

# BAB I

## PENDAHULUAN

### 1.1 Latar Belakang Masalah

Di era milenial saat ini, marak dijumpai perkembangan teknologi dengan berbagai inovasi terbaru. Dunia cyber yang dikenal dengan istilah dunia internet, juga mengalami perkembangan teknologi yang sangat pesat dan tersebar luas di masyarakat. Perkembangan dunia cyber menjadi fenomenal ketika teknologi cyber dapat diakses dengan mudah oleh berbagai kalangan masyarakat melalui berbagai perangkat telekomunikasi seperti komputer dan telepon seluler. Banyak hal positif dari dunia cyber yang dapat diperoleh para penggunanya, seperti kemudahan berinteraksi jarak jauh, memperoleh informasi dan mengikuti perkembangan zaman. Namun, dibalik sisi positif dari dunia cyber, ada sisi negatif berupa kejahatan yang disebabkan oleh oknum yang tidak bertanggung jawab. Kejahatan di dunia cyber ini dikenal dengan istilah *cyber crime*.

*Cyber crime* adalah perbuatan yang melanggar hukum dengan memanfaatkan teknologi komputer yang berbasis kecanggihan perkembangan teknologi internet. *Cyber crime* umumnya dilakukan melalui media perantara gadget dan internet. Banyak sekali jenis *cyber crime* termasuk merusak data di internet dan gadget. Efek dari *cyber crime* ada bermacam-macam, antara lain rusaknya data di gadget dan internet, pengintaian data pribadi, ancaman virus dan hilangnya data-data penting di gadget maupun di internet. Salah satu berita *cyber crime* yang cukup menggemparkan dunia baru-baru ini adalah tentang serangan *Ransomware* yaitu sejenis *malware* yang mengganggu keamanan data di komputer dan meminta tebusan ratusan dollar hingga lima ribu dollar untuk pemulihan datanya. Bapak Rudi Lumanto - Ketua ID-SIRTII/CC, sebagai lembaga pengawas keamanan jaringan telekomunikasi berbasis protokol internet, menginformasikan hasil pengamatan Symantec tentang distribusi serangan *ransomware* di Asia Pasifik selama tahun 2016, Indonesia berada di tingkat ke-13 dengan jumlah serangan *ransomware* sebanyak 14 kali setiap harinya. Dengan asumsi jumlah serangan *ransomware* dan nilai tebusannya tersebut, maka kerugian masyarakat Indonesia pengguna internet yang menjadi korban *ransomware* mencapai nilai lebih dari lima juta dollar atau setara dengan 60 milyar

rupiah per hari. ID-SIRTII/CC juga mengabarkan bahwa serangan *cyber* Indonesia yang berpotensi menjadi kejahatan *cyber* beragam jenisnya. Pada tahun 2016, ID-SIRTII/CC mencatat jumlah serangan jaringan di Indonesia mencapai 135,6 juta baik yang termonitor langsung maupun tidak langsung. Pada tahun yang sama, akses *traffic malware* di *host* yang ada di Indonesia angkanya sudah lebih dari lima milyar.

Di Indonesia, kasus *cyber crime* cukup banyak dan sudah lama terjadi, bahkan saat ini jaringan *cyber crime* internasional pun sudah masuk di Indonesia. Direktorat Reserse Kriminal Khusus Polda Metro Jaya memberitakan bahwa dari 1.627 kasus pidana yang ditangani pada tahun 2016, sebanyak 1,207 atau 74% adalah kasus *cyber crime* (Detiknews.com, 30 Desember 2016). Namun hal tersebut hanya menjadi perhatian beberapa pihak terkait dan kalangan intelektual yang bergelut di bidang *cyber* serta memahami teknologinya. Masyarakat awam sebagai pengguna *cyber* di Indonesia umumnya tidak memahami adanya kejahatan *cyber*, tidak mempermasalahkannya dan tidak mengetahui tindakan apa yang harus dilakukan jika menemui kasus tersebut. Padahal di dunia internasional kasus tersebut merupakan kasus terbesar dan menjadi sorotan publik. Kesadaran masyarakat terhadap *cyber crime* masih sangat rendah. Masyarakat awam jarang menggunakan perangkat lunak anti virus, tidak melakukan *back-up* data dan tidak cermat dalam penggunaan gadget. Jika komputer mereka terinfeksi virus atau *malware*, masyarakat awam umumnya hanya memasang ulang perangkat lunak yang baru pada komputernya tanpa memedulikan datanya yang hilang.

