IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received May 28, 2022, accepted June 11, 2022, date of publication June 16, 2022, date of current version June 22, 2022.

Digital Object Identifier 10.1109/ACCESS.2022.3183642

A Comparative Analysis of Information and Artificial Intelligence Toward National Security

MOHAMMED NASSER AL-SUQRI[1] AND MARYAM GILLANI[2]
[1]Department of Information Studies, College of Arts and Social Sciences, Sultan Qaboos University (SQU), Muscat 123, Oman
[2]School of Computer Science, University College Dublin (UCD), Dublin 4, D04 VIW8 Ireland

Corresponding author: Maryam Gillani (maryam.gillani@ucdconnect.ie)

This work was supported by University College Dublin, Ireland.

ABSTRACT Information is inevitable when it comes to national security. The information revolution seems to hold the massive potential to strengthen national security against current and upcoming threats and cyber-attacks. However, advancements in information accessibility possess innumerable complications for retaining stable national security. One of the preeminent information sources is social media which certainly raises information manipulation factors and destabilizes national security. To accomplish better national security plans, information technology can help countries to identify potential threats, share information securely, and protect mechanisms in them. Artificial Intelligence (AI) is one of the smart areas that robustly facilitates secure information handling to avoid threats and cyber-attacks. It intelligently scrutinizes information available to the public through social media and assists in refraining negative effects on national security. This research article widely focuses on four main analytical milestones; 1) Information available to the public 2) Information affecting national security 3) Risks of cyber-attacks 4) AI as paramount to national security for accomplishing competent information role. Our principal objective is to demystify information accessibilities perspectives for readers to understand the fundamentals of information accessibility and inaccessibility corresponding to national security. To support and manifest our milestones and objectives, Systematic Literature Review (SLR) is methodologically adapted to draw suitable conclusions and develop a farsighted model and frame of reference. This paper concludes with AI tool based categorization, algorithmic function and domain-specific analysis with area-based limitations to highlight current needs. Above all, this article is a thought-provoking kick-start for many naive social media users that usually avoid information-bearing elements and are victimized by cyber-attacks followed by national security compromises.

INDEX TERMS Artificial intelligence, cyber attacks, information role, information security, national security, social media information.

I. INTRODUCTION

National security is highly interconnected with the conduct of information. Various mechanisms have been developed over the years to address information handling [1]. However, the rapid and comparatively recent diffusion of social-media-based information, while bringing numerous benefits, has also demonstrated the urgent need to craft new national security mechanisms to cope with deteriorating circumstances. The Computer Emergency Response Team (CERT) for the Software Engineering Institute (SEI) [2] reported that security incidents are doubled every year followed by an increased growth rate since 2001. In response to these figures, there is a huge amount of security incidents that are never reported. The national systems of security largely rely on information that impacts current and future changes irrespective of national security interests [3]. National security systems are largely dependent upon information spread through various anti-national channels.

National security can be defined as to national strategy to ensure the protection of a nation's fundamental and enduring needs while protecting every citizen's essential safety needs with personnel and social values [4]. The exploitation of national security interests manipulates the desired security territorial parameters resulting in defamation of national values, interests, and global relationships [5]. Social media is by

The associate editor coordinating the review of this manuscript and approving it for publication was Jerry Chun-Wei Lin.

far the huge platform with billions of users posting the bulk of information per second anonymously which poses concrete threats to sustaining stable national security [6]. Online disinformation is an ongoing situation that is currently defenceless and adds worry to regulating the flow of information violating the principle of free speech [7].

Information circulating through various means is not obliged to spread within secure parameters [8]. For example, information on social media may also hinder national security. Social media information acts controversially in information warfare. It is used as a handy tool by hacktivists and criminals for cyber-exploitation, hacking, and extortion purposes [9]. Social media accounts and pages are critical to national security as millions of users interact commutatively at a given time providing immense exposure to national vulnerabilities and reputation damage.

Disinformation played a massive role in destabilizing national security measures without putting additional effort. It has become a partisan issue that has potentially paralyzed national action plans [10]. The heaviest price for being online is paid through circulations of fake news also known as disinformation or spam information. However, all categories of information (disinformation, spam information, fake manipulation of information, partial information) are resulting in a peculiar mixture of apprehension and inaction [11]. Information is also flooded with foreign meddling depending upon the other national enmity and intentions to dysfunction the national security.

To prevent facing threatening situations, Artificial Intelligence (AI) plays its part in the digital developments and implications for society of the information revolution [12]. AI-powered social media information monitoring tools can contribute as social listening tools to confront social information profiles and audiences. The involvement of AI to interpret social data information at different scales can facilitate investigating what's being said in them along with extracting culprits based on that information [13]. AI as content smarter in dealing with content-generating bots with information actions inspection as illustrated in Figure 1 through a hierarchy of stages and its sub-domains and related fields.

This research article covers the role of information in national security concerning the availability of information accessible and available to the public while critically scrutinizing the impact and effects of cyber-space complicity. More precisely, the objectives and milestones of this article are enumerated as follows:

1. Role of information specifically circulating on social media platforms concerning its effectiveness and potency on national security measures are potentially highlighted, discussed and analysed to pinpoint information role in national security.
2. Cyber-space rivalries, cyber-attacks, cyber-thefts, disinformation campaigns, and the potential risk of cyber-concerned factors are extensively discussed and explored to provide a broader and comprehensible vision to deduce substantial reasoning to measure and prevent national threats and attacks.
3. AI stance and aspect for national security relief and assistance to fight against dis-informers and various cyber-divisions i.e. to discuss AI fight to tackle digital information war against national interest is another cardinal objective of this research article.
4. Another objective is to disclose information circle for cyber-space violation that briefly discuss and highlight the interconnected linkages for traceability and tracking.
5. A model to limit/control information is designed and presented along with functional algorithm for possible tracking and stopping of social media information that is targeting and destabilizing national security.
6. Moreover, challenges and information gaps for national security are broadly and extensively covered to portray cyberspace violations with respect to national security. The proposed dendrogram presents broader picture of various connected recent factors of information flow and national security threats to diversify readers vision.

This article encapsulates a precise perspective of information's role in national security measures. However, the significance and novelty factors of this research article are as follows:

1. The existing surveys are neither comprehensive nor they are based on Systemic Literature Review. Moreover, to the best of our knowledge, existing does not cover all aspects regarding information coming from social media and its menace to national security.
2. The existing surveys are not up to date [14]–[16] and do not include recent works on artificial intelligence in the field of information role and national security measures.
3. Another significant aspect is application-specific analysis of artificial intelligence approaches that is not provided in the earlier literature.
4. AI Tool's categorization and analysis with respect to information flow specifically on social media is another distinguishing factor of this article that makes it different and significant from the rest of the literature viable so far.
5. Information authentication and in-authentication model is designed and supported through a functional algorithm along with utilizing the AI frameworks through series of steps for tool assistance.
6. The motivation and primary intention of this article for contributing towards knowledge is to comparatively analyse information and artificial intelligence towards national security to enlighten the threatening factors related to cyberspace violation, social media manipulators, and disinformation campaigns and their intensifying effects, measures and possible precautionary steps.

Research articles [14]–[16] discusses narrow scope rather than considering broader area. They identified weaknesses, strengths, and challenges along with threats and opportunities. While we focussed on designing a model and functional algorithm for potential solution against national threats, cyber-space violations and social media manipulators. Secondly, social media information circulation is less explored in these articles whereas we considered social media information analysis with much detailer context.

The rest of the article is organized as: Section II covers relevant background and literature review; Section III gives a detailed overview of systematic literature review parameters taken as a methodology with a brief knowledge of research questions and exclusion/inclusion criteria. Section IV, V, VI, and VII analytically cover the proposed research question along with supporting models, algorithm, and graphical representations. Section VIII concludes the paper.

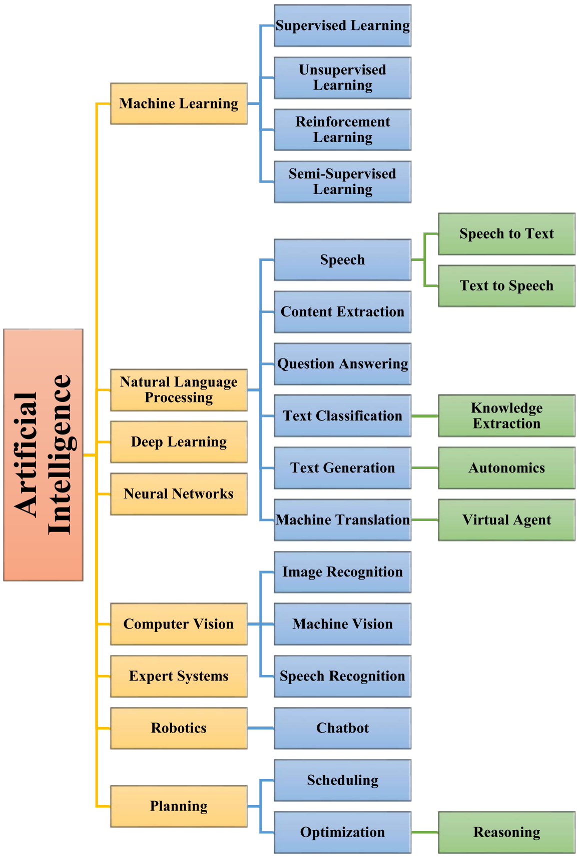

FIGURE 1. Hierarchal representation of AI areas critical to Information for National Security.

