PhD Viva Voce Presentation

By

Paul Asante Danquah

TOPIC:

An Assessment of Cyber Criminal Behavioural Patterns

Purpose of Research

To better understand the phenomena of cyber crime and the behavioural patterns of cyber crime perpetrators as a means of addressing the problem.

Research Problem

Problem Situation

US Internet Crime Report 2001- 2011: Shows consistent increase in number of reported cyber crimes (Fig1.1 and 1.2)

Silke and Demetriou's (2003): Considerable concerns were raised about crime and deviancy on the Internet

The Information Economy Report 2005 by UNCTAD emphasized that Cyber crime deter the use of the Internet in developing countries to increase commerce, investment, innovation, productivity and efficiency.

Srinivasan (2008): The potential for harm can be significant regardless of the offence that is committed

Brenner (2004): A model approach is needed to address cyber crime activities which are on the increase

Longe (2009) : As more people become aware of, and exposed to, a range of opportunities to commit various illegal and socially questionable behaviours, the total number of cyber crimes is very much likely to increase in number.

Research Work Done

Turvey (2002): Need for Cyber Criminal Profiling, based on Behavioural Evidence

Wilson (2006): "understanding the steps in the process of committing crime, and understanding the conditions that facilitate its commission, helps us to see how we can intervene to frustrate crime"

Stanley (2006) : Identifies behavioral based protections and justifies their relevance and usefulness in detecting and blocking attacks on websites that are based on Web 2.0 technologies and architecture.

Jaishankar (2008): Proposed theory to depict behaviour but insisted it requires further testing

Research Problem

Need to Address Problem

Pladna (2009) : Need to secure Machines

Jahankhani and Al-Nemrat (2010): confirm the challenges in determining behavioural patterns of cyber criminals and the tools they use.

Nigel Stanley (2006): Need for behavioral based protections and justifies their relevance and usefulness

Peter Firstbrook (2007) and Robert Clyde Symantec CTO (2004): Emphasized need for behavioural based blocking

GAP: How to proactively determine the behavioural patterns of cyber crime perpetrators

Annual Increase in Reported Crimes
Fig 1.1 (IC3)

Annual Increase in Financial Loss
Fig 1.2 (IC3)

Signature Based Blocking not Effective

Breach of Existing Counter Measures

Experts' Concern of Gap in Behavioural Based Blocking

Significance of Study

Unique contribution to understanding the phenomena of cyber crime as a means of addressing the problem via the ability to determine behavioural patterns ;

No	Finding	Implication
1	**Behavioural Patterns of Cyber Deception and Theft Perpetrators**	Relevant to Practitioners in Profiling, Researchers to improve counter measures and Policy Makers makers to control activities
2	**Behavioural Patterns Cyber Trespass Perpetrators**	Relevant to Practitioners in Profiling, Researchers to improve counter measures and Policy Makers to control activities
3	**Behavioural Patterns Cyber Violence Perpetrators**	Relevant to Practitioners in Profiling, Researchers to improve counter measures and Policy Makers to control activities
4	**Behavioural Patterns Cyber Pornography Perpetrators**	Relevant to Practitioners in Profiling, Researchers to improve counter measures and Policy Makers to control activities
5	**Empirically Tested Space Transition Theory**	Relevant for Researchers to extend theory

Proposed models to counter: 1. Socially Engineered Cyber Deception and Theft
2. Cyber Trespass

- **Research Findings could be used as a basis for extending Space Transition Theory if successfully replicated and Proposed Models could be used by practitioners to develop off the shelf solutions to prevent cyber criminal activities**

Literature Review

Theories

Routine Activity Theory
Cohen and Felson (1979)

Generic Crime Theory applies to Cyber Crime

Space Transition Theory
Jaishankar(2008)

Proposed Behavioural Pattern for Cyber Criminals is relatively new

Crime Displacement Theory
Cox, Johnson & Richards (2009)