Dengan maraknya kasus *cyber crime* yang seringkali tanpa disadari dialami oleh masyarakat awam dan minimnya pengetahuan masyarakat awam tentang *cyber crime*, maka kampanye sosial dibutuhkan sebagai salah satu upaya penanggulangan. Berbagai instansi dari kalangan Perguruan Tinggi, Menkominfo, hingga Kepolisian RI sudah mencoba melakukan sosialisasi tentang *cyber crime*, tetapi hasilnya dirasa masih kurang efektif untuk menjangkau masyarakat awam. Salah satu kelemahan program-program yang sudah ada, sosialisasi *cyber crime* tersebut hanya bisa diakses dan dipahami oleh kalangan tertentu yang berminat mendalami masalah *cyber crime*. Umumnya sosialisasi dan edukasi dilakukan melalui instansi-instansi, tidak langsung ke masyarakat. Informasi-informasi tersebut baru bisa diketahui jika masyarakat mengakses website terkait. Mengingat besarnya bahaya *cyber crime* dan terbatasannya informasi yang bisa menjangkau masyarakat awam, perlu kiranya dibuat kampanye sosial anti *cyber crime*.

Kampanye sosial anti *cyber crime* dapat digunakan untuk mengedukasi masyarakat awam dalam memahami bahaya *cyber crime*, jenis-jenis *cyber crime*, cara mencegah dan menanggulangnya serta mengajak masyarakat untuk menyatakan antipati terhadap *cyber crime*. Kampanye sosial ini bisa dipropagandakan melalui berbagai jenis media yang unik dan menarik, sehingga dapat menarik perhatian masyarakat awam.

## **1.2 Permasalahan**

### **1.2.1 Identifikasi Masalah**

- a. Tingginya angka kejahatan *cyber* di Indonesia
- b. Kesadaran masyarakat terhadap kejahatan *cyber* masih rendah
- c. Terbatasnya informasi kejahatan *cyber* yang bisa menjangkau masyarakat awam

### **1.2.2 Rumusan Masalah**

Bagaimana cara merancang media informasi tentang *cyber crime* yang efektif untuk masyarakat awam di Indonesia

## 1.3 Ruang Lingkup

Ruang lingkup ini terdiri dari :

### 1.3.1 Apa

- Tingginya angka kejahatan *cyber crime* di Indonesia
- Kurangnya kesadaran masyarakat terhadap kasus kejahatan di dunia maya

### 1.3.2 Siapa

- Target audiensi adalah masyarakat awam pengguna internet antara umur 18-40 tahun di wilayah perkotaan.

### 1.3.2 Kenapa

- Kampanye tersebut dilakukan karena banyaknya kasus kejahatan *cyber crime* di Indonesia

### 1.3.2 Kapan

- Kampanye dilakukan pada tahun 2017.

### 1.3.2 Bagaimana

- Penyelesaiannya adalah dengan mengampanyekan anti *cyber crime* secara umum.

### 1.3.2 Dimana

- Kampanye dilakukan di Indonesia.