II. LITERATURE REVIEW

The twentieth century has witnessed the most lethal and kinetic wars in the history of warfare and information sharing surfaces [17]. Whereas, the twenty-first century dawned with a multi-fold of information conflict that is on verge of bringing cyber-wars to destroy national security plans and features [18]. Physical wars with man force and weapons are now replaced with state and non-state actors to take control of significant places in cyber-space having aftermaths for the physical domain. Cyber-space freely allows these actors to extend their powers based on information manipulation corresponding to the social media domain at a much larger scale without any physical barrier. This was thought to be impossible earlier.

Social media is not only a technological life force that connects, informs and shares a common platform with millions of users, but also has the power of strong non-existential attacks to strike national securities [19]. Social media has assisted people globally to organize and plan aggressive riots, recruit terrorists, plotting attacks, glorify national wars, gangs compilations, and spread violence in response to minor/major events [20]. The credit for such activities goes to the information circulation on social media that has affected national security plans at a greater rate. These strong transitional waves not only amplify disastrous action but also coordinate actions against government and law enforcement [21].

To control information exchange, information manipulation control is the dire need of this time. The world is on verge of being extinct with peace if suitable measures are not taken timely and correctly. Artificial Intelligence has shifted the paradigm and contributed to managing information needs on various social media platforms [22]. Artificial Intelligence work through social media bots that spy through content smarter algorithms [23]. These algorithms act more swiftly than the opposing bots while learning, changing, and altering speed is way more dynamic. Real-time automated blocking is a better choice for creators as well. It allows smart blocking of users that target them with malicious attacks. One such algorithm and model is proposed in section III.

Cyber-space allows invaders to extend their powers in the social media domain with a much faster pace and ease which was considered impossible earlier [24]. However, Artificial Intelligence deals perfectly with state and non-state actors to stop misusing the marketplace of ideas and beliefs on this digital battlefield of Cyber-war. According to USA social media unit, information available on media brings tremendous threats to national security primarily relevant to social engineering, web applications attacks, and phishing threats [25]. Due to such unforeseeable consequences, the USA has banned Twitter and Facebook officially at government organizations.

Information damages national security by destabilizing the national causes in terms of generating huge economic losses. In 2013, the social media of a well-renowned press group was hacked and released news about two explosions at the white house resulting in injury to the President. This news was reached to the US stock traders within two minutes and it dropped 143 points i.e. $136.5 billion estimated loss. Few other prominent and highlighted cyber-attacks related to retrieve and manipulate information are hacking email accounts of CIA Director John Brennan and James Clapper, Director of National Intelligence; the 2011 RSA SecureID Cybersecurity attack; the 2016 Democratic National Committee email leak and the mysterious 2014 Sony Pictures hack, Brexit campaign, US elections by Cambridge Analytica [26].

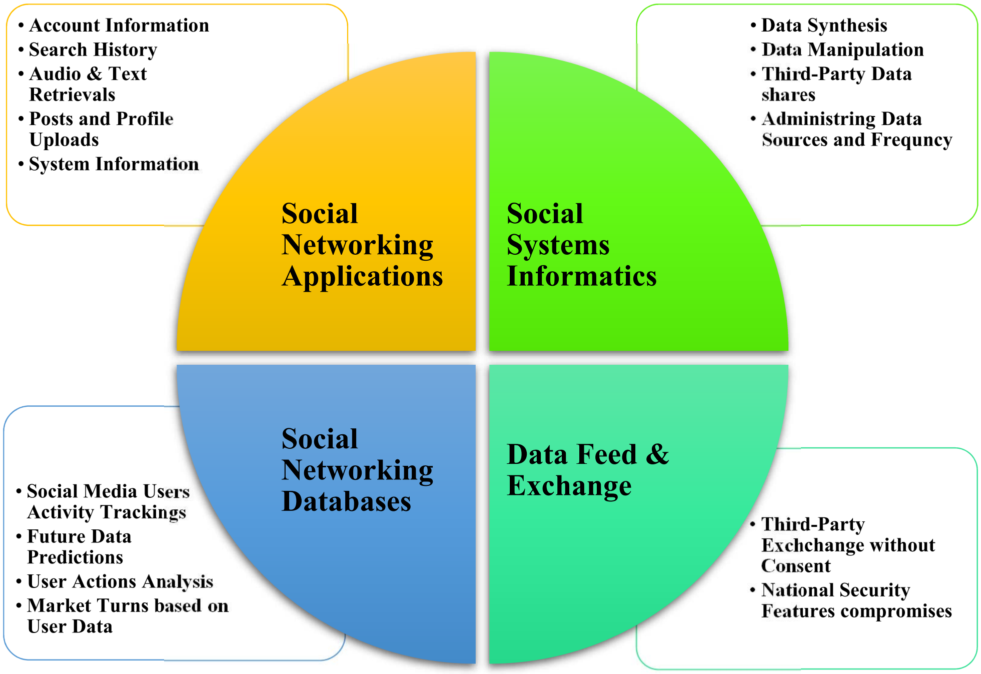
• Account Information
• Search History
• Audio & Text Retrievals
• Posts and Profile Uploads
• System Information
Social Networking Applications
• Data Synthesis
• Data Manipulation
• Third-Party Data shares
• Administring Data Sources and Frequncy
Social Systems Informatics
Social Networking Databases
• Social Media Users Activity Trackings
• Future Data Predictions
• User Actions Analysis
• Market Turns based on User Data
Data Feed & Exchange
• Third-Party Exchchange without Consent
• National Security Features compromises

FIGURE 2. Information Cycle on Cyber-Space and its integration with Social media.

Another prominent and most recent cyberspace violation with potential intervention for derailing national security was Google+. Google+ came to an end after 500,000 Google+ users data security was compromised when the private information of such a huge amount of users was breached raising shocking results afterward [27]. Many government officials were reported to be blackmailed after this incident reporting.

Information solely impacts the national security as crucial information like enemy's logistics, operational elements, training schedules and institutions, weapon ammunition details, army sensitive movements along with sensitive defence catalogues are majorly taken from social media through cyber-space violation [28]. Information-driven companies are suspiciously getting monitored and information can spread swiftly while bringing the negative impact of believing false information about national security. National security is on the verge of getting playful in the hands of anti-national movements that stays hidden while effectively targeting desired national interest.

Information-bearing element pressurizes the policymakers to react to domestic and international security differently that resulting in affecting national plans differently [29]. Instead of imposing bans on social media usage, national security agencies should implement information controlling laws that can restrict and filter information sharing capabilities of social media. This factor is only accomplishable through Artificial Intelligence discussed in detail in the following sections.

Figure 2 illustrates the information cycle in cyber-space and how social media is relevant as an integral part of it. Social networking applications and social systems informatics are in a coordinated bond to facilitate data synthesis, data manipulations, and third-party data sharing. Social systems informatics administers data sources and frequency closely functional with networking applications. It is more like a highly connected feature in which one information sets trigger others and the loop continues until a suitable audience is targeted and informed. While social networking application facilitates and provides users account information, their shared information along with search and interest history.

Most importantly, audio/video and text retrievals hold credible information to utilize against national security [30]. This set of information also helps in manipulating a user for fraud, blackmailing, and sometimes using a person against national interest [31]. As shown in Figure 2, the other two primary factors are social networking databases and data feed & exchange. Information in an organized form creates a database.

A social networking database provides complete sets of linkages that exist between millions of users. For example, a database for all residents of Oman is supposed to have the same data linkages and can be broadcasted with desirable information within a matter of seconds based on factors such as age, racial and ethnic groups [32]. Any information intended to manipulate can be spread based on such links while risking national security and national action plan.

Figure 2 also presents social networking databases contribution toward future data predictions, activity tracking, market trends, and users response rates in response to any national threats. Data feed features extend national compromises.

TABLE 1. Summary of query words and relevant search filters and results.

S. No	Search term	IEEE		Elsevier		ACM		Taylor & Francis		Springer	
		Count	Filter	Count	Filter	Count	Filter	Count	Filter	Count	Filter
1	Role of information in national security	956	OR	1002	OR	180	AND	1	OR	9	OR
2	Tools for information synthesis	1138	OR	987	OR	682	AND	0	OR	13	OR
3	Artificial Intelligence for national security	3952	OR	4456	OR	559	AND	0	OR	11	OR
4	National security based parameters	1568	OR	1128	OR	462	AND	0	OR	10	OR
5	Artificial Intelligence social media tools	345	OR	246	OR	103	AND	0	OR	13	OR
6	Social media constraints for national security	3	OR	15	OR	4098	AND	0	OR	0	AND
7	Social media prevailing factors	3	OR	14	OR	3969	AND	0	OR	0	AND
8	Information and national security relatedness	2	OR	1	OR	558	OR	2	OR	5	OR
9	National security and social media	271	OR	35	OR	102	AND	3	OR	438	OR
10	Social media information threats	276	OR	1663	OR	3282	AND	65	OR	0	AND

Even if a resident of a country lives outside the country's premises, a data feed still reaches through a mobile phone based on data links to trigger outrage. This factor is also accomplished through third-party data shares without consent [33]. The power of social media has unearthed the socially constructed information bombs that can act as a targeted disaster for national security within a few seconds while costing nothing.

