1945, upaya yang dapat dilakukan untuk menumbuhkan cinta tanah air ini adalah dengan memiliki pengetahuan,potensi SDA dan SDM yang unggul.

2) **Sadar berbangsa dan Bernegara**
   Sikap cinta tanah air pada setiap warga negara perlu ditopang dengan adanya sikap kesadaran berbangsa pada diri setiap warga negara sehingga menciptakan nilai-nilai kerukunan, persatuan kesatuan.

3) **Setia kepada Pancasila sebagai Ideologi Negara**
   Dalam membangun kesetiaan setiap warga negara terhadap Ideologi Pancasila perlu memahami faktor-faktor yang mempengaruhi seperti :
   a.Penegakan disiplin
   b.Sistem demokrasi
   c.Menumbuhkan sikap taat hukum
   d.Pengembangan etika politik

4) **Rela berkorban untuk bangsa dan negara**
   Dalam membangun sikap rela berkorban untuk bangsa dan negara perlu memahmi berbagai macam aspek diantaranya :
   a. Konsepsi jiwa
   b. Semangat dan nilai juang 1945
   c. Tanggung jawab
   d. Moral dan konstitusi
   e. Mendahulukan kepentingan nasional

5) **Memiliki kemampuan awal bela negara**
   Diartikan sebagai sebuah kesiapan atau potensi yang dimiliki setiap warga negara untuk melakukan aksi bela negara sesuai dengan kemampuan dan bidangnya masing-masing.

6) **Semangat mewujudkan negara yang bedaulat, adil dan makmur**
   Dilandasi dengan tekat persatuan dan kesatuan dalam menciptakan cita-cita suatu bangsa. Dengan terus mengikuti perkembangan zaman dan tetap selektif terhadap apa-apa yang kita terima, merupakan salah satu bentuk upaya untuk mewujudkan negara yang berdaulat, adil, dan makmur.

Melalui pemahaman terhadap nilai-nilai dasar bela negara, mengarahkan kita untuk bagaimana seorang warga negara bersikap, karena seiringnya perkembangan ilmu pengetahuan dan teknologi di era sekarang, ancaman bukan hanya aspek militer saja, melainkan juga aspek non militer, utamanya di era society 5.0 ini yang menjadi tantangan utama adalah serangan *cuybersecuirity.* Sehingga dalam rangka menjaga keamanan baik dari ancaman internal, eksternal, baik militer maupun non militer, perlu adanya sikap untuk mempertahankan negara dan menumbuhkan kesadaran bela negara teruatama kepada generasi milenial saat ini

**4. Strategi Peningkatan *Cybersecurity* pada Pengguna Sosial Media**

***1. Capacity Building***

Program pelatihan serta peningkatan mencakup upaya untuk meningkatkan kemampuan dan keterampilan dalam melindungi sistem informasi dari serangan siber. Hal ini melibatkan pelatihan, pendidikan dan pengembangan sumber daya manusia (SDM) yang memiliki keahlian dalam bidang keamanan siber. Dengan adanya capacity builiding, organisasi dan individu dapat lebih siap dalam menghadapi ancaman keamanan siber yang semakin kompleks dan berkembang.

**2. Peningkatan Sumber Daya Manusia**

Peningkatan SDM dalam keamanan siber merupakan langkah penting dalam memperkuat pertahanan terhadap serangan siber. Hal ini peerlu melibatkan pengembangan keterampilan teknis dan pemahaman yang mendalam tentang resiko keamanan siber. Melalui pelatihan dan sertifikasi, SDM dapat menjadi ahli keamanan yang mampu mengidentifikasi, mencegah, serta merespons adanya serangan siber dengan efektif.

**3. Pembentukan Undang-Undang khusus Tindak Pidana Siber**

Pembuatan undang-undang khusus yang mengatur tindak pidana siber menjadi hal penting dalam memberikan landasan hukum yang jelas dan tegas terhadap pelaku kejahatan di dunia maya. Undang-undang ini perlu menyertakan sanksi yang tegas agar dapat memberikan efek jera bagi pelaku kejahatan siber. Sehingga masyarakat dapat merasa lebih aman dalam beraktivitas di dunia digital.

**4. Kerjasama dalam Keamanan Siber**

Kerjasama antar berbagai lapisan seperti pemerintah, sektor swasta, lembaga internasional, dan masyarakat adalah kunci dalam meningkatkan keamanan siber secara menyeluruh. Dengan saling berbagi informasi, sumber daya, serta pengalaman, pihak-[ihak terkait dapat bersinergi dalam mengatasi ancaman keamanan siber yang bersifat lintas batas. Kerja sama juga memungkinkan adopsi praktik terbaik dan inovasi dalam menghadapi keamanan siber yang terus berkembang.

**5. Pencegahan *Malware***

Dengan melindungi perangkat setiap individu maka hal yang dapat dilakukan adalah dengan menginstall perangkat lunak keamanan yang terpercaya, menghindari tautan atau lampiran yang mencurigakan dan dengan tidak menginstall aplikasi dari sumber yang tidak dikenal.

.

## SIMPULAN

Seiring dengan zaman yang terus berkembang, utama pada ranah digital Dimana pada saat ini telah memasuki era *digital society 5.0*. Tentunya banyak dampak yang terjadi dari kemajuan di bidang teknologi ini, baik dampak positif maupun dampak negatif. Namun tentunya semakin berkembangnya zaman, tantangan dan ancaman yang dihadapi oleh masyarakat dalam konteks digital juga semakin meningkat. Sehingga perlu adanya sikap warga negara yang baik dan cerdas tentunya untuk menghadapi berbagai tantangan dan ancaman yang terjadi. Seperti *cyberbullying* yang kian marak terjadi, ancaman fisik, logikal, dan operasional yang menyangkut data diri pribadi individu yang akan berakibat fatal apabila disalahgunakan sehingga dapat merugikan banyak orang utamanya individu tersebut. Dalam menghadapi ancaman tersebut tentunya perlu berbagai upaya yang dilakukan dengan cara *capacity building*, peningkatan SDM, pemebntukan UU yang mengatur tentang tindak pidana siber, dan melakukan kerja sama keamanan siber. Berbagai upaya tersebut dapat dilakukan dengan baik apabila berlandaskan nilai-nilai bela negara, karena bela negara merupakan sikap untuk bagaimana bukan hanya mempertahankan bangsa dan negara tetapi juga keamanan setiap individu.

## DAFTAR PUSTAKA

[1] B. D. H. D. P. N. F. S. Arfan Dwi Madya, "Keefektifan Metode Proteksi Data dalam Mengatasi Ancaman Cybersecurity," *INDOTECH Indonesia Journal of Education And Computer Science,* vol. 1, pp. 127-135, 2023.

[2] D. W. A. I. Eko Budi, "Strategi

Penguatan Cyber Security Guna Mewujudkan Keamanan Nasional di Era Society 5.0," *Prosiding Seminar Nasional Sains Teknologi dan Inovasi Indonesia*, vol. 3, pp. 223-234, 2021.

[3] I. Y. M. S. A. I. T. Erva Yunita, "Penerapan Nilai-Nilai Bela Negara Dalam Menghadapi Tantangan Era Digital," *Jurnal Ilmu Hukum dan Tata Negara*, vol. 1, pp. 40-57, 2023.

[4] A. Aziz, "Pentingnya Pengetahuan Cyber Security Untuk Publik dan Negara," *Prosiding SAINTEK : Sains dan Teknologi*, vol. 2, 2023.