HYBRID POLICING AS AN ALTERNATIVE MODEL OF POLICING AGAINTS CYBERCRIME IN THE INFORMATION SOCIETY

Kisnu Widagso* and Orisa Shinta Hariyani**

Abstract

I. INTRODUCTION

Rapid ICT development features one of many components that contribute to social change worldwide. Calder (2005) acknowledge ICT Development by increase in usages of distributed computing, mobile computing, internet, VoIP and broadband technology, computer literacy and computer prices which is becoming relatively cheap. Those mentioned above formed information as an important role in social, economy, culture and politics and shaped a new form of society, information society.[1]

Information become important resource within modern society, highly influential to political, social and economic changes and de-

* Dept. of Criminology, Universitas Indonesia, ** Police Science Studies, Universitas Indonesia

[1] see Tolica et al, 2015, page xix.

velopment. Emerging such new dynamics and complexity in society, moreover enhancement in volume and diversity of data and information processing, including widespread use of ICT concept that gave birth to information society. Information society is a new step in human civilization, a symbol of new way of life that involve intensive use of information in every aspect of human activity and existence with significant economic and social impact. [2]

In the course of information society, several features of change mentioned by Laudon and Laudon (2004), such as:

1. Emergence of global economy. Cost-effective demand, increase in profit and the need of global operation, consequently render a powerful information system as essential need to compete and survive in business.
2. Transformation of industrial economics to knowledge and information based service economics. Knowledge and information has become an important asset and basic foundation in providing services and products. Information system later be required in knowledge and information stream optimization within organization and resource maximization of knowledge and information resources.
3. Transformation of the business enterprises. Orientation shift from mass produced to mass customized with main orientation to customer satisfaction, alter information system's role importance in coordinating organization
4. The emerging digital firm. Capability in connecting and communicating between organization and every other element in business chain (supplier, customer, labor etc.) digitally constitute competitive power and able to open many opportunities. This is only possible with a great information system implementation.

On the other hand, another feature of information society that enable cybercrime, according to Strabe (2004) among others are :[3]

1. Security are annoyance. Safe situation can only be realized when each and every individual related to information system keeps on learning and understanding factors contributing to system failure. Surely, it's an exhausting process and understandable if not all of

[2] Vladoiu, 2014, page 9.

[3] See Strabe, 2004, page 2-4

the individuals willing to do so.

2. Features are rushed to the market. Vendors concentrate more on additional features from their ICT products in light of increasing functionality, while security aspects frequently ignored.
3. Vendors who spend time on security are eclipsed by competition. In relation to the uniqueness of IT market, consumers are more attracted to new products, even though its questionable security. IT Products such that tends to attract customers and set the market standards.
4. Computers and software evolve very quickly. Including network technology. In certain context IT products are designed while ignoring security aspects. While its generally used and popular in society.
5. Programmers can't accurately predict flaws. Software developed and deployed in different environment. When its deployed, software are vulnerable to millions of malicious actors' attack.
6. There's little diversity in the software market. Especially Operating System, there are only Windows or Unix. So, criminals can focus more on picking their target.
7. Vendors are not motivated to reveal potential flaws with many reasons. While on the other hand, hackers diligently together exploiting, discussing and designing threats against those weaknesses.
8. Patches are not widely deployed and can cause problems when they are installed. Not every users of information systems would patch up-date unless there's already victims. In the other hand, often problems occur later as bugs or decrease in system performance

Criminology's attention to cybercrime is relatively new. The massive amount of damage caused by this kind of crime has raised more attention on cybercrime since 1960s.[4] Since then, various attempts in identifying victims and harms, consequences of cybercrime, offender profiling and social control of such phenomenon, including its policing attempt.

Even today, there's no single generally accepted definition of cybercrime [5]in 2000 on Tenth United Nation Congress on the Prevention of Crime and the Treatment of Offenders in Vienna, cybercrime was

[4] Skinner & Fream, 1997.