III. METHODOLOGY

This study has been undertaken as a Systematic Literature Review (SLR). This review entails a thorough, transparent, and replicable process for literature search and critical analysis. SLR as a methodology allows incorporating quantitative reasoning for the research questions with valid supporting arguments to build better research subjects. The SLR process is guided by [34] recommendations. The review process catered from [34] is followed as (a) Scoping (b) search and analysis (c) peer-reviewed papers selection guided by research questions. The research questions are designed to fulfil the current and latest subject of study. Research questions are formulated below.

Research Questions addressed in this article are:

1. **RQ1:** What kind of information is available to the public corresponding to national security through social media?
2. **RQ2:** How Information is affecting national security over time?
3. **RQ3:** What are the current and future risks of cyber-attacks, cyber-space manipulation, and Cyber-wars resulting from information driven media?
4. **RQ4:** How Artificial Intelligence is acting paramount to national security for accomplishing competent information role and acting as a saviour for national security?

A. SCOPE

The review is designed to scope only papers that specifically use the term '*Information*' and '*National Security*. This scoping allows a better and targeted review of our area of interest within the role of information for national security along with AI applications in such cases. According to [34] defined SLR recommendations, identification of synonyms and alternative terms are given in Table 1. Search terms are the query words that are used to dig out peer-reviewed research articles. There is a lack of definite systematic coverage of work on the role of information for national security, but this factor does not limit the interpretation of the findings. Alternatively, we have considered the closest general literature for our proposed area of study.

The relevance and clarity are checked by readings abstracts and concluding points of articles. The complete coverage of inclusion and exclusion criteria with stats of articles on elected journals are given in Figure 3. Figure 3 shows various parameters based on title-based rejections, abstract-based rejections, and selection based on a general and detailed study of selected research to cover a credible and broader area of research.

B. SEARCH AND ANALYSIS

For comprehensive search and analysis, relevant peer-reviewed literature is searched on credible search engines i.e. Google Scholar, Scopus [35], and Web of Knowledge [36]. As far as operational criteria for filtering are concerned, we have excluded papers where definite usage of information among national securities was of least concern. Secondly, articles with generic discussion in response to our query terms are also excluded. For inclusion, papers with combined use of '*Information*' and '*National Security*' and clearly stating our intended purpose of research are considered.

C. OVERVIEW OF REVIEWED PAPERS AND REFERRED WORKS

The earliest identified research article on the role of information in national security is almost 20 years old. However, the majority of the papers are considered from 2010 to 2021 to mainly target the recent digital era. The complete coverage of query responses and stats of articles on elected journals are given in Table 1. Table 1 also illustrates the publications years of the selected papers with their conferences and journals categories differentiations.

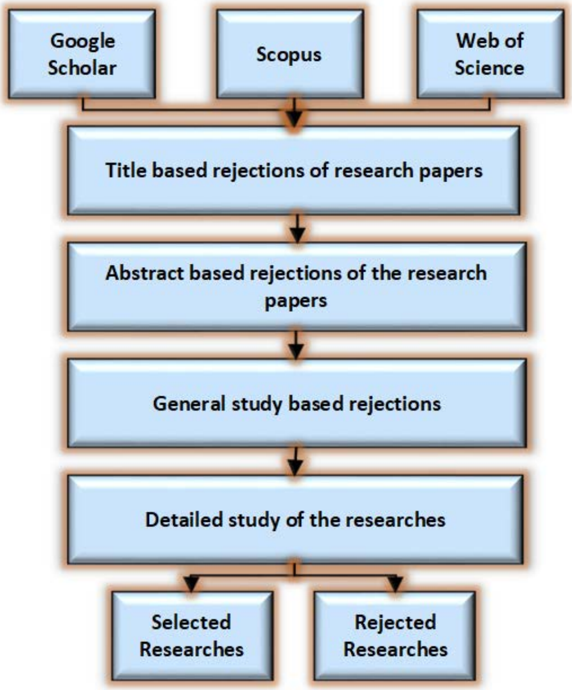
Google Scholar
Scopus
Web of Science
Title based rejections of research papers
Abstract based rejections of the research papers
General study based rejections
Detailed study of the researches
Selected Researches
Rejected Researches

FIGURE 3. Exclusion and Inclusion Criteria.

IV. INFORMATION & ITS IMPACT ON NATIONAL SECURITY

Information significance can be determined through the extent of being lethal on the fact that how fast the information can spread and how greatly the impact of believing false information can bring destruction to national security [37]. The huge relevance of social networks and the information available to them are the global setbacks that spurred the interest of national policymakers in response to retaining security [38]. The tremendous influence and pressure through information from social media platforms like Twitter and Facebook can conceivably derail domestic and international relations within less or no time [39].

The global national lawmakers believe that instead of denying the effective applicability of social media information and dismissing social media for being highlighted as a threat to national security, one should ensure the information sources and its credibility before it can reach to every citizen [40]. Information can be scrutinised and validated before it can be made available to the entire nation for better prevention of any actors wishing to spoil national securities [41]. It is desirable to locate whether the information circulating through social media should be considered trustworthy to root out its validity and credibility.

Information circulated through convention ways and Cyber-ways hold different spreading strengths and aftermath results [42]. The cyber-warfare has moved information sharing capabilities of a common person beyond controlling powers [43]. Change in audience and platforms now become a weapon of choice for national anti-security agents. Enabling information sharing capabilities to every person in use should be passed through defined filters to protect any negative and unforeseeable circumstances [44]. AI has the potential to apply filters and scrutinized the desirable checks on information to possibly control the national security plans and measures described below.

A. UNDERSTANDING AI-NEEDED FRAMEWORK FOR NATIONAL SECURITY

Online social networking is consistently showing explosive annual growth. After becoming the most widely used and adaptable information source, it caters a great deal to national interests [45]. Targeted advertising and viral marketing are introduced to exploit social information without prior checks and scrutiny [46]. False information tends to spread faster because re-sharing facility available on media platforms. To remove false information requires removing it from all associated people who already have shared it.

Removing threatening information is a seemingly tedious task, but eradicating its impact on people is much more threatening as well as challenging [47]. The everyday lives of people increasingly depend on online access to information and its related services. The manipulation of social media users through cyber-space is efficient yet convenient [48]. The effective differentiating between authorized and unauthorized information sources can significantly help to stop misinformation in the first place.

Information can be made stoppable and accountable by incorporating very easy checks proposed in figure 4. In figure 4, we have proposed a simple model that can act wisely to limit the spread of information to limit national compromises. As per the Model, information is derived from two sources 1) authentic sources such as approved users, national organizations, and government-owned media channels. 2) in-authentic sources such as millions of social media users and privately owned information broadcasting groups. In-authentic sources are effectively subjected to AI frameworks based on the requirement. Social media information is not only text-based. It also originates from Images, videos/visuals, and speech/audio contexts that can be significantly monitored through AI frameworks highlighted in the proposed model. After passing through extensive filtering and checks, information can either be approved (allowed to share by potential users) or disapproved (dumped). Detailed

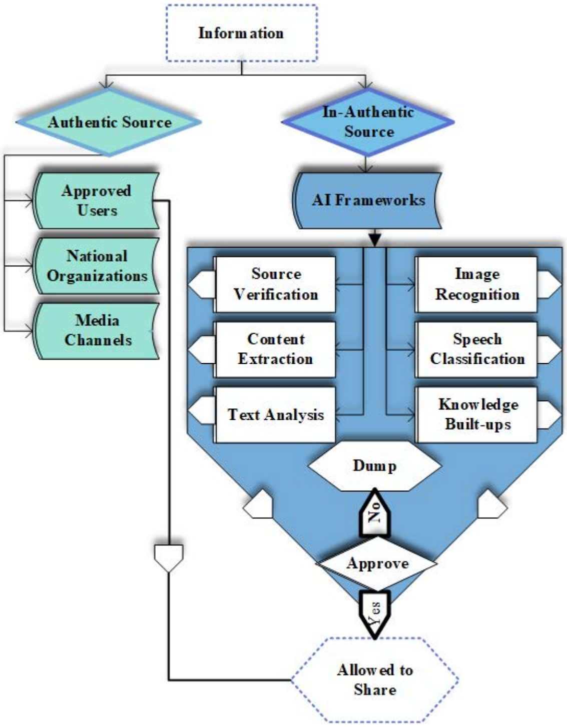

FIGURE 4. Model for Limiting Information.

Algorithmic functions are described in Algorithm 1 that explains step by step functional operations.

The AI frameworks proposed in the model can cater to issues like false information spread, anti-national users, stability threats, and filtering of information. This model encapsulates every information context i.e. Sources verification, content and text analysis, image and speech classification, and knowledge built-ups all collectively powered by AI mechanism. Moreover, it can also help in locating the source of information. In-authentic sources should always be checked before they can perform a certain action. AI mechanisms used in our model are discussed in the section below.

B. AI-BASED SOURCE IDENTIFICATION MECHANISMS

The source identification and information origin locating are critical factors to target the potential source of misinformation to snub them before they reach millions of users [49]. The social media accounts holder that is maliciously involved in cyber-space violations are hard to track and thus continue their anti-national mission to destabilize the actions plans [50]. The fear of getting caught and being traced is vital in counter-attacking such sources and tracing their backend supporting bodies.

