



## TABLE OF CONTENTS

<b>COVER</b> .....	I
<b>APPROVAL PAGE</b> .....	II
<b>PLAGIARISM STATEMENT</b> .....	III
<b>ACKNOWLEDGEMENT</b> .....	IV
<b>ABSTRACT</b> .....	V
<b>TABLE OF CONTENTS</b> .....	VIII
<b>LIST OF ACRONYMS &amp; GLOSSARY OF TERM</b> .....	XI
<b>TABLE OF FIGURES</b> .....	XVI
<b>CHAPTER I. INTRODUCTION</b> .....	1
<b>1.1. Background</b> .....	1
<b>1.2. Hypothesis Research</b> .....	3
<b>1.3. Problem Statement</b> .....	3
<b>1.4. Research Objective</b> .....	5
<b>1.5. Research Question</b> .....	7
<b>1.6. Research Scope</b> .....	7
<b>1.7. Research Conceptual Model</b> .....	9
<b>1.8. Originality</b> .....	12
<b>CHAPTER II. LITERATURE REVIEW</b> .....	15
<b>1.1. Cyberthreats on Spatial Cadastral Data</b> .....	15
<b>1.2. Spatial Data Infrastructures (SDI) and Cybersecurity</b> .....	16
<b>1.3. Advanced Technologies and Cyber Threats</b> .....	17



<b>1.4.</b>	<b>Case Studies from Other Countries.....</b>	<b>18</b>
<b>1.5.</b>	<b>Theoretical Frameworks and Models.....</b>	<b>18</b>
<b>1.6.</b>	<b>Summary and Research Gap.....</b>	<b>21</b>
<b>CHAPTER III. RESEARCH METHOD .....</b>		<b>23</b>
<b>3.1.</b>	<b>Combined socio-technical approach for CSRM .....</b>	<b>25</b>
3.1.1.	Presentation of combined social-technical approach: BPMN + Scope of study & Security Baseline .....	25
3.1.2.	BPMN: Elicitation Techniques and Data Collection .....	28
3.1.3.	Scope of study & Security Baseline: data collected. ....	29
<b>3.2.</b>	<b>Cyber Threat Intelligence platform for spatial cadastral data .....</b>	<b>30</b>
3.2.1.	Quantitative inductive exploratory approach.....	30
3.2.2.	Data Analysis Techniques .....	33
3.2.3.	Sources of Data and Sampling.....	34
3.2.4.	Sample Selection .....	35
3.2.5.	Validation of Results .....	36
3.2.6.	Tools and Technologies.....	36
3.2.7.	Comparison with Existing Practices.....	36
<b>CHAPTER IV. RESULTS AND DISCUSSION .....</b>		<b>38</b>
<b>4.1.</b>	<b>Combined Socio-Technical Approach .....</b>	<b>40</b>
4.1.1.	Results of Step 1': BPMN Identification of Potential Risks/Threats/Vulnerabilities ..	40
4.1.2.	Results Of Step 1: Workshop EBIOS RM Scope of Study & Security Baseline .....	44
4.1.3.	Main Findings Results.....	47
4.1.4.	Discussion .....	47
<b>4.2.</b>	<b>Cyber Threat Intelligence Platform for Spatial Cadastral Data.....</b>	<b>51</b>
4.2.1	Key Findings.....	51
4.2.2	Interpretation of Results.....	53
4.2.3	General Significance.....	58
4.2.4	Practical Implications.....	58
4.2.5	Study Limitations.....	62
4.2.6	Validation of Results .....	62



<b>CHAPTER V. CONCLUSIONS AND SUGGESTIONS.....</b>	<b>63</b>
<b>5.1. Conclusion.....</b>	<b>64</b>
5.1.1 Key Contributions of the Research .....	65
5.1.2. Limitations of the Research .....	67
<b>5.2. Suggestions.....</b>	<b>68</b>
5.2.1 Practical Recommendations.....	68
5.2.2 Strategic and Policy Recommendations.....	71
5.2.3 Suggestions for Future Research.....	72
5.2.4 Limitations and Conditions for Implementation .....	73
<b>5.3. General Conclusion.....</b>	<b>73</b>
<b>BIBLIOGRAPHY .....</b>	<b>76</b>
<b>APPENDIX .....</b>	<b>87</b>