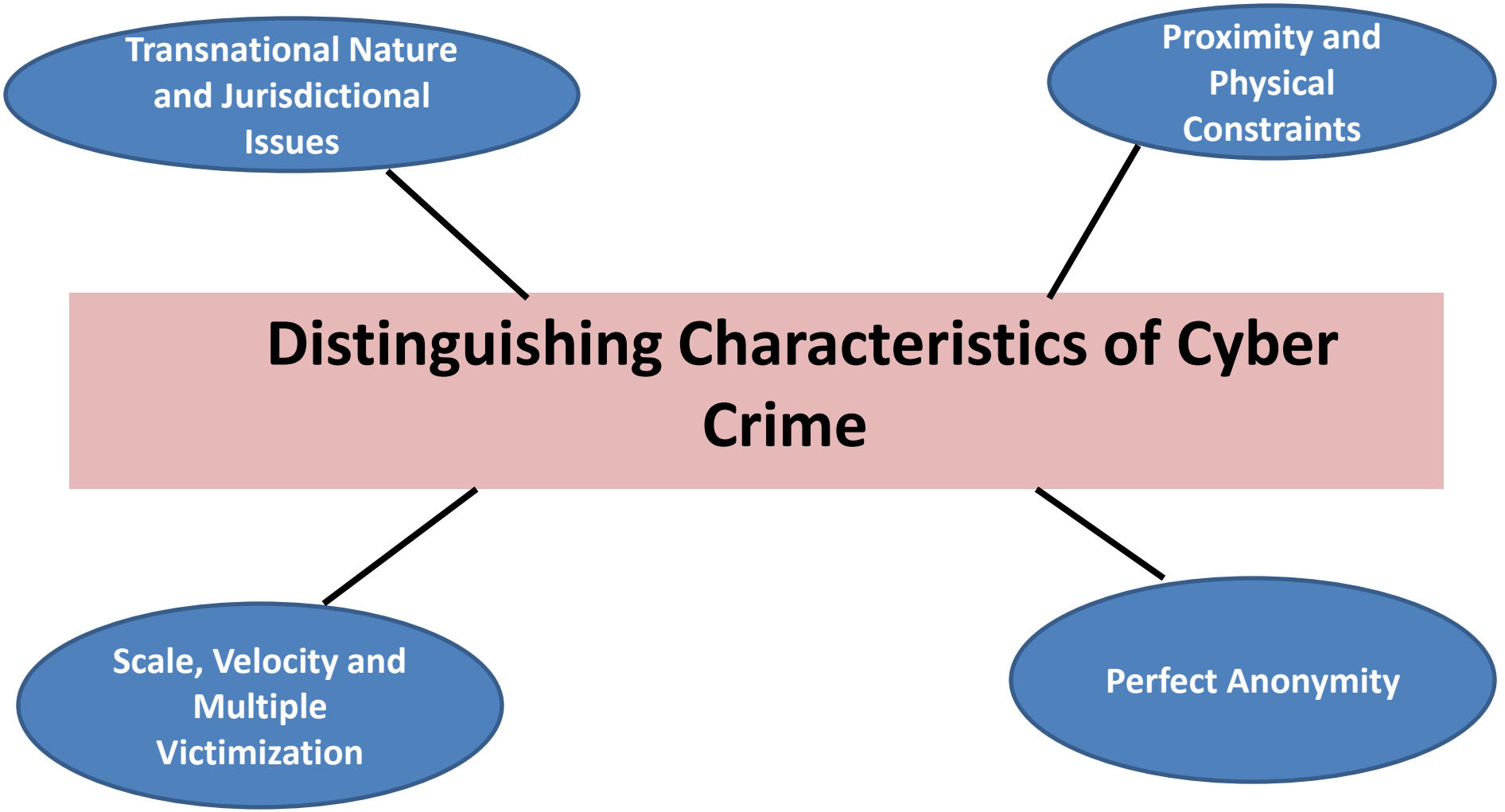
Objective Theory for Crime Prevention

Distinguishing Characteristics of Cyber Crime
Brenner(2004)

Not a Theory, however an Important Contribution to knowledge of Cyber Crime Characteristics

Literature Review

Brenner 2004a: McConnell International 2000



Literature Review

Industry Experts' Perspective

"The evolution of the threats has made protection based on **behavioral detection techniques indispenseable**" - Frost & Sullivan AV report 2006

"Based on signatures, anti-virus software is dying - we need **Behavior-based Interception**," John Pescatore, Gartner Analyst at Network World (2005)

"Traditional signature-based products can no longer protect companies from malicious attacks. Vendors must execute product and business strategies to meet the new market requirements for broader malicious code protection." - Gartner, February 2005 Magic Quadrant

"Reactive, signature-based protection is becoming less effective. The time from software patch to exploit is dropping below the time needed for companies to install the patch. Even if you start when the patch is released, most IT departments will take 30 days to test and patch a system and hackers are faster than that now. Therefore we need more proactive security",…"**behavior-blocking looks promising**", Robert Clyde, Symantec CTO, Vnunet.com (2004)

Literature Review

Confirmation of Knowledge Gap

The history, theories and current empirical evidence of cyber crime shows that the cyber threat is one of the most serious socio-economic and security challenges that the world faces today and there is also an inherent lag between social responses and innovative technologies, this calls for proactive strategies that can help determine behaviour and prevent cybercrime from occurring in the disjoints between social and technical systems.