AI-based source identification mechanisms can add great support for the tracing and locating features [51]. AI mechanisms have facilitated the tracing of data sources and their relative linkages with greater ease from the larger sets of data in seconds [52]. AI has penetrated its roots for tracing social media information and provides source trees for better traceability features in a matter of seconds. A large number of users were once difficult to manage and now AI introduces a mechanism that brings better traceability with high data volumes [53].

Algorithm 1 Information Authentication/ In-Authentication, Retrieval, Rejection, Approval.

```
Function Information_ Authentication {
While $\cap$ is unapproved information
 If $\cap \epsilon I(i)$ & $\cap \neq i$ and
u(u) = verification $(u(x|x \epsilon I(i))$
 then
   Approve to $I(i)$
   Declare I as Authentic
 Else If $(\theta)$ then
   Select $(i) \rightarrow$ Inauthentic
    If $\sum I(i)$ selects i as $\cap$ then
       $\cap$ transmits message to AI Frameworks
  checks
    End if
 End if
  End while
  }
  Function I_Rejection {
  Set information to Sink, information to
  AI_Report_User
  Send (information_message)
  }
  //Receive I message from U users
  Function recv_users_Credentials (){
   Set users [n][o] to $U_{ID}$
   Set users [L][1] to $U_{LOC}$
   Set users [IP][2] to $U_{IP}$
   Set users [A][3] to $U_{Attempt}$
  Set users [P][4] to $U_{IDpic}$
  }
  Function recv_users_Credentials {
   For $i = 0$ to N
      Allocate users to Dump Seg [m] by using
      $U_{ID}$, $U_{Loc}$, $U_{IP}$//d is index for segment
  Dump
   End For
   }
   //Authentic Procedure –– At AI Framework
   Function Authentic (){
   If $(\grave{A}) \rightarrow U(\upsilon)$ then
      Send Approve $(P(\rho)) \rightarrow$ (Media,
   National_Organization, )
      (P, users) $\leftarrow$ (u, $\emptyset$)
   Else
      Send Credentials $(U_{ID}, U_{Loc}, U_{IP}) \rightarrow$ AI
   Framework
   End if
   }
```

AI provides possible support to accurate mechanisms handling that shows great potential that information sources/users can easily locate out of millions of users. Few such mechanisms are:

1) ARTIFICIAL NEURAL NETWORKS (ANN)

For everything that is not meant to be easily tracked can be easily sorted out through neural networks. ANN proposes tools where humans are allowed to handle architectural decisions while optimization and traceability features are controlled and performed by networks mechanisms. ANN helps to develop associated links along with optimizing networks [54], [55].

2) SCIKIT-LEARN

It underpins unsupervised learning calculations to create choice trees and bunching group illustrations. It presents a very calculated and targeted order with an additional feature of information change. Information change at any stage can also be traced through feature determination and ensemble techniques that can be accomplished in a couple of lines and less time [56].

3) THEANO

It enables information counts up to multiple times to give calculated figures about how many times a piece of information is shared. It eases complex computational tasks for locating the number of users. A very essential feature to discover the severity of information spread [57].

4) MXNET

It is useful to tackle the whole set of new host devices and newly entered devices to align with a community-developed framework [58].

5) KERAS

For image recognition problems and picking a suitable architecture, KERAS can contribute well. Information sources available on social media are not only broadcasted and shared in textual format. Images are equally threatening for cyber-space violations [59].

6) H20

Risk and fraud analysis is a much-needed feature provided through H20. It used predictive analysis, insurance analytics, and advertising applications along with customer intelligence. Customer intelligence allows keeping activity records to produce required results without running extensive search activities [60].

C. NATIONAL SECURITY AND CONTROLLED INFORMATION PROCESSING

One of the prime advantages of social media is that it allows the government to share critical information in a crisis. One such incident is that benefitted the government reported in Turkey back in 2016 [61]. Turkey's president Erdogan used social media to beat military tanks through a powerful source of information to call the Turkish nation. Successfully, Turkish rebellious attempts were suppressed and Erdogan managed to sustain peace [62]. Reportedly, the plotted rebellious act was largely communicated and circulated through social media.

After surfacing such events, national security measures of different countries started taking different measures. Globally, the information controlling measures of social media to prevent national security varies and holds different choices and preferences. Some of the countries seem to be rigid while others are a bit relaxed in this regard. For example, China and North Korea are the top listed countries for controlled social media and all other heavily censored information-seeking platforms [63], [64]. All information passes through strict barriers before it could reach other audiences.

Moreover, these countries also impose penalties for the user violating the national security plan. Iran is another prominent country that strictly blocked all social media platforms along with heavily censoring political media to secure national stability. After North Korea, China and Iran, there are other countries like Belarus, Qatar, Syria, Thailand, and UAE that are rigid in heavily filtering the information being spread to deal better with national security [65]. Europe has also imposed suitable restrictions [66]. These countries have restricted social media as well as strongly monitored communication application barriers that limit information sharing rapidly and in controlled measures. Above all, most of the Gulf States have already discontinued wi-fi calls to keep stronger checks for stabilizing national security [67].

D. DIFFERENT POSSIBLE ATTACKS

Social media data and information is not the only factor that facilitates national security compromises. There are other different possible attacks by which national security hamper. The different possible attacking factors are however information driven majorly. For example, text messages, voice calls, fax, emails, pamphlets, printed information, and various other print media resources. Aforementioned sources are separate from social media but they are vital and strong enough to provide support to attacks and destabilise national security. Information dissemination sources either from social media or outside social media disturbs the national interest equally. However, social media works with fastest pace in comparison with other means. Detailed possible attacks with wide area coverage are mentioned in figure 6.

V. INFORMATION EVOLUTION OVER THE COURSE OF TIME

In less than a generation, information exchanging platforms have significantly evolved from merely a time-consuming electronic exchange to virtual real-time efficient 21st-century information centred tools [68]. Within a few years, social media has affected the lives of billions of people. We are now living digitally transformed lives where information is acting as one of the leading factors in driving how to lead a life.

The 1980s and '90s are considered to be a prominent era where emails and online servers like America Online [69], Prodigy [70], and CompuServe [71] acted as networking platforms but were somehow lesser-known and only limited to online chatting. At the earliest of 2000, Friendster [72] came as an attractive platform for millions of users and was limited to basic online interactions. 2002 was LinkedIn [73] launching year in which career-minded people were hosted that is now grown to more than 675 million users worldwide. However, this site only targeted job seekers interests and did not facilitate information violating national concerns.

2008's Facebook, 2011's Myspace, and 2012's Google+ acted as pivotal mediums for Information exchange mediums [74]. Within a short time, 72% of U.S adults use social media platforms and share information without any checks and filters. It is astonishing to note that 6000 tweets are sent per second which is 350000 per minute and 500 million per day and 200 billion per year [75].

Information evolution is not restricted to merely users' profiles platforms but has broadened its dimensions towards streaming videos platforms, weblogs and Blogs to provide a sense of being authentic and genuine [76]. For example, information exchanged by personnel users might not stark a controversy as swiftly as a blog owned by a well-renowned media agency can do. Various video-based channels can destabilize too.

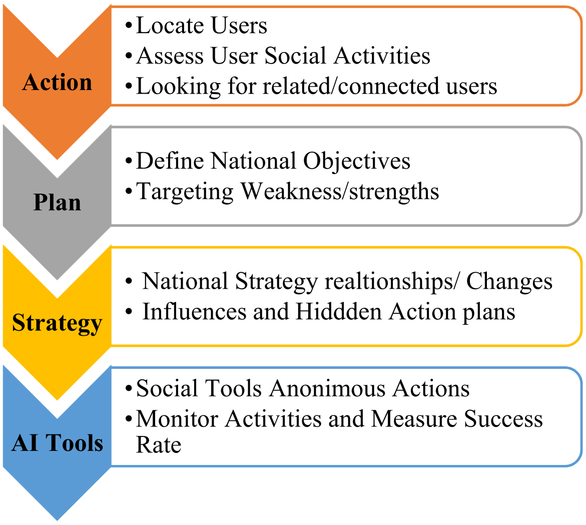
Action
•Locate Users
•Assess User Social Activities
•Looking for related/connected users
Plan
•Define National Objectives
•Targeting Weakness/strengths
Strategy
• National Strategy realtionships/ Changes
• Influences and Hiddden Action plans
AI Tools
•Social Tools Anonimous Actions
•Monitor Activities and Measure Success Rate

FIGURE 5. **Course of action for information ages.**

During the pre-social media time, information was communicated to inform others and never meant to be manipulated. Most of the time, newspapers, magazines, and journals were distributed once a day and thus any details and information is supposed to reach after hours. There was a penalty of time to check the authenticity of information [45]. Now, the case is different. Information spreads more quickly than information negating the previous information.

A. INFORMATION AGES AND COURSE OF ACTION

There are two information ages i.e. Primary information age and secondary information age. The primary information age is about the era before the internet and is mainly comprised of newspapers, radio, and television [77]. Mostly, the information sector was government-owned and excellently controlled, and slow. The secondary information age is the era of the internet and satellite television. Information sharing is based on quick platform that is privately owned without any filter, controlling checks, or government intervention [78].