[5] Kshetri,2010.

defined as crime acted with help of computer system or network within a certain system or computer network towards other system or computer network. Chin (2004) argues cybercrime is a crime utilizing computer network, especially the internet, in which can be done while sitting in front of a computer keyboard. While Rho (2007) defines cybercrime as crimes done using computers or computer networks as its main tool. Ngo & Paternoster also defines cybercrime as crimes committed through computer and or computer network.

Cybercrime is a unique typology of crime. At least two features of uniqueness of cybercrime, which are its crime target aspect and crime locus. Newman and Clarke (2003) explains cybercrime target within the frame of CRAVED – concealable, removable, available, valuable, enjoyable and disposable.[6]

Concealable refers to the condition of something's easily hidden in a pocket or bag. Hardly identified object or easily concealed object from others knowledge is a potential target. Criminals consider this aspect so it will be easily carried away, remove or sell. Within certain context, it is said that offenders can easily hid themselves from their victims or targets.

Removable means on certain conditions something can be removed from one place to another with ease will be a potential crime target, because:

1. Mobility of crime target because it is easy to remove or transferred from one location to another
2. Physical size of crime target which are compact, lightweight, small and space efficient.
3. Crime target is within the process of transference
4. Criminals have the opportunity or enough time window to move the target

Available refers to the concept of several aspects, such as:

1. Crime targets usually a new product or a new innovation which attract criminals and quickly creates illegal market.
2. Something considered as crime target if its accessible by potential criminals.

[6] Clarke, 1999 & Newman, 2009.

3. Something considered as crime target if it has visibility that leads to exposure to potential criminals

Valuable refers to a condition in which something potentially a crime target because potential criminals perceived it as something with high value. Current concept emphasizes not only on material value, but also cultural value within certain peer group.

Enjoyable, a concept that emphasize on something can be a potential crime target if its enjoyable, consumable or useable to the extent of potential criminal's life. While disposable means a certain condition when a potential crime target is something easily disposed (usually by selling it back to the market).

Locus of cybercrime is an environment known as computing environment, Newman & Clarke argue this particular environment has specific characteristics. Both explained that specific characteristics of computing environment leads to targeting of information system. Those specific characteristics are:

1. Stealth. Computing environment enables offenders to easily conceal their identity utilizing other's identity by various means or techniques.
2. Challenge. Computing environment brings out climate or a motivating culture towards potential offender to be able to outsmart information system's security measures undetected.
3. Anonymity. Computing environment enables offender to hide their identity, replacing and copying it by various means or techniques
4. Reconnaissance. Computing environment enables offender to pick targets by exploiting software or blending into an online community
5. Escape. Computing environment also enables offender to easily make their escape undetected and untraceable, frequently victims are unaware of such criminal act.
6. Multipliable. Computing environment enables offenders to automate and commit several different criminal act at the same time.

Subsequently, Newman add another concept, called networking, where enables offender to coordinate or in consort with certain groups or organizations to increase effectivity and ensure successful criminal act.[7]

[7] Newman, 2009, page 59.

Cybercrime phenomenon is unique, later considered requires an also unique reaction. In light of understanding that is impossible to expect reducing crime rate to a point of zero, accordingly policing attempts are directed towards crime control to an extent socially acceptable within general society. This is when cyber policing emerges. Many countries embodied cyber policing in a special unit tasked specifically for cybercrime cases. In general, there are several police functions, such as:

1. Related to main function of police as:
   - Law enforcement
   - Maintaining security and order
   - Crime prevention
   - Civil rights and freedom protection
   - Public services (Wrobleski & Hess, 2006, page 119)
2. Function directly related to contemporary demands for police to perform community policing and crime problem solving alongside general society in order to sort out crime problems, reduce fear of crime and crime prevention (Wrobleski & Hess, 2006, page 123)
3. Other function in relation with supplementary function such as recruitment, promotion, rotating and processing public complaints of police works (Siegel, 2011, page 166).

Considering unique characteristics of cybercrime, cyber policing unit also exploit ICT in performing their tasks and not all of them carried out by this particular unit. Within law enforcement context, police are official body to define violation of law, investigation and apprehension of criminals while assisting other bodies in criminal justice system in order to seek justice and enforce law. Generally, cyber units develop cyber forensics in order to perform their tasks.

