International Journal of Cyber-Security and Digital Forensics (IJCSDF) 7(1): 87-98
The Society of Digital Information and Wireless Communications (SDIWC), 2018 ISSN: 2305-001

# Cyber Intelligence & OSINT: Developing Mitigation Techniques Against Cybercrime Threats on Social Media

## A Systematic Review

**July 2017**

[1]**Abel Yeboah-Ofori**
School of Architecture, Computing & Engineering
University of East London. United Kingdom
u0118547@uel.ac.uk

[2]**Prof. Allan Brimicombe**
Head. School of Geo-Information Studies
University of East London. United Kingdom
a.j.brimicombe@uel.ac.uk

**ABSTRACT**

Open Source Intelligence (OSINT) involve the collection or processes of gathering data and profiling of publicly available private and public sector information sources about individuals and business intelligence purposes. These sources includes internet and other social media platforms such as Facebook, emails, twitters, what's apps for. Much debate and research has been done on the threats, vulnerabilities and the impact of the use of social media sites but this study is to minimize bias.

Objective: To systematic review and synthesis findings on current empirical research topic on cyber intelligence and open source intelligence profiling to identifying both the threats and vulnerabilities on online social networks for mitigation purposes.

Methods: A systematic narrative review of research using rigorous searching on online databases. The results were then subjected to review using a quantitative and quality appraisal tool and a narrative synthesis methodology. A theoretical framework was developed for the synthesis using concepts from the literature 'The Effectiveness of Neighborhood Watch'. A Campbell Systematic Review

Results: The systematic search retrieved 18 original research papers investigating and exploring the effects of online social media technologies on open source intelligence concepts. The use of social media were reported as enhancing social cohesion among peers, improving business opportunities as information gets to customers quickly. Safe identity experimentations, OSINT and cyber intelligence social media gathering is especially vital in the modern war on terror. Understanding terrorist network topologies, crime data analysis and mining, countering improvised explosive devices. The study also highlighted potential negative impacts and threats and the effect of social engineering threats in SNSs, threats of social networking and identity crime. Vulnerabilities of HTTP header information and cookies being sent to third-party aggregators as well harmful effects of exposure to threats.

Conclusion: The systematic review has revealed extraordinary evidences and contradictory concepts. It has also revealed the underlining research challenges impacting on open source intelligence. Due to the invincibility nature of social media technologies, social media platforms are constantly being used for social, business and intelligence gathering purposes but to ensure proper and advance mitigating circumstance, further research is required to gain situational awareness and appropriate counter measure.

**KEYWORDS**

Cyber Intelligence, OSINT, Cybercrime, Threats, Social Media, Systematic Review

## 1. INTRODUCTION

Open Source Intelligence (OSINT) involves the collection, analysis and use of data from openly available sources for intelligence purposes [13]. The advent of the internet and the

electronic business websites have made it possible for almost everyone to access and transact businesses online. Social media platforms has emerged as an important strategic open source tool for organizations to facilitate communication with their employees, customers. Facebook pages and twitter feeds are mined for business intelligence purposes and one fairly recent trend of change in our culture that seem bound to have an important influence in intelligence testing, is the way that information is transmitted and received [9]. The study seeks to carryout out systematic review in the area of open source intelligence gathering and profiling and how mitigating techniques are develop against threats on social media/network platforms.

### 1.2 Systematic Review Questions.

The main question being addressed by this review are:

- What is the extent of the use of OSINT in mitigating threats on social media platform?
- What OSINT research topics are there to address the threats in the domain of using social media such as Facebook, twitters, and What's apps?
- What research approaches do cyber intelligence organizations use in information gatherings and profiling?
- What empirical research methods do cyber intelligence researchers use in the domain of cybercrime?

### 1.3 Theory of Open Source Intelligence

Open source has been in existence for many years but with the explosion of the internet and the World Wide Web (WWW) has brought with it a number of cyber security professional and researchers publishing journals and articles on cybercrime threats, cyber profiling and gatherings.

With the advent of social media and rapid information transfers available today, a great deal of actionable and predictive intelligence can be obtained from public and unclassified sources. The significance of OSINT has become a conflict between the private sector, the government and the military over how intelligence data should be gathered from different sources. Some of the challenges has been the gathering, exploiting and disseminating the information gathered in a timely manner for the purpose of addressing specific intelligence requirements.

Data from 'EU kid online' suggested surveys that an estimated average of 15-16 year olds spend about 118 minutes of time per day on online social network sites. [17]. Hence are vulnerable to threats such as sexting, cyberbullying and cyber stalking. Within the last few years there have been lots of journals writing on the subject of cybercrime and cyber security vulnerabilities and the potential threats it poses to individual, businesses and countries. Internet access to articles has also created a phenomenal number of hits for us to explore when writing or carrying out a research. This has brought about the challenge of building and maintaining the required skills needed to use the variety of information and the electronic media accesses available.