The tertiary information age is the current era that is connected with mobile devices with millions of users having the liberty of sharing information without prior scrutiny. In other words, viral advertisements and hype-giving content are greatly supported to destabilize national security plans [79]. The tertiary information age is potentially threatening as well as risking nation interest with greater intensity. To compete with transforming information ages, Figure 5 that illustrates a four-step plan of action that vigilantly performs its action to deal with the tertiary information age as follows:

1) ACTION

The very first step is Action, which needs to be functional based on real-time response. Action to locate users and interpret their social activities against national interest can eradicate anti-national movements from the very beginning. Locating and tracing connected users that might be acting as co-culprits can also risk down the potential source of cyberspace violations.

2) PLAN

The second step is planning before executing a strategic national action plan. This step is based on national objectives and agenda. Planning a suitable course of action can contribute to prediction analysis for future correspondence. Above all, Targeting and rooting out the strengths and weaknesses of attackers are other aspects gained through accomplishing this step.

3) STRATEGY

National strategic measures are vital and confidential in sustaining security and dealing with upcoming changes. Define strategy and make it confidential to attack hidden action plans. The robustness of strategic measures helps retain flawless security.

4) AI TOOLS

AI-based tools as described in the model are corrective and the right use can contribute to locating anonymous activities [22]. Monitoring activities and catching culprits with suitable penalties can lower the risk of future setbacks. Above all, AI tools can also ensure the measurement of success ratios against implemented national security plans. Refer to IV (B).

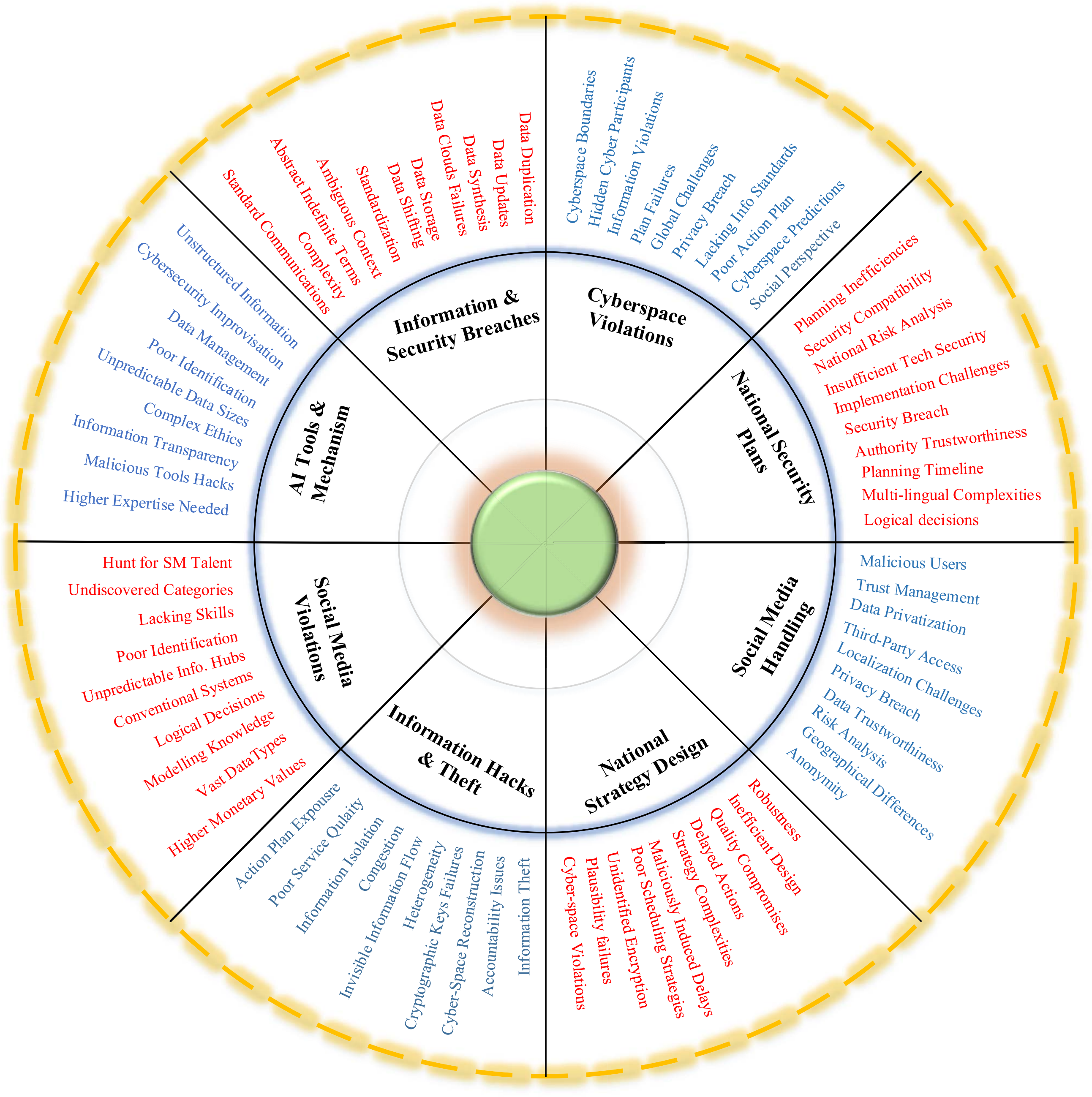

FIGURE 6. Dendrogram for Challenges and Information gaps for National Security.

VI. CURRENT AND FUTURE RISKS OF CYBER-SPACE VIOLATION TO NATIONAL SECURITY

There are many current and future risks of cyber-attacks, cyber-space manipulation, and cyber-wars resulting from Information driven media. Things are inevitably going out of hand because of severe cyber-space violations [80]. The most important area greatly affected is national securities. Physical wars are now shifted to virtual cyber wars where demoting a country's national progress and agenda is much simpler than using deadlier weapons and actual armies.

Currently, social media has reached 5 billion mobile devices users worldwide [81] and the network has anchored its roots deeper to feed users minds within minutes. These information spilling devices are being carried by users wherever they want hence assuring information accessibility at its best and situation as worst for cyber-attacks [82].

Specifically, government and army officials are high targets when it comes to stealing sensitive information for targeting national securities [83]. The current fact is that our digital lives appear to be completely and utterly susceptible to cybercriminals and spies. A flurry of cyber-attackers is

TABLE 2. **AI tools for information assistance on social media.**

Tool	Purpose	Preferred Application Areas
DeepText [104]	To understand conversation better for information processing, Translation of different languages	Social Media applications specifically Facebook
FBLearner Flow platform [105]	To run thousands of user classifications along with content understanding	Primarily developed, used, and adapted by Facebook
MonkeyLearn [106]	To gain insight from social media Text data.	Natural language processing based social media applications
Aylien [107]	To deal with large volumes of real-time content from the new outlet and social media content	Academic publications, New reporting applications, entity extraction, and sentiment analysis platforms
IBM Watson [108]	To deal with information available on Clouds based on extracting keywords, categories, and entities.	Specifically designed by IBM to tailor industrial information needs and dive documents.
TextBlob [109]	For text classification, part-of-speech tagging	Excellent, easy, and user-friendly interface for easy and beginners applications.
GenSim [110]	Recognizing text similarities, text indexing, and navigating text documents.	For handling large volumes of data that needs a fast and scalable solution.
FAIR [111]	Facebook Artificial Intelligence Researchers tool to analyze and develop AI systems with the intelligence level of humans.	For AI-based research and innovation. Specifically, Facebook (a social media application) uses FAIR.
CRM[112]	AI-powered automation platform designed for scheduling a call and other audio-aided features.	Every social media application allows users for making/scheduling a call thus it is used by almost all current applications.
Chatbots [113]	Intelligent and self-supported auto answer generator (in response to user questions).	Specifically used for automated customer help, and widely used in online selling and buying websites.
rasa.io [114]	For one-to-one conversations for millions of contacts	Marketing, subscribing, and other broadcasting applications.

clinging to the biggest national organizations to get sensitive information that matters most for the country's dignity and security [84].

Among various risks of cyber-space violation, few risks are shaking the securities parameters with greater ease. Ransomware Apocalypse is one of the keys and the popular phenomenon of cyber violations [85]. The malicious global attackers ask for a healthy ransom with a threat to share the information publically if conditions are not met. Cyberspaces violations are also posing a certain risk in dealing with global cyberspaces. Every cyberspace is following different standards and protocols [86].

A recent example is the U.S Intelligence 'SolarWinds' hack 2021 [87] in which hackers gather untold extent of intelligence information from the U.S government and sensitive sector to do blackmailing in response to huge ransom. SolarWinds hack involved targeting three vital US firms (SolarWinds, Microsoft, and VMWare) along with 12 federal agencies (NASA and Federal Aviation Administration) as per reports by Cybersecurity and Infrastructure Security Agency (CISA) [88]. This attack was initiated to destabilize the US reputation and exposed the secrets vital for retaining USA national securities [89].

Figure 6 illustrates in-depth challenges, AI and information gaps for national security recently. There are eight highlighted factors. Social Media Violations is accountable for creating a suitable and skilled team that can effectively deal with any possible threats [90]. There is a suitable gap in expertise levels to prudently deal with social media attacks [91]. Undoubtedly, manipulators that use social media platforms to create information threats are skilled with high technology specs. To deal with such an expertise level, a higher and more compatible team is needed to cancel the threatening effects [80].