Methodology

Philosophy

Realism

Approximation of Reality

Interpretivism

Truth is Subjective

The **rationale** for using this philosophy is because this research requires gaining direct experience with the setting to ascertain true behavioural patterns

Realism involves forces that are not directly observable or measurable to provide the general context for social behaviour.

Interpretivism on the other hand explains social phenomena behaviour and requires an understanding of the meanings that the social actors involved bring to the situation (Amory 1999).

Methodology

1. Approach :
Deductive and Inductive
Test of Space Transition Theory (Deductive)
Development of Model (Inductive)

2. Fact Gathering Method:
Primary & Secondary

3. Instrumentation:
Observation, Interviews, and Experimental Case Study (Website)

4. Sampling:
Convicted Culprits: 8 , Non-Convicted Culprits: 8, Victims of Cyber Crime, 8, Law Enforcement Agencies: 9, General Public: 42

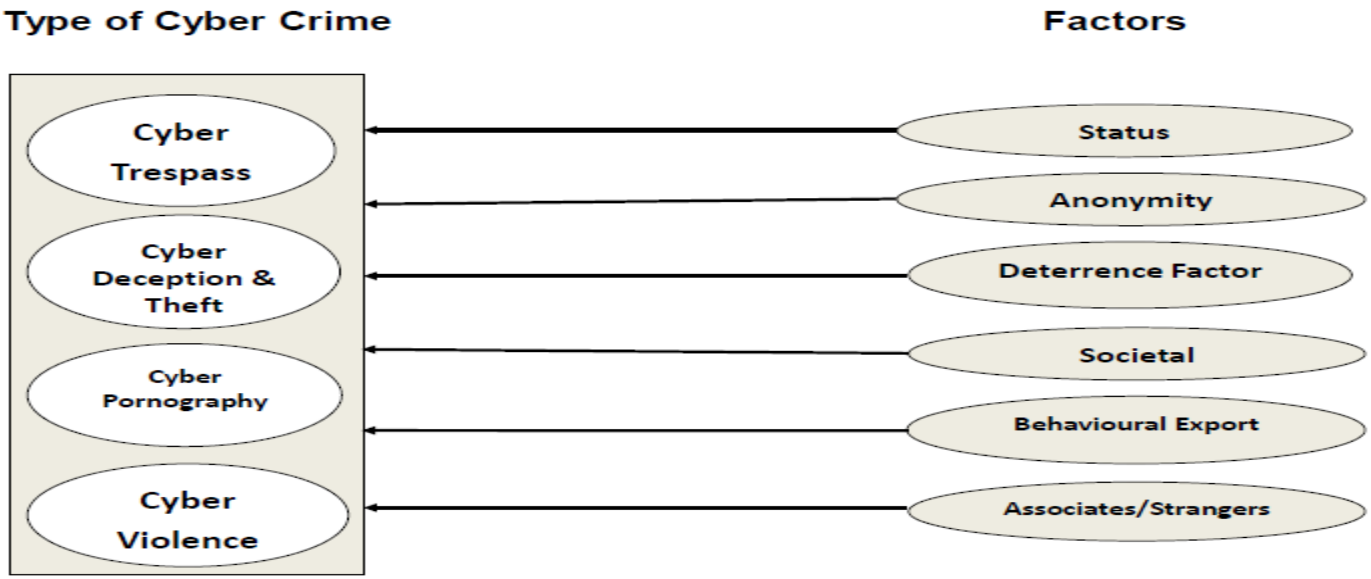
5. Analysis: Qualitative and Quantitative

6. Evaluation:
Relevance and Rigour

Methodology

Driving Theory and Variables

The Space Transition Theory is the driving theory that was employed as a framework for data collection and analysis. The under listed were variables used in the research.