### 1.4 The Need for OSINT Systematic Review

To Individual and business, the amount of information available online can be overwhelming, and the lack of awareness and expert knowledge can cause potential damages and lead to false belief in unreliable information which in turn can raise potential information security assurance issues. The availability of the internet and the vulnerabilities that exist on it makes it not unusual for the number of published studies to run into huge numbers before they are reviewed.

Some studies may give unclear, confusing or contradictory results, and at time they may not be published in English hence, will lack clarity as to whether it can be generalized into other countries system security. Every journal or article may provide a little insight into the vulnerability at hand. Therefore, the need for a systematic review in the area of OSINT will provide us an unbiased and right information. Also an unbiased information will assist in facilitating information gatherings by means of transferring knowledge through research and publications, education,

decision support systems and trainings to facilitate decision makings. The rationale will be to understand the vulnerabilities that exist and it impacts on business processes using open source tools.

### 1.5 Aims and Objectives

The aim of this systematic review is to access the effective use of OSINT to develop mitigating techniques against threats and abuse on online social media platforms for intelligence purposes.

The Primary objectives are:

- To investigate into OSINT methods and techniques using existing literatures with the idea of conducting reviews on online social media platforms.
- To identify studies that evaluate the effective used of methods on existing OSINT tools with the view of generating and identifying vulnerabilities and build threat profiles.
- To identify gabs in knowledge of the list of studies that meet the required criteria for cybercrime threats and vulnerabilities.
- To obtain a comparable measure of most effective studies to review.
- To conclude on the effectiveness of using OSINT gathering tools to mitigate risks.

## 2 METHOOLOGY

A systematic narrative review method of research involves using rigorous searching on online databases. The approach will be to eliminate biases by establish eligibility criteria using inclusion and exclusion criteria's in certain key word searches in the selection strategy. The results will then subjected to review using a quantitative and quality appraisal tool and a narrative synthesis methodology. A theoretical framework will be developed for the synthesis using concepts from the literature 'The Effectiveness of Neighborhood Watch'. A Campbell Systematic Review. [20]

### 2.1 Inclusion and Exclusion Terms

Open Source Intelligence is often implemented alongside other factors such as a particular crime, jurisdiction, a person, a threat or a vulnerability. The crime could be a Distributed Denial of Service (DoS) where the perpetrator can initiate attack a remotely. Social media crimes can be committed globally but normally they are reported locally hence, the issues of jurisdiction comes into play and could involve the cyber laws that exist in different countries or continents. The perpetrator could be anywhere in the world and with access to internet will be able to commit social media crimes irrespective of the gender, age or profile.

### 2.2 The following types of interventions will be included in the review:

- Cyber intelligence gatherings of person (contacts, websites visited, types of conversations and languages used)
- Profiling to establish relationships between threats on social media platform
- Cyber intelligences vulnerabilities to mitigate threats.

### 2.3 Criteria for Selecting Studies

The techniques used in the study utilized relevant research studies relevant to the topic. For the purpose of the review, OSINT is defined as the gathering of threats and vulnerabilities then profiling them to mitigate probable threats.

### 2.4 Selection Criteria

- The review included published and unpublished literature
- Search was based on documented evaluations
- There were no restrictions to countries of origin
- The evaluation were reviewed in English
- No restrictions on source sector (e.g. academic, government, policy etc)
- No restrictions of period time of covered by the evaluation (e.g. Short or long term effects)
- There are no restrictions to terms of years (e.g. year of publication, study or implementation)

To address the review questions above, the search terms will include narrative, qualitative and quantitative research methods empirically to identify the chains of vulnerabilities that exist on social media/network platforms and the risk access spots. The techniques and procedures adopted to gathered, analyses and synthesized the research data will define the methodology used.

### 2.5 Search Strategy

The objective of the review is the need to apply automated search to gather primary literature. The following sources were used for selecting the studies and search strategies used to search were:

1. Online databases (journals, reports and articles)
2. Online library catalogues for books
3. Reviews of the literatures on using OSINT to develop effective mitigating techniques against threats on online social media
4. Search bibliographies of publications on open OSINT

### 2.6 Databases Searched

Resources used for the searches includes online databases, digital libraries and search engines such as UEL Athens, Library Learning Services (LLS) and Google Scholar were access to search engines and repositories such as:

- Science Direct
- IEEE
- eBook Library
- JSTOR
- ACM Digital Libraries
- EBSCO Database and others
- SAGE Journals
- Emerald e-Journals
- Cambridge Journals Online
- Oxford Journals