Information hacks and theft are another way to risk national security. The planned course of action by the national agency is threatened with theft which makes hackers more powerful to counterstrike the national plan [92]. Action plan exposures are dangerous and cause invisible information flows. Even if the information is stored through suitable encryption and decryption features, stolen cryptographic keys are altered to reveal the information [93].

National Strategic Design is another integral factor that contributes to information manipulation [94]. Quality Compromises along with strategic complexities are possible leading causes. Secondly, maliciously induced delays for strategic actions also allows information to spread that causes potential harm and results in cyber-space violations [95].

Social media handling also contributes to achieving better national security. Malicious and unidentifiable users, third-party access, localization breaches, and trust management among internationally developed social media links are adding threatening elements to national security [96]. Geographical differences (time zone and language barrier) are also vital factors necessary to fix to have stable national security [97].

National Security Plans are established with poor compatibility and inefficiency to deal with global threats. Implementation challenges to executing a defined plan is another way to allow a malicious user to perform their actions freely [98]. Time liberty is itself a very tedious act that directly facilitates intruders.

Cyber space violations include crossing defined boundaries, hidden participants, and incompatible social perspectives for cyberspace predictions. Cyberspace predictions are necessary to anticipate the next possible manipulator's action that might risk national security [99]. The lack of Information standards to do such predictions is also adding alarming situation.

Information and Security Breaches in terms of data duplication, data updates, data cloud failures, data storage, and data shifting are very critical actions that unknowingly facilitate security breaches. Lack of communication standards is also a contributory factor to information and security breaches.

VII. ARTIFICIAL INTELLIGENCE TOOLS FOR NATIONAL SECURITY

Artificial Intelligence is acting paramount to national security for accomplishing competent information roles and acting as a saviour for national security [100]. AI is an inspiring technological platform that is the most powerful tool in generations for benefitting national security [101]. AI is not limited to improving human life for natural problems. IT has broadened the ways of looking into unlocking mysteries that seemed to be impossible and now are game-changing superpowers [102].

AI has anchored its roots in social media-based platforms due to its diverse set of applications and amenities. Table 2 is covering various tools with their purpose and possible applications that can cop-up many of the issues identified above. These tools are providing a solution to many of the current cyber-space problems and are acting as guarding agents against anti-national factors. Every tool identified is unique in its nature application and purpose [103]. These tools are subjected to desirable feature extraction and edition too based upon user selection of choices.

Table 2 Tools are Artificial Intelligence-based and contribute to automating many tedious tasks highlighted in Figure 6. These tools are making social media management controllable along with larger-scale social media monitoring. AI enables social media and its relevant information to better understand national preferences [103]. AI helps to target and eradicate threatening factors effectively and conveniently.

VIII. CONCLUSION

Artificial Intelligence is revolutionizing the information role with its applications and helping solve complex cyber-space problems. AI can provide social media users with real-time information personalization based on their intentions and behaviour. It can be used to edit, forbid, and locate anti-national campaigns to meet national security needs. AI can also help with content scrutiny to find matches of anti-state agents, the national cyber-criminals, and security plan spoilers. It can be used to handle routine tasks like performance analysis, anti-state campaign reports, and much more.

In our article, we have identified AI tools that can help to process social media information to protect national security in a better way. We have identified initial ways of manipulating information to derail national security with current and most recent attacks meant for shaking national security parameters and plans. This paper briefly covers how information can critically get involved in sensitive information retrievals, spreading disinformation, creating spam to drive users' minds falsely, and possible privacy theft for blackmailing purposes with ample examples as limitations of current functional areas.

All the content covered in this article is catered through Systematic Literature Review (SLR) to deduce credible and authentic arguments in response to formulated research questions such as information impact on national security, information evolution, current, and future risks of cyber-space violation to national securities with specifically highlighting Artificial Intelligence as a saviour for national security. In the last section, a list of tools vital for information investigation and analysis with purpose and application area are given to facilitate readers better for information usage and prevention for retaining national security.

FUTURE DIRECTIONS

The possible future course of action for upcoming researchers is to establish all-purpose multi-functional information handling tool for information flow that can help in sustaining better national security measures. Secondly, another future direction is to draw testified and traceable parameters to meet security standards with respect to information coming from social media platforms. These parameters can help to establish accountable measures to catch national threats before they can harm security plans.

REFERENCES

[1] D. C. Rowe, B. M. Lunt, and J. J. Ekstrom, "The role of cyber-security in information technology education," in *Proc. Conf. Inf. Technol. Educ. (SIGITE)*, New York, NY, USA, 2011, pp. 113–122, doi: 10.1145/2047594.2047628.

[2] (2021). S. E. Institute. *CERT Coordination Center*. [Online]. Available: https://sei.cmu.edu/about/divisions/cert/index.cfm

[3] D. C. Mowery, "National security and national innovation systems," *J. Technol. Transf.*, vol. 34, no. 5, p. 455, 2009.

[4] A. Dutta and K. McCrohan, "Management's role in information security in a cyber economy," *California Manage. Rev.*, vol. 45, no. 1, pp. 67–87, Oct. 2002, doi: 10.2307/41166154.

[5] T. E. Copeland, ''The information revolution and national security,'' Army War College, Carlisle Barracks PA, Strategic Stud. Inst., USA, Tech. Rep., 2000. [Online]. Available: https://apps.dtic.mil/sti/pdfs/ADA382498.pdf

[6] S. L. Jarvenpaa and A. Majchrzak, ''Knowledge collaboration among professionals protecting national security: Role of transactive memories in ego-centered knowledge networks,'' *Org. Sci.*, vol. 19, no. 2, pp. 260–276, Apr. 2008.

[7] E. C. Tandoc, D. Lim, and R. Ling, ''Diffusion of disinformation: How social media users respond to fake news and why,'' *Journalism*, vol. 21, no. 3, pp. 381–398, Mar. 2020.

[8] S. J. Schwartzstein and W. A. Owens, *The Information Revolution and National Security: Dimensions and Directions*. Washington, DC, USA: Center for Strategic & International Studies, 1996. [Online]. Available: https://www.ojp.gov/ncjrs/virtual-library/abstracts/information-revolution-and-national-security-dimensions-and

[9] V. V. Novikov, ''Digitalization of economy and education: Path to business leadership and national security,'' *Bus. Ethics Leadership*, vol. 5, no. 2, pp. 147–155, 2021.

[10] J. Der Derian, ''Global events, national security, and virtual theory,'' *Millennium, J. Int. Stud.*, vol. 30, no. 3, pp. 669–690, Dec. 2001, doi: 10.1177/03058298010300030301.

[11] K. A. Oluwadamilola, ''The role of information technology in national security: 'A case study of Nigeria,''' *Global J. Comput. Sci. Technol.*, vol. 16, no. 3, pp. 1–7, 2016. [Online]. Available: https://computerresearch.org/index.php/computer/article/view/1443

[12] J. Norbekov, ''Ensuring information security as an ideological problem,'' *Mental Enlightenment Sci. Methodol. J.*, vol. 2020, no. 1, pp. 56–65, 2020.

[13] Z. D. Clopton, ''Territoriality, technology, and national security,'' *Univ. Chicago Law Rev.*, vol. 83, no. 1, p. 45, 2016. [Online]. Available: https://heinonline.org/HOL/P?h=hein.journals/uclr83&i=47

[14] S. Fischer and A. Wenger, ''Artificial intelligence, forward-looking governance and the future of security,'' *Swiss Political Sci. Rev.*, vol. 27, no. 1, pp. 170–179, Mar. 2021.

[15] G. Mani, ''Data processing and analytics for national security intelligence: An overview,'' in *Data Management, Analytics and Innovation*. Singapore: Springer, 2022, pp. 293–315, doi: 10.1007/978-981-16-2937-2.

[16] A. Bratko, A. Datskov, D. Oleshko, V. Vychavka, and O. Olytskyi, ''Some aspects of capability-based planning in the field of national security,'' *Turkish J. Comput. Math. Educ.*, vol. 12, no. 6, pp. 2219–2225, Apr. 2021, doi: 10.17762/turcomat.v12i6.4827.

[17] F. D. Kramer, S. H. Starr, and L. K. Wentz, *Cyberpower and National Security*. Washington, DC, USA: Potomac Books, 2009.

[18] D. S. Reveron, *Cyberspace and National Security: Threats, Opportunities, and Power in a Virtual World*. Washington, DC, USA: Georgetown Univ. Press, 2012.

[19] C. Whelan, *Networks and National Security: Dynamics, Effectiveness and Organisation*. Evanston, IL, USA: Routledge, 2016.

[20] P. Y. Logan, ''Crafting an undergraduate information security emphasis within information technology,'' *J. Inf. Syst. Educ.*, vol. 13, no. 3, pp. 177–182, 2002.

[21] R. von Solms and J. van Niekerk, ''From information security to cyber security,'' *Comput. Secur.*, vol. 38, pp. 97–102, Oct. 2013.

[22] J. L. Hayes, B. C. Britt, W. Evans, S. W. Rush, N. A. Towery, and A. C. Adamson, ''Can social media listening Platforms' artificial intelligence be trusted? Examining the accuracy of crimson hexagon's (now brandwatch consumer research's) AI-driven analyses,'' *J. Advertising*, vol. 50, no. 1, pp. 81–91, Jan. 2021.