## 1.4 Tujuan Perancangan

Adapun beberapa tujuan yang ingin dicapai :

1. Mengampanyekan anti *cyber crime* kepada masyarakat secara meluas
2. Memanfaatkan media visual yang berisi himbauan tentang bahaya *cyber crime*
3. Mengenalkan lebih dekat bahaya *cyber crime* serta penanggulangannya kepada masyarakat

## 1.5 Cara Pengumpulan Data

Dalam mengumpulkan data, perancang menggunakan beberapa teknik untuk melengkapinya, yaitu :

### a. Studi Literatur

Dalam rangka menelusuri literatur serta menelaah studi yang ada pada perpustakaan, maka peneliti harus lebih dahulu mengenal perpustakaan secara lebih baik, termasuk sistem pelayanan, system penyusunan literatur dan klasifikasi buku yang dianut oleh perpustakaan tersebut(Nazir, 2005:93).

Data dan informasi diperoleh dari literatur pustaka serta visual. Literatur pustaka yang digunakan seperti buku artikel ilmiah,jurnal, fenomena yang terjadi dalam beberapa tahun ini di media massa dan situs internet yang berkaitan dengan masalah yang diangkat sebagai laporan tugas akhir.

### b. Wawancara

Wawancara lebih dari sekedar percakapan biasa, wawancara selalu ada tujuan “percakapan dengan suatu tujuan (*conversation with a purpose*)”. Pewawancara dapat mengarahkan pembicaraan sedemikian rupa untuk mendapatkan topik yang diminatinya, sekaligus mengarahkan diskusi ke arah yang diinginkan dengan mengajukan beberapa pertanyaan(Soewardikoen, 2013:20).

Wawancara dalam penelitian ini mengutip pendapat para ahli mengenai dampak dari *cyber crime* terhadap masyarakat serta antisipasinya. Sehingga, didapat beberapa data pendukung untuk nantinya akan ditemukan solusi yang tepat.

### c. Kuisisioner

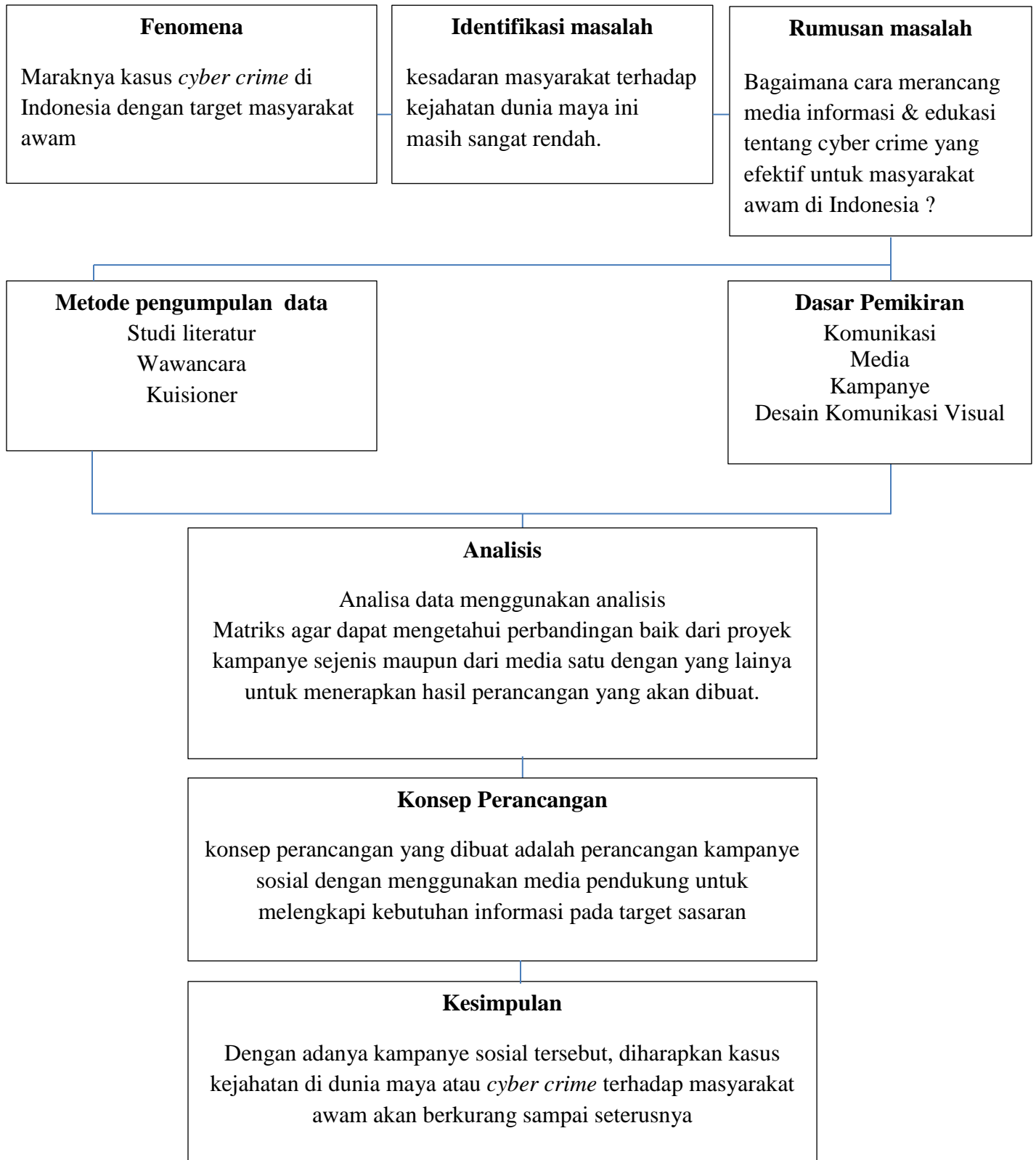
Kuisisioner adalah cara untuk memperoleh data dalam waktu yang relatif singkat karena banyak orang dapat sekaligus dihubungi. Pertanyaan sudah disiapkan terlebih dahulu, diarahkan ke suatu jawaban untuk dikuantifikasi (Soewardikoen, 2013:25).