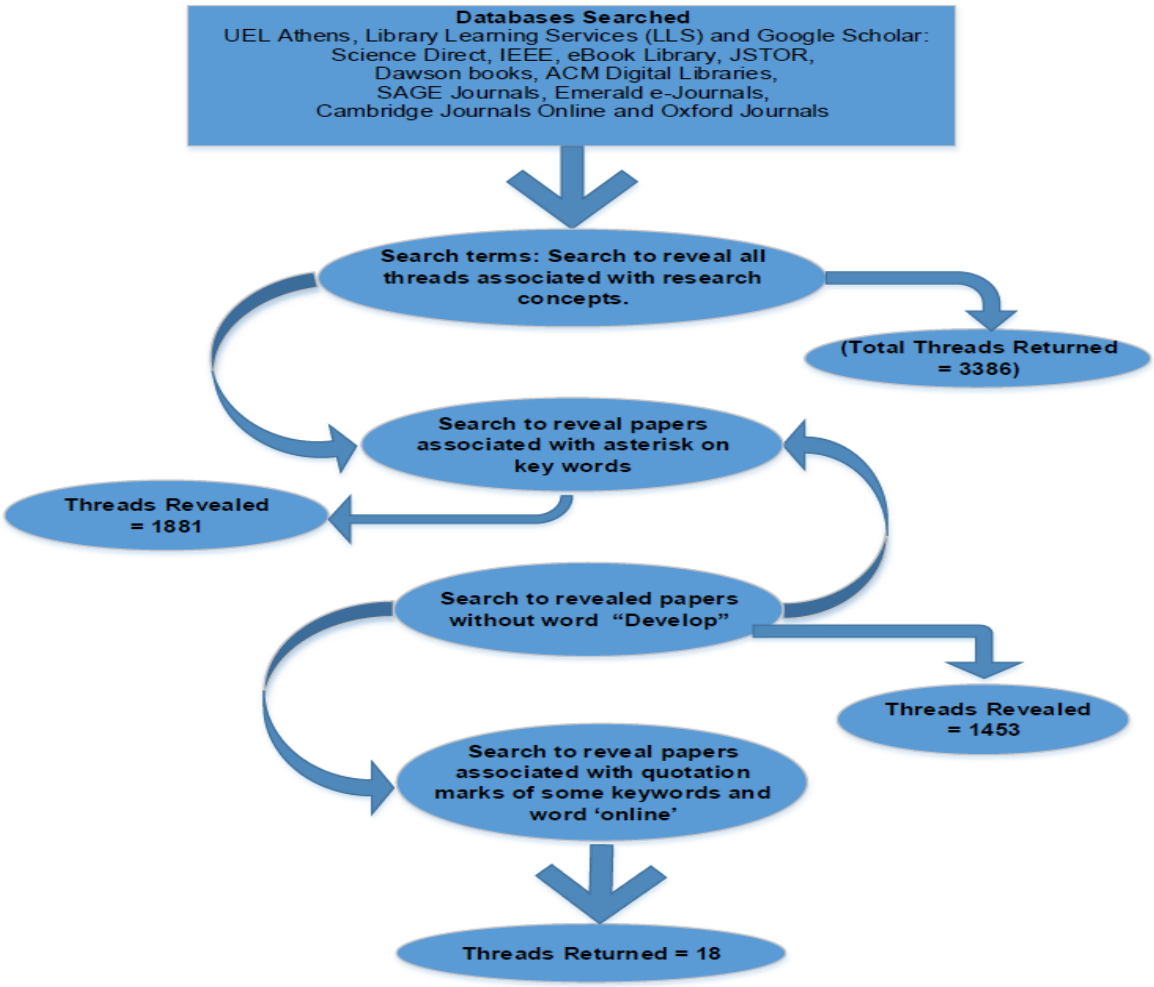


***Figure 1. Systematic Search Method***

### 2.7 Search Terms

The following search terms were used in the database searches:

Open Source intelligence, Cyber Intelligence, OSINT, Open Source intelligence threats, Open Source intelligence vulnerabilities, Open Source intelligence gatherings, Open Source intelligence profiling, OSINT threats, and OSINT vulnerabilities. Social Media.

### 2.8 Types of Outcomes

The review focuses mainly on the impact of using OSINT to mitigate cybercrime. The types of cybercrime covered in the review are those that OSINT might be able to reduce. These includes online crimes on social media/network platforms such as Face Book, What's Apps and Twitters.

### Extracted Evidence

Using pre-inclusion criteria, title, abstracts and introductions were reviewed and selected based on the originality, age, quality, peer reviewed and statistically tested.