[23] A. Monti and R. Wacks, *National Security in the New World Order: Government and the Technology of Information*, 1st ed. India: Routledge, 2021, doi: 10.4324/9780367809775.

[24] J. A. Lewis, J. S. Nye, and E. Schlather, *Computer Exports and National Security: New Tools for a New Century: A Report of the CSIS Commission on Technology Security in the Twenty-First Century*. Washington, DC, USA: CSIS, 2001.

[25] S. A. Taylor, ''The role of intelligence in national security,'' *Contemp. Secur. Stud.*, pp. 67–249, 2007. [Online]. Available: http://people.exeter.ac.uk/mm394/Intelligence/Collins%202007%20Intelligence%20(Taylor).pdf

[26] J. Crawford, ''The computer misuse act and hackers: A review of those convicted under the Act,'' Inf. Secur. Group, Roy. Holloway Univ. London, Egham, U.K., Tech. Rep., 2021. [Online]. Available: https://regmedia.co.uk/2021/04/12/techreport-jamescrawford.pdf

[27] A. K. Franck and D. Vigneswaran, ''Hacking migration control: Repurposing and reprogramming deportability,'' *Secur. Dialogue*, Apr. 2021, Art. no. 0967010621996938, doi: 10.1177/0967010621996938.

[28] B. Charoenwong and M. Bernardi, ''A decade of cryptocurrency 'hacks': 2011–2021,'' SSRN 3944435, Nat. Univ. Singapore, Singapore, Tech. Rep., 2021, doi: 10.2139/ssrn.3944435.

[29] N. Caidi and A. Ross, ''Information rights and national security,'' *Government Inf. Quart.*, vol. 22, no. 4, pp. 663–684, Jan. 2005.

[30] S. Jeong, J. Lee, J. Park, and C.-K. Kim, ''The social relation key: A new paradigm for security,'' *Inf. Syst.*, vol. 71, pp. 68–77, Nov. 2017, doi: 10.1016/j.is.2017.07.003.

[31] C. Antonoudis, ''Using social networks for law enforcement. The hellenic paradigm,'' Int. Hellenic Univ., Thermi, Greece, Tech. Rep., 2021. [Online]. Available: https://repository.ihu.edu.gr//xmlui/handle/11544/29722

[32] E. Elsawy, ''Digital platforms and its importance in enhancing the educational and media role of the national records and archives authority in Oman,'' in *Proc. 22nd Int. Arab Conf. Inf. Technol. (ACIT)*, Dec. 2021, pp. 1–8.

[33] G. Hitman and M. Zwilling, ''Normalization with Israel: An analysis of social networks discourse within Gulf states,'' *Ethnopolitics*, pp. 1–27, Apr. 2021, doi: 10.1080/17449057.2021.1901380.

[34] B. A. Kitchenham, ''Procedures for performing systematic reviews,'' Keele Univ., Keele, U.K., Tech. Rep., 2004. [Online]. Available: https://www.inf.ufsc.br/ aldo.vw/kitchenham.pdf

[35] P. Mongeon and A. Paul-Hus, ''The journal coverage of web of science and scopus: A comparative analysis,'' *Scientometrics*, vol. 106, no. 1, pp. 213–228, Jan. 2016.

[36] A. A. Chadegani, H. Salehi, M. M. Yunus, H. Farhadi, M. Fooladi, M. Farhadi, and N. A. Ebrahim, ''A comparison between two main academic literature collections: Web of science and scopus databases,'' *Asian Social Sci.*, vol. 9, no. 5, pp. 18–26, Apr. 2013.

[37] F. Hernandez, ''The threat of social media to society and national security: A call for social media policy and legislation,'' Liberty Univ., Lynchburg, VA, USA, Tech. Rep., 2021.

[38] H. Lu and S. Yuan, ''What motivates information sharing about disaster victims on social media? Exploring the role of compassion, sadness, expectancy violation, and enjoyment,'' *Int. J. Disaster Risk Reduction*, vol. 63, Sep. 2021, Art. no. 102431.

[39] L. Almadhoor, ''Social media and cybercrimes,'' *Turkish J. Comput. Math. Educ.*, vol. 12, no. 10, pp. 2972–2981, 2021.

[40] M. J. Baeth and M. S. Aktas, ''An approach to custom privacy policy violation detection problems using big social provenance data,'' *Concurrency Comput., Pract. Exper.*, vol. 30, no. 21, p. e4690, Nov. 2018.

[41] C. C. Ashbrook and A. R. Zalba, ''Social media influence on diplomatic negotiation: Shifting the shape of the table,'' *Negotiation J.*, vol. 37, no. 1, pp. 83–96, Jan. 2021.

[42] C. L. Ventola, ''Social media and health care professionals: Benefits, risks, and best practices,'' *Pharmacy Therapeutics*, vol. 39, no. 7, p. 491, 2014.

[43] H. Okamoto, ''Solving the security-rights paradox: How to re-imagine individual politics within the confines of national security,'' Univ. Chicago, Chicago, IL, USA, Tech. Rep., 2021, doi: 10.6082/uchicago.3275.

[44] D. Ma, H. Liu, and D. Song, ''Word graph network: Understanding obscure sentences on social media for violation comment detection,'' in *Proc. CCF Int. Conf. Natural Lang. Process. Chin. Comput.* Cham, Switzerland: Springer, 2020, pp. 738–750, doi: 10.1007/978-3-030-60450-9.

[45] T. Aichner, M. Grünfelder, O. Maurer, and D. Jegeni, ''Twenty-five years of social media: A review of social media applications and definitions from 1994 to 2019,'' *Cyberpsychology, Behav., Social Netw.*, vol. 24, no. 4, pp. 215–222, Apr. 2021.

[46] P. Harrigan, T. M. Daly, K. Coussement, J. A. Lee, G. N. Soutar, and U. Evers, ''Identifying influencers on social media,'' *Int. J. Inf. Manage.*, vol. 56, Feb. 2021, Art. no. 102246.

[47] A. Monti and R. Wacks, *National Security in the New World Order: Government and the Technology of Information*. Evanston, IL, USA: Routledge, 2021.

[48] K. Patel and D. Chudasama, ''National security threats in cyberspace,'' *Nat. J. Cyber Secur. Law*, vol. 4, no. 1, pp. 12–20, 2021.

[49] M. Kryshtanovych, L. Antonova, B. Pohrishchuk, Y. Mironova, and R. Storozhev, ''Information system of anti-crisis management in the context of ensuring national security,'' *Int. J. Comput. Sci. Netw. Secur.*, vol. 21, no. 12spc, pp. 719–725, 2021.

[50] O. M. Rieznik, N. S. Andriichenko, and I. V. Zvozdetska, "Results and perspectives on policing as part of the national security sector," *Linguistics Culture Rev.*, 2021. [Online]. Available: https://essuir.sumdu.edu.ua/handle/123456789/86772

[51] B. Babic, D. L. Chen, T. Evgeniou, and A.-L. Fayard, "A better way to onboard AI," *Harvard Bus. Rev.*, vol. 98, no. 4, pp. 56–65, 2021.

[52] C. Collins, D. Dennehy, K. Conboy, and P. Mikalef, "Artificial intelligence in information systems research: A systematic literature review and research agenda," *Int. J. Inf. Manage.*, vol. 60, Oct. 2021, Art. no. 102383.

[53] E. Schmidt, B. Work, S. Catz, S. Chien, C. Darby, K. Ford, J.-M. Griffiths, E. Horvitz, A. Jassy, W. Mark, and J. Matheny, "National security commission on artificial intelligence (AI)," Nat. Secur. Commission Artif. Intell., Washington, DC, USA, Tech. Rep., 2021. [Online]. Available: https://apps.dtic.mil/sti/pdfs/AD1124333.pdf

[54] I. A. Akour, R. S. Al-Maroof, R. Alfaisal, and S. A. Salloum, "A conceptual framework for determining metaverse adoption in higher institutions of Gulf area: An empirical study using hybrid SEM-ANN approach," *Comput. Educ., Artif. Intell.*, vol. 3, Jan. 2022, Art. no. 100052.

[55] R. Amalraj and M. Dharmalingam, "A work point count system coupled with back-propagation for solving double dummy bridge problem," *Neurocomputing*, vol. 168, pp. 160–178, Nov. 2015, doi: 10.1016/j.neucom.2015.06.001.

[56] M. Khorrami, M. Khorrami, and F. Farhangi, "Evaluation of tree-based ensemble algorithms for predicting the big five personality traits based on social media photos: Evidence from an Iranian sample," *Personality Individual Differences*, vol. 188, Apr. 2022, Art. no. 111479.

[57] A. Kumar and N. Sachdeva, "A bi-GRU with attention and CapsNet hybrid model for cyberbullying detection on social media," *World Wide Web*, pp. 1–14, Jul. 2021, doi: 10.1007/s11280-021-00920-4.

[58] X. Zhang, "Research on colour matching in art design based on neural network mathematics models," *Math. Problems Eng.*, vol. 2022, pp. 1–8, Mar. 2022.