On the context of public service, police constitute means to provide information, instruction, wisdom, counseling, vehicle license and registration, domestic interventions, traffic control and such. Furthermore, police also provide educational program on crime, drugs, safety and etc. (Hess, 2009). In many countries, although not fully implemented, in most cases cyber unit constitute, develop and maintain website accessible to public in order to inform and provide services covering their functions and responsibilities.

While in the context of crime prevention, police pose means of eradicating certain situations potentially criminal and or harmful. [8]Displaying themselves in patrols, rapport building with juveniles, working alongside the community and educating them. This is then known as cybercrime prevention programs or for specific issues also introduced certain prevention programs such as online child pornography. Within the context of maintaining security and order, police play role as means of intervention towards non-criminal act that may occur during public activities (i.e. crowds), social relationships (i.e. domestic disturbance) and traffic control. Furthermore, police also function as method of resolving civil disturbance and riot. On protection of civil rights and freedom, police are exemplary of human rights practice, especially in offender treatment. Respecting offender rights during investigation play essential role in preventing abuse of power and excessive force.

In Indonesia, police function constituted from the second (2nd) article of UU No 2 Tahun 2002 tentang Kepolisian Negara Republik Indonesia (POLRI, Indonesian Police Force). Mentioned in the 2nd article that police forces function as one of government function in maintaining public safety and order, law enforcement, protection, serve and public service. While definition and typology of cybercrime constituted in UU no 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (ITE, Electronic Information and Transaction). Several acts forbidden such as:

1. Illegal contents, including immorality, gambling, contempt or humiliation, threats and extortions (Article 27, 28 and 29 UU ITE)
2. Illegal Access (Article 30)
3. Data interference (Article 32)
4. System interference (Article 33)
5. Misuse of device (Article 34)

Based on UU No 11 tahun 2008 about Electronic Information and Transaction (ITE) then investigation, arrest, prosecution and punishment performed on cybercrime offenders and referring to UU No 2 Tahun 2002 about Indonesian Police Forces (POLRI), especially chapter 3, starting from Article 13 to 19, policing of cybercrime cases is fully acknowledged as domain and responsibility of Police Forces (POLRI). Data from cybercrime unit of Police Force Headquarters (Mabes POL-

[8] Hess, 2009.

RI) reported that since 2011 to July of 2014 there are 81 cases of UU ITE violation as describe below:

Table 1 : Cases of*Cyber Crime* 2011 - 2014

	2011	2012	2013	January – July 2014
Total	20	13	28	20

(Source: Cyber CrimeUnit Mabes Polri 2014)

Even though, it seems that crimes related with electronic transaction and information is far from decreasing, police haven't been able to handle this problem properly, data showed that, cited from kompas on April 2013, stated:

> *"...entirely, cybercrime cases in Indonesia achieve 520 cases ini 2011 and 600 cases next year, 40% of total is cyber fraud, consequently libel cases around 30% and the rest are hacking and other cybercrime cases"* [9]

Latest news coverage, on December 2015 stated:

> *"Cybercrime unit reported during 2012 there are 781 cases of cybercrime, only 86 of them closed on completion. In 2013, number of cases increased to 1.347 reports with number completion of only 115 cases. While in 2014 there were 1.324 reported cases with completion of 307 cases, as far as January to October 2015 there already are 1.325 reported cases while 255 of them already closed on completion."*[10]

This condition surely caused by several factors. Yar (2006) argue "*... the Internet has distinctive features that shape the crimes that take place in cyberspace. These features pose difficulties for tackling crime when approached by established structures and processes of criminal justice systems*" (Yar, 2006, page 16). Referring to Adler et al. (2009) other factors are:

1. *"It is difficult to police the Internet, and the necessary resources are not available to adequately handle this type of crime.*
2. *There is no public outcry against computer crime, since the public*

[9] *Kompas,* April 2013.

[10] http://nasional.kompas.com, December 19, 2015.

is more interested in violent crime.