All included journals must have some cyber intelligence gathering relating to OSINT. Search that reveal all the titles that have internet, online social and social networks were used. Due to time constraints, non-English language papers were excluded. Journals that emphasized on social media or social networks without its online or cyber threats, vulnerability, risk and impacts were excluded on less they contain variables that relates to OSINT.

### Search Terms

| Motivation | Search Terms | Threads |
|---|---|---|
| **Search to reveal all threads associated with research concepts** | (Open* OR source* OR intelligence* OR develop* OR mitigate* OR technique*)<br>AND<br>(cybercrime* OR threats* vulnerabilities*)<br>AND<br>(social media* OR online* OR social network*) | **3386** |

**Table 1. Search to Reveal all Threats Associated with Research Concepts**

| Motivation | Search Terms | Threads |
|---|---|---|
| Search to reveal papers associated with asterisks on some key words | (Open source intelligence* OR develop mitigate technique*) AND (cybercrime* OR threats* OR vulnerabilities*) AND (social media* OR social networks*) | 1881 |

**Table 2. Search to Reveal Papers Associated with Asterisk on Some keywords**

| Motivation | Search Terms | Threads |
|---|---|---|
| **Search to reveal papers without word 'Develop'** | (Open* source* intelligence* OR mitigate technique*) AND (cybercrime* OR threats* vulnerabilities* OR abuse*) AND (social media* OR social networks*) | **1453** |

**Table 3. Search to Reveal Papers Associated without word 'Develop'**

| Motivation | Search Terms | Threads |
|---|---|---|
| **Search to reveal papers associated with quotation marks of some keywords and word 'online'** | ('Open source intelligence' OR mitigate* OR technique*) AND (cybercrime* OR threats* OR* vulnerabilities*) AND (social media* OR online* OR social network*) | **18** |

**Table 4. Search to Reveal Papers Associated with Questions Marks of some keywords and word 'online'**

### 2.9 Search Terms Applied and Threads Returned

The following search terms were applied and the following threads returned:

- Search to reveal all threads associated with research concepts = 3386
- Search to reveal papers associated with asterisks on some key words = 1881
- Search to reveal papers without word 'Develop' =1453
- Search to reveal papers associated with quotation marks of some keywords and word 'online' = 18

#### 2.9.1 Search Matrix

To conduct a meta analyze using statistical methods from the quantitative data collected from the primary studies, the search matrix below was developed to answer the key review questions extracted. The empirical research methods was used to analyze the findings such as narrative, qualitative and quantitative review combined [15].

Odds Ratio (OR) were calculated for each of the three evaluations and a weighted mean odds ratio was calculated for all the studies combined. Then the significance of the research to the review questions emphasized in the meta-analysis section below will be coded into using SPSS to generate an Odds Ratio graph. Time did not permit me to get and run the SPSS tool to the test results properly.

## 3 SYNTHESIZING REPORT

The aim of this phase is to review the individual evidence regarding the various OSINT techniques that are used to mitigating threats on social media in order to provide an overall estimate of its effectiveness in cyber profiling. The methodology the study adopted was developed and influenced by a systematic review technique that describes synthesis as a process of extracting data from individual research studies and interpreting and representing them in a collective form.

### 3.1 Synthesis Methods

The synthesis involves collating, combining and summarizing finding of individual studies included in the matrix table above [20]. The empirical methods used in the review includes narrative, qualitative and quantitative techniques to consider the strengths of evidences as well as explore whether the results collated are consistent across evidences. The synthesis will then provide a means of combining the outcomes of the number of prior studies in an analysis that assesses the combined outcomes or the meta-analysis of previous studies to enable reliable conclusions to be drawn [20]. The study seeks to address the following reviews:

### 3.2 Narrative Synthesis

The narrative review reveals a descriptive summary of findings provided in the matrix table required to interpret the collected evidence for the significance of open source intelligence. Here the synthesis answers the question as to what is the extent of the use of OSINT in mitigating threats on social media platforms. Four study reveals that information abounds on social media networks such as facebook, twitter What's App. [1] [3] [4] [22]. However two studies highlights results that narrative review has revealed contradictory evidence of threats of social wellbeing while revealing an absence of robust causal research. Whiles relationships between elements of language in use of OSINT remains a core issue in both machine translation and cognitive science in the implications of the automatic translation of the human language resolutions of lexical ambiguity in machine translation. [4] [22]. Whilst three studies indicate that use of social engineering attacks in SNSs is affected by the characteristics of four main entities: the SNSs (the environment), social engineer, (the attacker), plan and technique (the tricker), and the SNS user (the victim). This reveals the evaluated entities and sub entities that affect social engineering threats in SNS. [1] [3] [4].