The variables were derived from Yar's (2005) categorization publication and Jaishankar's (2008) STT

Methodology

Validity and Reliability

Validity: Review of Fact Finding Approach by specialists and peers (through publication)

- Danquah P. & Longe, O.B (2013). Towards a Framework For Evaluating Behavioral Patterns of Cyber Criminals. Proceedings of the iSTEAMS International Multidisciplinary Conference, Conference Centre, University of Ibadan, Ibadan, Nigeria pp 217 – 226

Reliability: Multiple Data Collection methods from same source

- **Convicted Culprits: Interview and Court Proceedings**
- **Non-Convicted Culprits: Interview and Observation**
- **Law Enforcement Agencies: Published Records and Interviews**
- **Victims: Interview and Documentary Evidence**
- **Multiple Tools for Data Gathering on Website (AwStats, Webalizer,SDT)**

Methodology

Data Analysis

No	Research Question	Analysis Method	Reasons
1	Do persons, with repressed criminal behaviour (in the physical space) have a propensity to commit crime in cyberspace, which, otherwise they would not commit in physical space, due to their status and position.	Ethnography, Content & Conversation Analysis	Most Ideal to determine influence of status on behaviour
2	Does identity flexibility, dissociative anonymity and lack of deterrence factor in the cyberspace provide the offenders the choice to commit cyber crime	Ethnography, Content & Conversation Analysis	Most Ideal to determine influence of identity on behaviour
3	Would criminal behaviour of offenders in cyberspace be imported to physical space which, in physical space may be exported to cyberspace as well.	Content & Conversation Analysis	Essential to confirm exportable behaviour
4	Do the intermittent ventures of offenders into the cyberspace and the dynamic spatio-temporal nature of cyberspace provide the chance to escape.	Descriptive Statistics and Content Analysis	Essential to confirm spatio temporal nature
5	Are strangers likely to unite together in cyberspace to commit crime in the physical space.	Content & Conversation Analysis	Most Ideal to determine evidence and possibility of occurrence
6	Are associates of physical space likely to unite to commit crime in cyberspace.	Conversation Analysis & Ethnography	Most Ideal to determine evidence and possibility of occurrence
7	Are persons from closed society are more likely to commit crimes in cyberspace than persons from open society.	Content Analysis	Most ideal due insufficient primary data collected

Results and Analysis

Summary of Data Collected

No.	Source	Sub Total	Total
1	**Cyber Criminals**		**16**
	- Convicted Criminals	8	
	- Non-Convicted Criminals	8	
2	**General Public**		
	- Total Number of Visitors	1,935	**1,935**
	- Total Registered	92	
	- Crime Related Registrations	42	
3	**Victims**	8	**8**
4	**Law Enforcement Agencies**		**9**
	- Police	8	
	- Prisons	1	
5	**Secondary Cases**	68	**68**

Results and Analysis

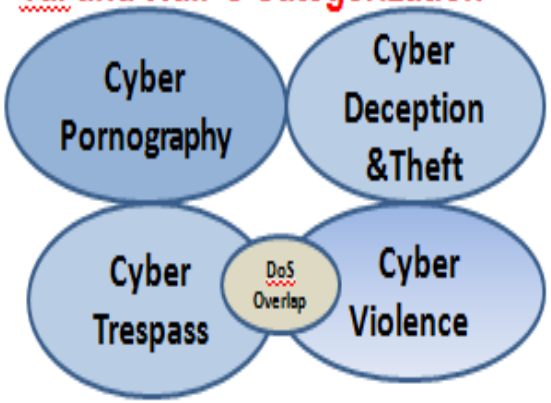
Research Questions, Analysis and Results

Question 1. What are the forms of Cyber Crime?
Approach: Reviewed Literature

Results

- **ITU Legislation**
  - Unauthorized Access to Computers, Computer Systems, and Networks
  - Unauthorized Access to Computer Programs, Computer Data, Content Data, Traffic Data
  - Interference or Disruption
  - Interception
  - Misuse and Malware
  - Digital Forgery
  - Digital Fraud, Procure Economic Benefit
  - Extortion
  - Aiding, Abetting, and Attempting
  - Corporate Liability

Yar and Wall 's Categorization



Question 2. What are the socio economic effects of Cyber Crime?
Approach: Reviewed Literature

Results

Type	Socio-Economic Effects
Cyber Trespass	•Loss of Revenue • Wasted Time • Damaged Reputations • Reduced Self Esteem
Cyber Deception and Theft	•Loss of Revenue • Wasted Time • Damaged Reputations • Reduced Self Esteem
Cyber Pornography	• Damaged Reputations • Reduced Productivity • Reduced Self Esteem
Cyber Violence	•Loss of Revenue • Wasted Time • Damaged Reputations • Reduced Productivity • Reduced Self Esteem

Results and Analysis

Research Questions, Test and Results

Question 3: Do the postulates of the Space Transition Theory form a reliable and viable basis for determining behavioural patterns of cyber criminals?