3. *Finally, many police officers feel that they did not choose their profession to police computer crime, but rather to help people and arrest the criminals.*"[11]

Harnish also emphasize '*Cybercrime is complex and difficult for police to address through either traditional forms of policing or community policing*." [12]Based on explanations above, coincide with Rossmo when a crime can no longer be explained, offenders escaping punishment, including miscarriage of justice will bring criminal justice system to destructive situation.[13]

Crime, within this context cybercrime, has become one of emerging features of social change. This condition generally responded with or demands of different models of policing. Current attempts in policing of cybercrime cases, despite of adequate resources in information system and technology, seemingly ignoring specific characteristics of computing environment in information society.

Such ignorance resulting in weak formal social control on cybercrime, reflected on increasing number of cybercrime cases and huge numbers of unsolved cases, lack of trust in police forces, including economic and social cost that follows. So that it's important to formulate a unique model of policing – hybrid policing, a model of policing enhanced with information system and technology, support and collaboration from stakeholders, including victims.

II. RESEARCH METHOD

Current research utilizes qualitative approach while descriptively illustrating the problem and its analysis which systematically constructed around cybercrime policing problem in Indonesia. Data of current research collected through literature studies and mass media articles related to policing and also cybercrime cases in Indonesia. Official police

[11] Adler et al., 2009, page 284.

[12] Harnish, 2013, page 111.

[13] Rossmo, 2009, page 3.

crime statistics also used within current research. Then, analyzed through framework constructed from publication studies, such as scholarly journals and books. With the result that can describe problems in cybercrime policing, consequently offering alternative cybercrime models of policing, hybrid policing as research output. It is considered as an appropriate solution in policing of cybercrime, especially in Indonesia

III. RESULT AND DISCUSSION

A. POLICE, POLICING AND COMMUNITY POLICING

Referring to Button (2002) policing defined as "…,*however, is essentially a function of society that contributes to a particular social order that is carried out by a variety of different bodies and agents*" (Button, 2002, page 6). While Jones and Newburn(2006) defined policing as "*organized forms of order maintenance, peacekeeping, rule or law enforcement, crime investigation and prevention and other forms of investigation and associated information-brokering ... undertaken by individuals or organizations, where such activities are viewed by them and/or others as a central or key defining part of their purpose*."[14]

According to O'Brien & Yar (2008) policing is an act of regulating in order to monitor social behavior and ensure conformity in law and normative code. Policing can be informal and organized formally, involving social actors and institutions."[15]While Mawby (2008) defines*policing*as, "*..., a term we might apply to the process of preventing and detecting crime and maintaining order, is an activity that might be engaged in by any number of agencies or individuals...*"[16]

Kirby (2013) explain policing as a general process of crime prevention, crime detection and also order maintenance, which involve many institutions or individuals within (Kirby, 2013, page 4). Defining as "formal institutional forces whose responsible of law enforcement in the name of public and finally directed by and answered to government. So in this case, police force is a part of various institution which performs policing in every layer of society.[17]

[14] Jones and Newburn, 2006, page 3 – 4.

[15] O'Brien and Yar, 2008, page 122.

[16] Mawby, 2008, page 17.

[17] O'Brien & Yar, 2008, page 122.

In performing their responsibility, there are certain situations or factors that contribute to failure of police force in crime control. Kirby (2013) differentiate them into two factors, Internal and External Factors, such as: [18]

1. **Late modernity and the contemporary policing environment – keeping pace with change***,* police are unable to adapt its organization, governance, methods towards rapid changes in political, social, economic, technology, environmental and law within society.
2. **Partnership and plural policing**, police are unable to develop partnership network with other stakeholders in crime control, including emerging commercial agents, develop and paid to control crime.
3. **The role of the police and how they are measured**, police are considered fail to promote their role alongside society's development in need, demand and focus of crime control. On the other hand, that's exactly how police failure and success are measured.
4. **The emergence of stakeholders: politics, the media and other influences,** police's failure in establishing timetable and goals as the result of political pressure or interference, media and critical experts as emerging stakeholders.
5. **The operational environment and the conscious opponent,** failure in understanding characteristics, surrounding and community situations, including certain individuals within as locus and operational subject of police.