### 3.3 Quantitative Synthesis

The quantitative review focus on describing commonly used methods of combining study results and exploring heterogeneity imbedded in the review framework. Quantitative study considers the size and directions of any observed intervention effects in relation to strength of evidence [20]. The review asked what OSINT research topics are there to address the threats in the domain of using social media. Six studies reviews the relationship that determine the theoretical framework and a survey of active users were reviewed of behavioral patterns on social networks. Personal characteristics and technical efficacy of users show how users with high-risk propensity are more likely to become victims of social media threats. Also to mitigate risks, the methodology used the concepts of the "Theory of Planned Behaviour" a model from the study of psychology that is used to predict behaviors. Surveys reveals that of all the users who received the application, only a few took action to change the public-search option visibility from public to private indicating users are vulnerable. [2] [18] [5] [16] [23]. However, four papers suggests network clustering and the number of non-person contacts were a predictive of vulnerability. Whiles modeling transnational terrorism groups, provided knowledge discovery for intelligence analysis and interdiction of plots as well as mining for countering improvised explosive devices hidden links in social media networks and prediction [5] [9] [10] [23].

To review the question as to what research approaches do cyber intelligence organizations use in information gatherings and profiling, the study adopted empirical methods such as narrative, qualitative and quantitative techniques to consider the strengths of evidences. The study then combining the outcomes of the number of prior studies in the analysis that assesses the combined meta-analysis.

Four studies adopted narrative review approach of researches published, semantic error processing in WWW and applying wed crawlers and text bases analytics to human trafficking online as well social engineering. [1] [3] [4] [14] [22]. Three studies used the qualitative approach to examine popular social network sites indicating online users community formation and increase belongings as well as purposive sampling to gather information [14] [7] [12].

With the quantitative review, eleven studies adopted quantitative approach to determine the scientific bases to study the behavioral patterns, large sample size, incidence and frequencies of occurrences [19] [18] [9] [5] [16] [23] [13] [6] [8] [2] [10]. Four studies used surveys and quantitative approach to determine public responses of vulnerabilities and used questionnaires to determine behavioral patterns as well as planned behaviors of physiological models. [19] [15] [9]' Four studies explored the concepts of social media threats in relation to social network and identity theft, advance persistence threats analysis in cyberspace and malware vulnerabilities and threats on social media sites. [2] [10] [16]. Considerable evidence supports the changing human information relationships resulting from the emergence and growing dominance of the internet and www looking at four studies to support open source intelligence.

### 3.4 Qualitative Synthesis

With qualitative review, the study review three journals that looks at specific groups and did a purposive sampling using interviews and from policy makers to review the paper. [12] [7] [14]. One study reviews the legal implications and the criminal procedural laws that exists in relation to OSINT [12]. Two studies looks at how open source is use in information leaks and how use of social media in human soft senses can assist in generation situational awareness. [7] [14].

### 3.5 Meta-Analysis

In order to conduct a meta analyze using statistical methods from the data collected on mitigating techniques against threats on social media platforms, the search matrix was developed to answer the key review questions extracted [15]. All evaluations in the analysis employed the same research design to analyze the findings in the narrative, qualitative or quantitative reviews.

## 4 MEASURED OUTCOMES

The total number of data used to evaluate the measured outcome of threat was (n=18), with Narrative Review (n=4), Qualitative Review (n=3) and Quantitative Review (n=11). To obtain the odds Ratio (OR) for the analysis, the three types of data collected requires different methods as the outcome in each study measures the probable threat posed. There were no evaluation included in the review that provided information that is the standard deviation to allow ORs to be calculated from respondents that can be used from the mean threat rates. Therefore the meta-analysis is based on ORs derived from frequencies of threats and probable risks.

The measured outcome of each effective impact for findings in the narrative review based on threats and risks is the OR. The difference in the level of threats and risks may vary depending on the odds.

**The OR is calculated as shown in following.**

| | Before | After |
|---|---|---|
| Threat | a | b |
| Risk | c | d |

Where a, b, c, d are number of threats

OR = a*d/b*c

The null or no effect value of OR is 1.0. To the extent that when the OR exceeds (>) 1.0, it might be concluded that the threats are possibly higher. Also to the extent that the OR falls below (<) 1.0, it might be concluded that the risks impacts are possibly higher. It is also possible that some schemes might serve to increase the number of recorded threats and risks such as social engineering, spam and phishing.

The Variance of OR is calculated from its natural logarithm (LOR)

VAR (LOR) = 1/a +1/b +1/c +1/d

In order to produce a summary threat ratio in a meta-analysis, each effect size (LOR) is weighted by the variance of its inverse (1/V). This estimates of the variance is based on the assumption that total numbers of threats and risks (a, b, c, d) have a Poisson distribution to determine the ratio of threat that may attack a user per day. If the number of threats have a Poisson distribution, it variance should be the same as its mean. However, the large numbers of changing extraneous threat factors may cause over dispersions, that is, where the variance of the number of threats VAR may exceeds the number of risks N.