Approach : Postulates Transformed to Research Questions and Varied Methods of Analysis Used

No	Research Question	Analysis Method	Results of Analysis			
			CD&T	CT	CP	CV
1	Do persons, with repressed criminal behaviour (in the physical space) have a propensity to commit crime in cyberspace, which, otherwise they would not commit in physical space, due to their status and position.	Ethnography & Conversation Analysis	Positive Relationship	Positive Relationship	Positive Relationship	Positive Relationship
2	Does identity flexibility, dissociative anonymity and lack of deterrence factor in the cyberspace provide the offenders the choice to commit cyber crime	Conversation Analysis & Ethnography	Positive Relationship	Positive Relationship	Positive Relationship	Positive Relationship
3	Would criminal behaviour of offenders in cyberspace be imported to physical space which, in physical space may be exported to cyberspace as well.	Content & Conversation Analysis	No Relationship	Positive Relationship	Positive Relationship	No Relationship
4	Do the intermittent ventures of offenders into the cyberspace and the dynamic spatio-temporal nature of cyberspace provide the chance to escape.	Content Analysis & Descriptive Statistics	Positive Relationship	Positive Relationship	Positive Relationship	Positive Relationship
5	Are strangers likely to unite together in cyberspace to commit crime in the physical space.	Content & Conversation Analysis	Positive Relationship	No Relationship	No Relationship	No Relationship
6	Are associates of physical space likely to unite to commit crime in cyberspace.	Conversation Analysis & Ethnography	Positive Relationship	Positive Relationship	Positive Relationship	Positive Relationship
7	Are persons from closed society are more likely to commit crimes in cyberspace than persons from open society.	Content Analysis	Positive Relationship	Positive Relationship	Positive Relationship	Positive Relationship

Results and Analysis

Key Findings

Deduced Behavioural Patterns for Cyber Crime Perpetrators

Cyber Deception & Theft

1. Attract Attention
2. Collect/Exchange Information
3. Develop Cordial Relationship
4. Establish Trust
5. Trigger a bait/ Access Victim
6. Commit Offense
7. Clear Tracks (Optional)

Cyber Violence

1. Identify Opportunity
2. Gain Access
3. Commit Offense
4. Clear Tracks (Optional)

Cyber Trespass

1. Reconnaissance
2. Gain Access
3. Commit Offense
4. Clear Tracks

Cyber Pornography

1. Attract Attention
2. Collect/Exchange Information
3. Build Cordial Relationship
4. Establish Trust
5. Trigger a bait/ Access Victim
6. Commit Offense
7. Clear Tracks (Optional)

Proof of Space Transition Theory

Postulate	Category of Cyber Crime			
	Cyber Trespass	Cyber Deception & Theft	Cyber Pornography	Cyber Violence
1: Repressed Physical	√	√	√	√
2: ID& Anonymity	√	√	√	√
3: Behaviour Export	√	x	√	x
4: Spatio Temporal	√	√	√	√
5a: Strangers	x	√	x	x
5b: Associates	√	√	√	√
6: Closed	√	√	√	√

Discussion

Summary

No.	Research Objectives	Research Questions	Research Findings	Relevance / Beneficiaries
1	Assess Forms of Cyber Crime	What are the forms of cyber crime? What are the socio economic effects of the various forms of cyber crime	Categories and Socio Economic Effects Determined	Practitioners, Policy and Researchers
2	Test Space Transition Theory	Do the Postulates of the theory form a viable and reliable basis for predicting behaviour of cyber criminals?	Determined the applicability of postulates to various categories of cyber crime	Practitioners and Researchers
3	Develop Models/Framework to combat cyber crime		Developed Models for: - Cyber Deception & Theft - Cyber Trespass	Practitioners, Researchers and Policy Makers

Discussion

Relationship between Findings and Literature

Essential Related Literature:

1. **Jaishankar (2008): Space Transition Theory**

   Findings provides contribution to extension of Space Transition Theory

2. **Brennar (2004): Distinguishing Characteristics of Cyber Crime**

   Findings confirm Brennar's distinguishing characteristics of Cyber Crime

3. **Cox, Johnson & Richards (2009): Crime Displacement Theory**

   Models leveraged Crime Displacement Theory principles to prevent cyber crime

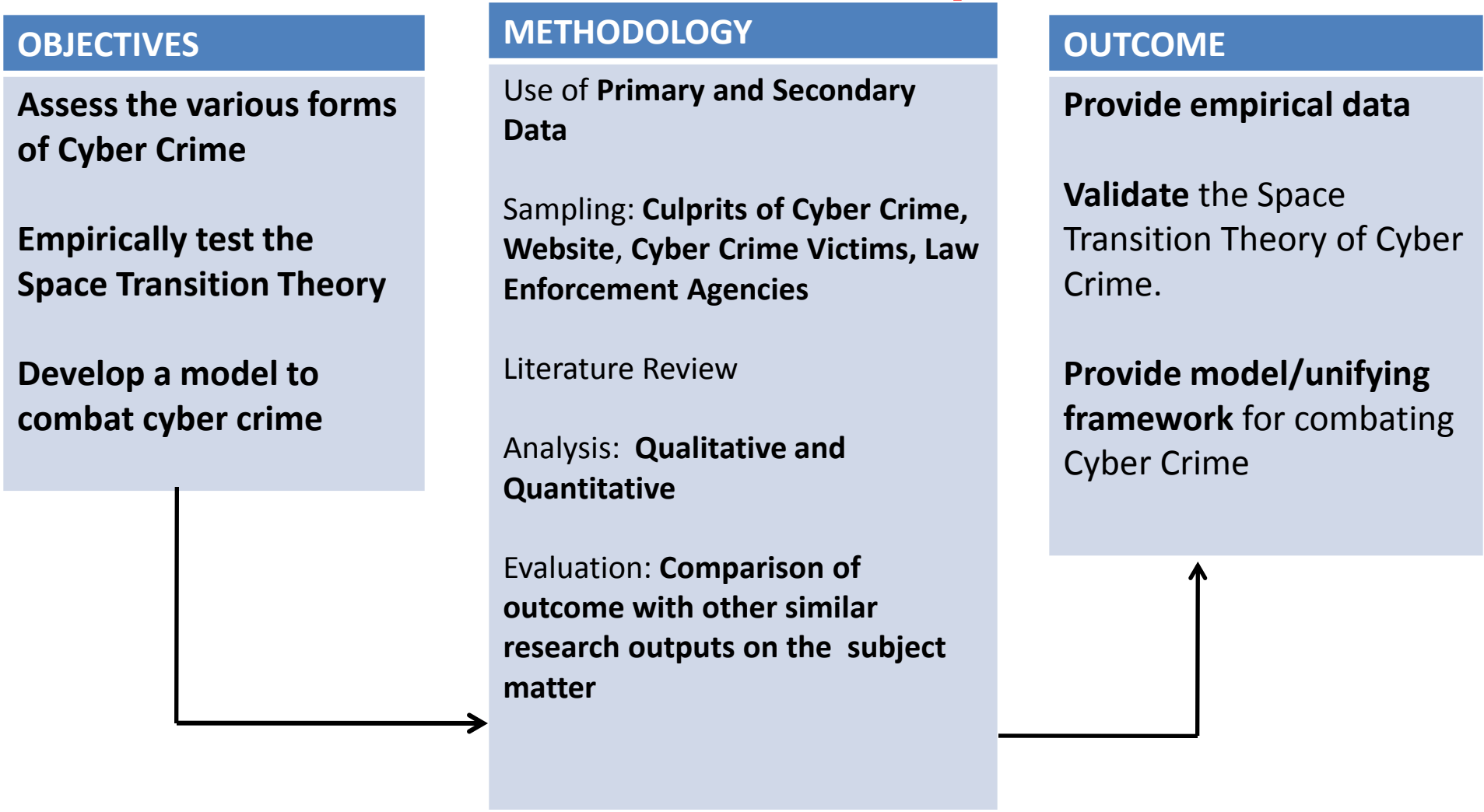
Conclusion

Relevance of Research Findings

Research Finding/Outcome	Practical Implication	Theoretical Implication	Policy Implication
Reliability of Space Transition Theory		For Extending the Theory to be used as a reliable basis for predicting behaviour	
Deduced Behavioural Patterns	For Profiling Cyber Criminals		Policy Makers to control activities
Models to Combat Cyber Crime	For developing products that profile and prevent Cyber Criminals		For drafting policies that provide law enforcement agencies reserved privilege to monitor behaviour

Conclusion

Entire Research in Perspective



Conclusion

Highlights of Research Work

Highlight / Novelty
Deduction of Behavioural Patterns
Test of Space Transition Theory
Development of Models for: - Socially Engineered Cyber Deception & Theft - Cyber Trespass
Framework Depicting Relationship between Theory Findings and Models
New Research Proposals - Varying Responses - Cyber Porn & Violence

Thank You