While internal factors, according to Kirby (2013), including:[19]

1. The police organizational culture and the use of discretion
2. The police leader
3. Choosing the correct intervention. Knowledge of 'what works;
4. The police practitioner – competence, knowledge and motivation

In order to achieve the ideal police, pointing to Wong (2012), the general framework includes:[20]

1. Making the police organization more rational (i.e. scientific, rule-

[18] See Kirby 2013, page 2 – 14.

[19] See Kirby, 2013, pp 14-21.

[20] See Wong, 2012, page 219.

bound, and results-oriented)
2. Making police personnel more qualified (i.e. educated, trained and specialized)
3. Making police services more professional (i.e. responsive, responsible, and competent)
4. Making police conduct more accountable (i.e. more open and better supervised)

Therefore, in Wong (2012) mentioned several measure can be done to achieve such standards, such as:[21]

1. Modernization of the concept of law enforcement (Police stakeholders considering more of social changes)
2. Data-driven policing (utilizing data and information as foundation of police conduct, nevermore only intuition, experience and coercive measures)
3. Integration of strike, prevention and control of crime strategies (integration of different approaches in prevention and law enforcement in order to control crime and maintaining order)
4. Standardization of police practices (institutionalized, rational and standard)
5. Standardization of expenditures and equipment (cost and equipment efficiency in rational police practice)
6. Regularization of police establishment (organization in ideology, recruitment, training, order and control to ensure accountability and professionality)
7. Scientific utility assessment (periodic and well-planned evaluation of policing practice based on scientific research and measures)

Adler defines community policing as a model of policing that is decentralized and has officers working with community members to increase feelings of safety in communities.[22] Referring to Siegel (2013) community policing can be defined as measures of adopting restorative justice into law enforcement. Restorative justice depends on the fact that criminal justice policy maker need to listen and respond needs of those affected by their decision and community policing defined as a

[21] See Wong, 2012, pp 223-224.

[22] Adler et al, 2009, page 163.

concept closely related to concept of order, problem solving community-based and redefining purpose of police force (Lab, 2014, pp 239)

Development of community policing as policing practice because community policing viewed and valued as an ideal form. Not only providing space for suggestions and attentions from society, but also actively involving then into policing practices, especially crime preventions. While empowering community through partnership in order to control crime and reduce fear of crime, aligning in perceptions of safety, order and improving quality of live and environment (Keppler & Gaines, 2011, pp 4) With several considerations mentioned above, starting from 2005, POLRI implement community policing as policy and strategy in performing their duty.

According to Siegel (2011) community policing include three important components such as community partnerships, organizational transformation and problem solving. **Community Partnerships** explains as collaborative partnerships between police institution and individuals or organizations in order to develop solutions and building trust. Extent and potential of this partnership is wide and can also function as means of reaching two related goals, which are solution development towards collaborative problem solving and increasing public trust. While involving community to be able and willing to play role in prioritizing and solving problem of security.

Organizational Transformation is required in order to align management in organization, structure, personnel and information system to support community partnership and proactive problem solving methods. It also encompasses implementation of modern management in the name of efficiency and effectiveity. Community policing emphasize on structural transformation in each and every aspect within its organization.

Problem Solving as process of systematically analyzing identified problems in order to develop and evaluate effective form of interventions. Community policing emphasize systematic and sustainable problem solving. Compared to responding crime when occur, community policing motivates police to proactively develop solutions to criminogenic factors in community. Innovative thinking in problem solving and varying in policing practice as one of many possible options available.

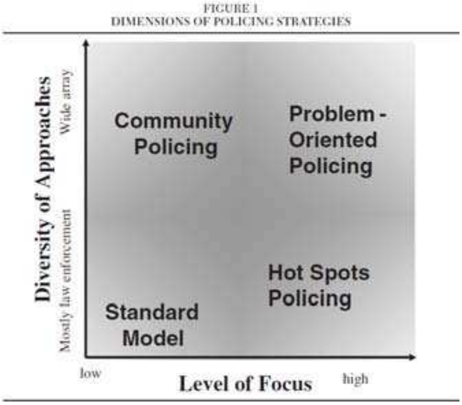
B. MODELS OF POLICING

Referring to Smelser dan Warner (1976) model defined as

"*..., is a construction of concepts, on the basis of which we make conditional predictions about what we expect to happen in the real world*". While according to Lave dan March (1993) "*A model is a simplified picture of a part of the real world. It has some of the characteristics of the real world, but not all of them. It is a set of interrelated guesses about the world*"[23]