The analysis was therefore adjusted to deal with the threats of possible over dispersions that is greater than expected variance.

The D = VAR/N

D increases linearly with N and was correlated with N indicating the median number of threats in the study.

### 4.1 Data Review

For the studies, based on various data review of threats and risks on social media platforms, the OR was calculated from the log of OR (LOR) using the formulae below.

LOR = Ln = (a2*d2/b2*c2) – Ln = (a1*d1/b1*c1)

Where a2, b2, c2, d2, are before numbers a1, b1, c1 d1 are after.

| | **BEFORE** | |
|---|---|---|
| **AFTER** | | |
| | Impact | No Impact |
| | Impact | No Impact |
| Threats | a1 | b1 |
| | b2 | b2 |
| Risks | c1 | d1 |
| | c2 | d2 |

The Variance of LOR is calculated using the following formulae.

VAR (LOR) = 1/a1 + 1/b1 + 1/c1 / 1/d1 + 1/a2 +1/b2 +1/c2 + 1/d2

This method is based on comparing before and after effects of OR on threats and risk. The method was preferable to compare after and ORs only as this would not control for pre-existing differences between the experimental and control areas.

### 4.2 Individual Effect

The table 5 below summarizes the 18 evaluations of included in the meta-analysis. The table shows that 15 evaluations had an OR greater than one and three had an OR less than one. Hence, in the majority of evaluations, threats was associated with a risks on social media platform. Four of the 15 evaluations with an OR greater than one were statistically significant. The graph shows a clear pattern of small positive effects.

### 4.3 Mean Effect

The aim of the meta-analysis was to calculate the extent of weighted mean effect that is the odds ratio (OR). There are two ways of calculating the extent of the weighted mean effect and these are Fixed Effects (FE) and Random Effects (RE). In the case of the fixed effects (FE) method, each threat impact is weighed by the inverse of its variance (1/VAR), so that studies based on serious threats are given greater weight than those based on minor threats. The FE method is based on the assumption that the extent of threat are consistent in the sense that they are all drawn form a random distribution of effect sizes about some mean. However, the nature of an impact might violate this assumption and be significantly diverse. One method of addressing the problem of diversity of threats is to use the 'random effects' model. The random effects (RE) method minimizes diverse threats by adding a constant to the variance of each threat.

### 4.4 Fixed Effects

The table below shows that the weighted mean OR for the 18 evaluations combined was 1.19 using the FE model. This finding was statistically significant as an OR of 1.19 can be interpreted to mean that threats increased by 19% due to social engineering threats and therefore the need to mitigate these threats are high and must be control. Compared with the risk, there was decreased by 16% (1/OR) in the impact due to awareness.

### 4.5 Random Effects

The 18 studies were significantly diverse according. Therefore, the RE model was used. The weighed mean OR for the 18 evaluations combined was 1.36 using the RE model. An odds ratio of 1.36 means that threats increased by 36% compared with the risks that decreased by 26% due to situational awareness.

### 4.6 Limitations

We should emphasize that the estimate of the variance of ORs may not be accurate, while the best available at present, are not exact figures and may be slightly inaccurate. Therefore, there may be some inaccuracy in the weightings used in the meta-analyses. Due to time constraints, the Confidence Intervals (CI) around the weighted mean impact may be slightly inaccurate. It needs to me worked on a little more to be accurate statistically.