Penulis membuat kuisisioner dengan responden masyarakat awam pengguna internet sebagai data untuk laporan tugas akhir.

#### d. Analisis

Analisis merupakan bagian yang amat penting dalam metode ilmiah, karena dengan analisis, data tersebut dapat diberi arti dan makna yang berguna dalam memecahkan masalah penelitian. Data mentah yang telah dikumpulkan perlu dipecahkan dalam kelompok-kelompok, diadakan kategorisasi, sehingga data tersebut mempunyai makna untuk menjawab masalah dan bermanfaat untuk menguji hipotesis(Nazir, 2005:346) Penulis menggunakan analisis matriks agar dapat mengetahui perbandingan baik dari proyek kampanye sejenis maupun dari media yang lainnya untuk menerapkan hasil perancangan yang akan dibuat.

## 1.6 Kerangka Perancangan



## **1.7 Pembabakan**

Penulisan karya Tugas Akhir ini terbagi menjadi lima bab, yaitu :

**BAB I** Pendahuluan berisi latar belakang permasalahan dari topik yang diangkat, permasalahan dari topik, ruang lingkup, tujuan dari perancangan, manfaat perancangan, metodologi perancangan, kerangka perancangan, sampai kepada pembabakan.

**BAB II** Dasar dari pemikiran untuk menjelaskan dasar dari teori – teori yang relevan untuk panduan di dalam perancangan.

**BAB III** Data dan analisis masalah berisi hasil pengumpulan data yang diperoleh dari studi literatur, wawancara, kuisisioner dan analisis.

**BAB IV** Konsep dan hasil dari perancangan mengungkapkan perancangan berupa konsep pesan, konsep pendekatan dan konsep media (media yang digunakan) untuk memecahkan masalah penelitian tersebut.

**BAB V** Penutup yang berisi dari kesimpulan dan saran.