Johnston (1992) utilize models of policing to differentiate police functions into three (3) types, **reactive force, proactive service** and combination of subsequent called **velvet glove and iron fist**.[24] While Weisburd and Eck (2004) apply the concept, models of policing, then distinguish four different dimensions of policing, based on diversity of approaches and level of focus, which are: **standard model, community policing, hot spot policing** and **problem oriented policing** in order to evaluate effectivity of mentioned models in crime and order control which illustrated as follows:

Picture 1 Dimensions of policing Strategies



(Source: Weisburd and Eck, 2004, page 45)

[23] Lave and March, 1993, page 3.

[24] See Johnston, 1992, pp 186.

C. HYBRID POLICING

Referring to existed literature, as a concept, hybrid policing was originally used by Johnston (1992) without any clear definition. Such concept was a chapter's title of his book, in order to illustrate existence of other government bodies or institutions, beside police, who also have responsibility and power to perform policing practice and law enforcement (Johnston, 1992, pp 116). Other bodies mentioned and identified are:

1. *Bodies engaged in functions related to state security*.
2. *Special police forces*.
3. *Departments of state*.
4. *Municipal bodies*.
5. *Miscellaneous regulatory and investigative bodies*. (see Johnston, 1992, page 116 – 118)

Button (2002), wrote citing Johnston (1992), define*hybrid policingas* "… *embraces all those public bodies (and some private bodies), other than the public police, which are engaged in policing*" (Button, 2002, page 10). While Manning (2014) define*hybrid policing* "… - *this includes all varieties of policing, i.e. noticing, responding to and, perhaps, sanctioning behavior*" (Manning, 2014, page 29 - 30).

Pakes (2010) apply hybrid policing concept realizing that this concept can overcome police (human resources) and private security (legitimacy) weaknesses. Pakes consider hybrid policing concept can be performed effectively (Pakes, 2010, pp 162-163). While de Guzman (2013) utilize hybrid model of policing in explaining model of policing for terrorism. Combining elements of community policing, such as community partnership, problem solving and geographic focus with elements of homeland security policing, like emergency response, preparedness, early warning devices and community mobilization. On the other hand, Parnell (2013) also defined hybrid policing as "*a hybrid form of policing that combines bureaucratic regimentation with the necessity of democratic self-governance*" (Parnell, 2013, page 209).

In light of involvement of other bodies in policing, even its not called hybrid policing, Vladiou (2014) identifies ideal role of parties involve in policing, that are:

1. The government and its institutions (stimulating and controlling behavior and transition process towards information society)
2. The business community (providing affordable high technology products and services)
3. The academic community (constructing framework to better understand phenomenon in information society while developing research and innovating technologies)
4. The civil society (play important role in formulating requirements and priorities of new technology usage in general society's interest while responding on government policy and regulation) (See Vladiou, 2014, page 10)

Hybrid Policing Model for Cyber Crime

According to Wall (1998) considering development of cybercrime resulting in emergence of various policing practice of internet users, internet service provider, state funded non-police organizations also state funded police organizations. Within certain part, Wall (1998) highlight policing practice of state funded police organization. He argues that what has been done is far from adequate in controlling cybercrime, as a result from lack of training and understanding on cybercrime phenomenon, discrepancy or contradiction in policies regulating cybercrime. With the result of pluralistic model of policing which combine elements of public and private models of policing.

Other attempts in defining ideal models of policing within the context of cybercrime, such as Haggerty and Ericson (1999) with military policing model emphasize police force to adapt military technology and method in order to control cybercrime. Kao & Wang (1999) highlight importance of digital footprint (i.e. IP Address, Timestamp) when investigating cybercrime cases, believed to play important role in police current failure in solving cybercrime cases. Jones and Newburn (2002) acknowledge changes in policing system spring from public policing reformation and development of private security industry that led to pluralization of policing.