**Evaluation Table**

| Author & Date | Journal Type Used | Extent of Social Media use High/Low | OR | CI | Z | P of Z |
|---|---|---|---|---|---|---|
| Best, Manktelow & Taylor (2014) | Systematic Review | High | 2.23 | 0.87-6.53 | 1.67 | ns |
| Koops (2013) | Investigation into OSINT legal Constraints | High | 2.49 | 0.49-4.53 | 0.71 | ns |
| Spence, Lachlan and Rainear (2015) | Information Dissemination | Low | 1.85 | 1.23-2.77 | 5.03 | <0.0004 |
| Saridakis, Benson, Ezingeard & Tennakoon (2015) | Impact of Victimization | High | 2.59 | 0.12-57.52 | 0.96 | ns |
| Gulenko (2015) | Risk Mitigation | Low | 1.47 | 1.08-1.20 | 5.03 | <0.0001 |
| Buglass, Binder, Betts & Underwood (2015) | User Vulnerability | High | 1.75 | 1.38-2.22 | 4.61 | <0.0001 |
| Mansour (2015) | Information Dissemination | Low | 1.35 | 0.30-6.13 | 0.39 | ns |
| Kock Wiil (2011) | Counter Terrorism | High | 2.850 | 0.13-63.52 | 0.66 | ns |
| Koop, Hoepman & Leenes (2013) | Legal | Low | 0.10 | 0.01-1.80 | 1.56 | ns |
| Coyne & Bell (2011) | Review | High | 2.55 | 0.62-10.51 | 1.29 | ns |
| Glassman & Kank (2012) | Review | High | 2.64 | 1.32-2.02 | 4.57 | <0.0001 |
| Andress & Winterfeld (2014) | Review | High | 2.55 | 0.27-3.11 | -0.13 | ns |
| Watters, (2012) | Review | High | 2.35 | 0.16-1.65 | -1.12 | ns |
| Giacobe, et.al (2010) | Review | High | 2.15 | 0.69-1.58 | 0.19 | ns |
| Brewster, et al (2014) | Review | High | 2.25 | 0.65-3.50 | 0.95 | ns |
| Eric Holm (2014) | Review | High | 1.95 | 0.60-2.11 | 0.36 | ns |
| Krishnamurthy & Wills (2009) | Review | Low | 0.36 | 0.67-2.46 | 0.75 | ns |
| Algarni, Abdullah, Xu, Yue, Chan, Taizan & Tian, Yu-Chu (2013) | Review | Low | 0.42 | 0.82-1.69 | 0.87 | ns |
| **Total n=18** | | | | | | |
| Fixed Effects | | | **1.19** | **1.13-1.14** | **7.25** | **<0.0001** |
| Random Effects | | | **1.36** | **1.15-1.61** | **3.36** | **<0.0004** |

**Table 5. Summary of 18 Evaluations Included in Meta-Analysis**

**Ns = Not Significant**

### 4.6 Moderator Analysis

An OR of 1.19 can be interpreted to mean that threats increased by 19% due to social engineering threats and therefore the need to mitigate these threats are high and must be control. Compared with the risk, there was decrease by 16% (1/OR) in the impact due to awareness compared with the probable risk.
The weighted mean OR for the 18 evaluations combined was 1.36 using the RE model. An odds ratio of 1.36 means that threats increased by 36% compared with the risks that decreased by 26%.

## 5 RESULTS

To answer the first research question, the findings in the various review shows that OSINT has revealed contradictory evidence while revealing an absence of vigorous fundamental research to the extent of the use of OSINT in mitigating threats on social media platform?

With the research question (2) above, of what OSINT research topics are there to address the threats in the domain of using social media such as Facebook, twitters, and What's apps. Ten studies revealed that threats and vulnerabilities exist including Social engineering attacks in social networks systems and are affected by the characteristics of four main entities such as environment, social engineer that is the attacker, the plan and technique used to trick, and the SNS user or the victim.

To answer the research question (3), Research approaches that cyber intelligence organizations use in information gatherings and profiling varies and seven studies reveals some challenges due to jurisdiction, legal, language barriers impacts on evaluating legitimacy of reported data and identified deceptions in the open source channels to a verifiable effect. Whiles one study identifies intelligences gatherings from different user perceptions and their unwillingness to reveal information.

The empirical research methods used by researchers in the cyber intelligence domain of cybercrime varies also widely with research question (4) above. The study reveals that out of the eighteen hits, narrative review indicated four studies that points positively to the relationships between users of social media and the probable threats. But the narrative review was limited in that it is based on the counts of users and simply not enough in cyber intelligence gatherings. Eleven studies quantitatively identified vulnerabilities on the social media due to lack of user awareness and it is clear from the research that profiling may be effective in developing mitigating techniques social media threats.
With the qualitative study, research reveals three studies that identifying the narrow set of private information that users really need to share to accomplish specific interactions on social media sites. However, according to theory, qualitative research in cyber intelligence gathering may be effective in profiling threats and migrating threats.

### 5.1 Conclusions and Future Directions

The review has classified research finding in terms of the use of open source intelligence and the threat and vulnerabilities that exist on social media platforms. The systematic review has revealed extraordinary evidences and contradictory concepts. It has also revealed the underlining research challenges impacting on Open Source Intelligence. Due to the invincibility nature of social media technologies, social media platforms are constantly being used for social, business and intelligence gathering purposes but to ensure proper and advance mitigating circumstance, further research is required to gain situational awareness, to mitigate threats and ensure appropriate counter measures.
The limitations in the meta-analysis were due to time constraints as the study was aimed at looking at the threats from narrative, qualitative and quantitative approach. The implication for further research will include lack of resources, conflict of interest and inability to gather secondary data, financial constraints and building trust from individual sources.

## REFERENCES

1. Algarni, Abdullah, Xu, Yue, Chan, Taizan, & Tian, Yu-Chu. 2013. Social Engineering in Social Networks Sites: Affect Based Model. In Proceeding Paper of IEEE International Conference. Queensland University of Technology, Brisbane, Australia. Pp. 508-515.

2. Andress, J. & Winterfeld, S. 2014. Cyber Warfare: Techniques, Tactics and Tools for Security Practitioners. 2nd Edition. Elsivier, Syngress.

3. Best, P., Manktelow, R. & Taylor, B. 2012. Online Communication, Social Media and Adolescent wellbeing: A Systematic Narrative Review. Journal of Children and Youth Service Review. Elsevier. University of Ulster. UK.

4. Brewster, B., Ingle, T. & Rankin, G. 2014. Crawling Open-source Data for Indications of Human Trafficking. IEEE/ACM International Conference on Utility and Cloud Computing. Intelligence and Organized Crime Research. Sheffield Hallam University. UK.

5. Buglass, S.L., Binder, J.F., Betts, L.R., & Underwood, J. D. M. 2015. When Friends Collide: Social Heterogeneity And User Vulnerability on Social Networks Sites. Journal of Computers In Human Behavior. Elsevier. Nottingham Trent University. UK

6. Coyne, J. W. & Bell, P. 2011. The Role of Strategic Intelligence In Anticipation Transnational Organised Crime: A Literature Review. International Journal of Law, Crime & Justice. Queensland University of Australia. Australia.

7. Giacobe, N. K., Kim, H. & Faraz, A. 2010. Mining Social Media in Extreme Events: Lessons Learned from the DARPA Network Challenge. Pennsylvania State University. USA.

8. Glassman, M. and Kang M.J. 2012. Intelligence in the internet age: The emergence and evolution of Open Source Intelligence (OSINT). Journal of Computers in Human Behavior, Elsevier, Ohio State University.

9. Gulenko, I. 2013. Social Against Social Engineering: Concepts And Development of A Facebook Application. Journal of Information Management & Computer Security. Emerald Insight. Vol 21 ISS 2 ppp.91 – 101. University of Technology, Munich, Germany.

10. Holm, E. 2014. "Social Networking and Identity Theft in The Digital Society", The International Journal on Advances in Life Science. Faculty of Law, Bond University, Australia

11. Horn, J. L, 1979. Trends in the measurement of intelligence. Intelligence, 3, 229-240.

12. Koops, B. 2014. Police Investigations In Internet Open Source: Procedural-Law Issues. Journal of Computer Law & Security Review, Elsevier. Tilburg University, Netherlands.

13. Koops, BP., Hoepman, JP. & Leenes, R. 2013. Open Source Intelligence and Privacy By Design. Journal of Computer Law & Security Review, Elsevier, Tilburg University, The Netherlands

14. Krishnamuthy, B. & Wills, C. E. 2009. On The Leakage of Personally Identifiable Information Via Online Social Networks. Worcester Polytechnic Institute. Worcester, MA USA.

15. Lipsey, M.W. & Wilson, D.B. 2001. Meta-Analysis. Thousand Oaks, California: Sage

16. Mansour, R. F. 2015. Understanding How Big Data Leads To Social Networking Vulnerability. Journal of Computers in Human Behavior, N, V, Assiut University, Egypt.

17. O'Neil, B. & Mclaughlin, S. 2011. Recommendations on Safety Initiaitves. Reports D7.1. EU Kids Online, London, UK.

18. Saridakis, G., Benson, V., Ezingeard, J. & Tennakoon, H. 2015. Individual Information Security, User Behaviour and Cyber Behavior Victimizations: An Empirical Study of Social Networking User. Journal of Technological Forecasting & Social Change. Elsevier, Kingston University, UK.

19. Spence, P.R., Lachlan, K. A, & Rainear, A, M. 2015. Social Media and Crisis Research: Data Collection and Direction. Journal of Computers in Human Behavior, Elsevier, University of Kentucky, USA.

20. Systematic Reviews. Guidelines for Undertaking Reviews in Healthcare. 2009. Center for Reviews and Disseminations (CRD). University of York. UK. ISBN 987-1-900640-47-3

21. Wardlaw, J.M. 2010. Advice on How to write a Systematic Review.

22. Watters, P. A. 2012. Challenger to Automated Allegory Resolution in Open Source Intelligence. Third Cybercrime and Trustworthy Computing Workshop. University of Ballarat. Australia.

23. Wiil, U. K. 2011 Counter Terrorism and Open Source Intelligence: Lecture Notes In Social Networks. Vol 2. 15 – 28. Denmark.