On the other hand, Hues and Rosenberg (2004) suggest, in policing cybercrime, certain policy needs to be develop in order to provide authority to the police over ISP (Internet Service Provider) in collecting, investigating and prosecuting cybercrime offenders. Broadhurst (2006) also emphasize on partnership, in the context of international mutual legal assistance (MLA) in case of cybercrime policing. While Jones (2007) also emphasize on partnership, he argues that previously reactive investigative model needs to be replaced with community policing model, implementing through usage of open source software in order to supervise and deter cybercrime offenders.

In the context of role of certain institutions, actors or bodies, there were also several previous studies referring to this, such as Wall and Williams (2007) who highlight the importance of involving online communities in regulating and maintaining order within their domain while building virtual police service alongside conventional police service as form of de-monopolizing of police function. There's also research from Zhong and Grabosky (2009) resulted in public/private policing which combine roles of private security with public security police in China. While Levi and Willams (2013) acknowledge capability of policing bodies, including police force in controlling cybercrime, while promoting partnership between stakeholders in cybercrime prevention, called multi-agency partnerships.

In reference of previous studies, reviewed in table 2 below, basically, models of cybercrime policing generally constituted of only one or two factors. Ideally various factors identified should be taken to consideration in a balanced manner in developing model of policing, factors mentioned include:

1. Characteristics of cybercrime
2. Characteristics of social change
3. Weaknesses in policing institution, especially police
4. Policing orientation or goal
5. Current models of policing

Table 2

Summary of Previous Studies on Cyber Crime Models of Policing

Researchers/ Writers	Elements					Model of Policing Offered
	Cybercrime Characteristics	Information Society Characteristics	Policing Institution Weaknesses	Policing Orientation or Goal	Current Models of Policing	
Wall (1998)			V			Pluralistic model of policing
Haggerty dan Ericson (1999)		V	V		V	Military/ policing model
Kao dan Wang (1999)			V	V		IP address&time stamp
Palfrey (2000)			V	V		Extending Authority
Huey dan Rosenberg (2004)			V	V		Extending Authority
Broadhurst (2006)	V		V	V		mutual legal assistance (MLA) Improvement
Jones (2007)			V		V	Virtual Neighborhood Watch
Wall dan Williams (2007)		V	V			Virtual police service.
Tetzlaff-Bemiller (2011)			V		V	Undercover online.
Liang dan Lu (2012)	V		V			Campaign-style policing.
Levi dan Williams (2013)		V	V			Multi-agency partnerships
Leukfeldt, Veenstra, dan Stol (2013)			V			Institutional Enhancing.

(Source: Researcher's Summary)

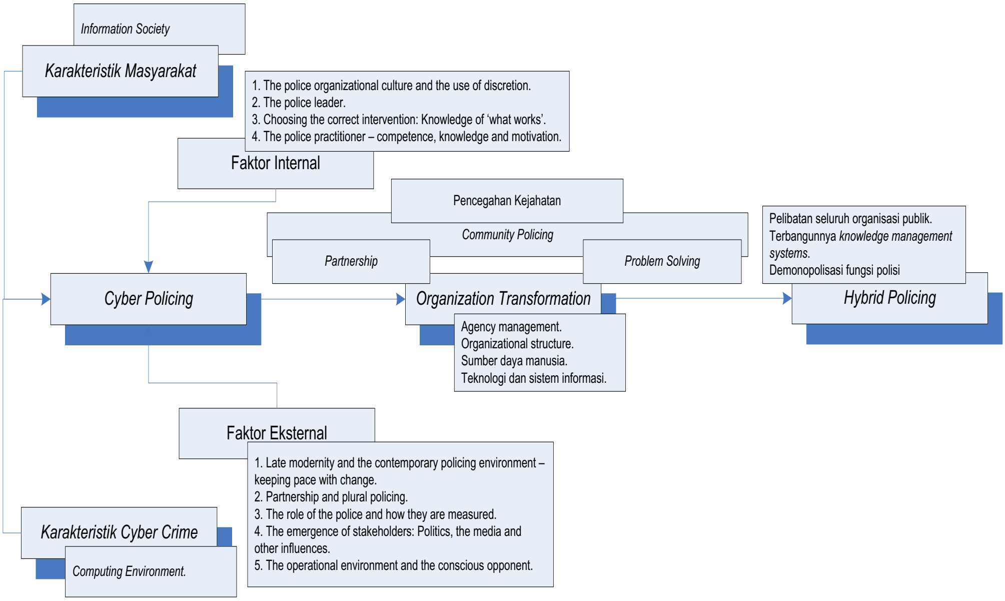
One of methods in model building or modelling is system dynamics. Modelling with system dynamics basically used to understand complexity of feedback systems, where objects within interact one with another in a causal relationship. System dynamics utilized in constructing or modelling basic structure of a system in order to understand and constitute sustainable structure.[25]

Newsome (2008) wrote that in order to build a model using system dynamics modelling, then what needs to be done are:

1. Formulating goals of modelling, in this case explaining failure of current cybercrime policing and constructing a new model of policing for cybercrime
2. Identifying key concepts and variables in order to draw the system, including cause-effect relationships involved
3. Identifying relationship between factors constitute police failure in cybercrime social control so that its able to understand current model of policing in cybercrime context.

Picture 2

Research Framework


Information Society
Karakteristik Masyarakat
1. The police organizational culture and the use of discretion.
2. The police leader.
3. Choosing the correct intervention: Knowledge of 'what works'.
4. The police practitioner – competence, knowledge and motivation.
Faktor Internal
Pencegahan Kejahatan
Community Policing
Partnership
Problem Solving
Pelibatan seluruh organisasi publik.
Terbangunnya knowledge management systems.
Demonopolisasi fungsi polisi
Cyber Policing
Organization Transformation
Hybrid Policing
Agency management.
Organizational structure.
Sumber daya manusia.
Teknologi dan sistem informasi.
Faktor Eksternal
1. Late modernity and the contemporary policing environment – keeping pace with change.
2. Partnership and plural policing.
3. The role of the police and how they are measured.
4. The emergence of stakeholders: Politics, the media and other influences.
5. The operational environment and the conscious opponent.
Karakteristik Cyber Crime
Computing Environment.

(Source: Researcher's Summary of Various Resources)

[25] Newsome, 2008, pp 166.

Hybrid policing model acknowledge unique characteristics of cybercrime, which already explained above by Newman and Clarke (2003) where its crime locus is computing environment while social changes constitute information society as explained by Laudon and Laudon (2004) and Strabe (2004) including police weaknesses as identified and summarized by Kirby (2013).

Model of policing needs orientation or goal as reference and it is believed within this research crime prevention is the appropriate one. Crime prevention needs to be emphasized in contemporary society today. Reckoning Siegel (2012) noted that law enforcement alone can never control crime rate, potentially conflicting even trigger lack of trust.[26] Waller (2010) believe in crime prevention in terms of reducing crime rate up to 50% within 10 years.[27] While reflecting back to early 19th century where policing was originally performed in order to prevent crime.[28]

IV. CONCLUSION

When it comes to model of policing oriented in crime prevention, then community policing become highly relevant. Because of its valued as an ideal form of policing. Not only disclosing space for aspiration and attention from community, but also involving community itself within policing practices, especially crime prevention and empowering society while building trust and partnership with police as a crime control system and overcoming fear of crime, aligning perception on disturbance in security and order, at the same time, improving quality of life and environmental condition. [29] So that transformation in models of policing should in line with the concept of community policing. Where finally hybrid policing should lead to changes with features, such as:

1. Involvement of public organizations and its elements as explained by Johnston (1992)
2. Constitution of Knowledge Management System utilized in build-

[26] Siegel, 2012, pp 583.

[27] See Waller,2010, pp 218.

[28] See Gilling, 1997, pp 76; Schnider, 2015, pp 329.

[29] Kappeler and Gaines, 2011, pp 4.

ing partnership and problem solving, and

3. De-Monopolization of Police function and responsibilities.