[59] D. Sumathi and K. Alluri, "Deploying deep learning models for various real-time applications using keras," in *Advanced Deep Learning for Engineers and Scientists*. Cham, Switzerland: Springer, 2021, pp. 113–143, doi: 10.1007/978-3-030-66519-7.

[60] G. Z. Savaci, B. K. Bayraktar, and Ç. Özen, "The impacts of behavioral factors on social media addiction," *J. Comput. Educ. Res.*, vol. 9, pp. 1059–1083, Dec. 2021.

[61] M. Savci and M. D. Griffiths, "The development of the Turkish social media craving scale (SMCS): A validation study," *Int. J. Mental Health Addiction*, vol. 19, no. 2, pp. 359–373, Apr. 2021.

[62] M. Oz and A. Yanik, "Fear of surveillance: Examining Turkish social media users' perception of surveillance and willingness to express opinions on social media," *Medit. Politics*, pp. 1–25, Mar. 2022.

[63] X. Wu and R. Fitzgerald, "'Hidden in plain sight': Expressing political criticism on Chinese social media," *Discourse Stud.*, vol. 23, no. 3, pp. 365–385, Jun. 2021.

[64] S. Park, L. M. Bier, and H. W. Park, "The effects of infotainment on public reaction to north Korea using hybrid text mining: Content analysis, machine learning-based sentiment analysis, and co-word analysis," *El Profesional de la Información*, vol. 30, no. 3, May 2021.

[65] P. S. Motahar, R. Tavakoli, and P. Mura, "Social media influencers' visual framing of Iran on Youtube," *Tourism Recreation Res.*, pp. 1–13, Dec. 2021, doi: 10.1080/02508281.2021.2014252.

[66] V. Van Roy, F. Rossetti, K. Perset, and L. Galindo-Romero, "AI watch-national strategies on artificial intelligence: A European perspective," Joint Research Centre (Seville site), Seville, Spain, Tech. Rep., 2021. [Online]. Available: https://ideas.repec.org/p/ipt/iptwpa/jrc122684.html

[67] N. I. Alnaghaimshi and E. Pearson, "Empowering Arab tribal culture in the twenty-first century: Social media use in the Gulf states," *Inf., Commun. Soc.*, pp. 1–19, Nov. 2021, doi: 10.1080/1369118X.2021.1993956.

[68] T. Ngoensuk and C. Viriyavejakul, "A privacy violation behaviors preventive system in using social media by graduate students of king Mongkut's institute of technology Ladkrabang," *Medit. J. Social Sci.*, vol. 10, no. 4, p. 102, 2019.

[69] H. Postigo, "America online volunteers: Lessons from an early coproduction community," *Int. J. Cultural Stud.*, vol. 12, no. 5, pp. 451–469, Sep. 2009.

[70] J. Kosseff, "2. The prodigy exception," in *The Twenty-Six Words That Created the Internet*. Ithaca, NY, USA: Cornell Univ. Press, 2019, pp. 36–56.

[71] S. E. Bennett, "Canning spam: CompuServe," *Univ. Richmond Law Rev.*, vol. 32, no. 2, p. 545, 1998. [Online]. Available: https://heinonline.org/HOL/P?h=hein.journals/urich32&i=563

[72] D. M. Boyd, "Friendster and publicly articulated social networking," in *Proc. Extended Abstr. Hum. Factors Comput. Syst. (CHI)*, 2004, pp. 1279–1282.

[73] J. van Dijck, "'You have one identity': Performing the self on Facebook and LinkedIn," *Media, Culture Soc.*, vol. 35, no. 2, pp. 199–215, Mar. 2013.

[74] P. Kaur, N. Islam, A. Tandon, and A. Dhir, "Social media users' online subjective well-being and fatigue: A network heterogeneity perspective," *Technol. Forecasting Social Change*, vol. 172, Nov. 2021, Art. no. 121039.

[75] J. M. Banda, R. Tekumalla, G. Wang, J. Yu, T. Liu, Y. Ding, E. Artemova, E. Tutubalina, and G. Chowell, "A large-scale COVID-19 Twitter chatter dataset for open scientific research—An international collaboration," *Epidemiologia*, vol. 2, no. 3, pp. 315–324, Aug. 2021.

[76] E. Kross, P. Verduyn, G. Sheppes, C. K. Costello, J. Jonides, and O. Ybarra, "Social media and well-being: Pitfalls, progress, and next steps," *Trends Cognit. Sci.*, vol. 25, no. 1, pp. 55–66, Jan. 2021.

[77] I. O. Hilary and O.-O. Dumebi, "Social media as a tool for misinformation and disinformation management," *Linguistics Culture Rev.*, vol. 5, no. S1, pp. 496–505, Aug. 2021.

[78] S. Sanasi, D. Trabucchi, E. Pellizzoni, and T. Buganza, "The evolution of meanings: An empirical analysis of the social media industry," *Eur. J. Innov. Manage.*, vol. 25, no. 6, pp. 97–121, Mar. 2021.

[79] L.-V. Szabo, "Mass media, social media and technological evolution today: A theoretical approach," *J. Media Res.*, vol. 14, no. 3 pp. 95–105, Nov. 2021.

[80] S. Lebovitz, N. Levina, and H. Lifshitz-Assaf, "Is AI ground truth really 'true'? The dangers of training and evaluating AI tools based on experts' know-what," *Manage. Inf. Syst. Quart.*, vol. 45, no. 3b, pp. 1501–1525, May 2021.

[81] O. D. Apuke and B. Omar, "Fake news and COVID-19: Modelling the predictors of fake news sharing among social media users," *Telematics Informat.*, vol. 56, Jan. 2021, Art. no. 101475.

[82] S. Wagenpfeil, F. Engel, P. M. Kevitt, and M. Hemmje, "AI-based semantic multimedia indexing and retrieval for social media on smartphones," *Information*, vol. 12, no. 1, p. 43, Jan. 2021.

[83] A. Dafoe, Y. Bachrach, G. Hadfield, E. Horvitz, K. Larson, and T. Graepel, "Cooperative AI: Machines must learn to find common ground," *Nature*, vol. 593, no. 7857, pp. 33–36, May 2021.

[84] P. van Esch and J. Stewart Black, "Artificial intelligence (AI): Revolutionizing digital marketing," *Australas. Marketing J.*, vol. 29, no. 3, pp. 199–203, Aug. 2021.

[85] J. A. Kroll, J. B. Michael, and D. B. Thaw, "Enhancing cybersecurity via artificial intelligence: Risks, rewards, and frameworks," *Computer*, vol. 54, no. 6, pp. 64–71, Jun. 2021.

[86] R. Montasari, F. Carroll, S. Macdonald, H. Jahankhani, A. Hosseinian-Far, and A. Daneshkhah, "Application of artificial intelligence and machine learning in producing actionable cyber threat intelligence," in *Digital Forensic Investigation of Internet of Things (IoT) Devices*. Cham, Switzerland: Springer, 2021, pp. 47–64, doi: 10.1007/978-3-030-60425-7.

[87] M. Willett, "Lessons of the SolarWinds hack," *Survival*, vol. 63, no. 2, pp. 7–26, Mar. 2021.

[88] O. Analytica, "Solarwinds hack will alter us cyber strategy," Expert Briefings, Oxford Analytica, Oxford, U.K., Tech. Rep., 2021, doi: 10.1108/OXAN-DB259151.

[89] O. Analytica, "Audacity of SolarWinds hack will harden Western policy," Emerald Expert Briefings, Oxford Analytica, Oxford, U.K., Tech. Rep., 2020, doi: 10.1108/OXAN-ES258311.

[90] P. Ranade, A. Piplai, S. Mittal, A. Joshi, and T. Finin, "Generating fake cyber threat intelligence using transformer-based models," in *Proc. Int. Joint Conf. Neural Netw. (IJCNN)*, Jul. 2021, pp. 1–9.

[91] U. Reisach, "The responsibility of social media in times of societal and political manipulation," *Eur. J. Oper. Res.*, vol. 291, no. 3, pp. 906–917, Jun. 2021.

[92] B. Alhayani, H. J. Mohammed, I. Z. Chaloob, and J. S. Ahmed, "Effectiveness of artificial intelligence techniques against cyber security risks apply of IT industry," *Mater. Today, Proc.*, Mar. 2021, doi: 10.1016/j.matpr.2021.02.531.

[93] W. Steingartner, D. Galinec, and A. Kozina, "Threat defense: Cyber deception approach and education for resilience in hybrid threats model," *Symmetry*, vol. 13, no. 4, p. 597, Apr. 2021.

[94] S. Rodgers, "Themed issue introduction: Promises and perils of artificial intelligence and advertising," *J. Advertising*, vol. 50, no. 1, pp. 1–10, Jan. 2021.

[95] A. Tursunbayeva, C. Pagliari, S. Di Lauro, and G. Antonelli, "The ethics of people analytics: Risks, opportunities and recommendations," *Personnel Rev.*, vol. 51, no. 3, pp. 900–921, Apr. 2022.

[96] I. Anica-Popa, L. Anica-Popa, C. Rădulescu, and M. Vrîncianu, "The integration of artificial intelligence in retail: Benefits, challenges and a dedicated conceptual framework," *Amfiteatru Economic*, vol. 23, no. 56, pp. 120–136, 2021.

[97] V. Galaz, M. A. Centeno, P. W. Callahan, A. Causevic, T. Patterson, I. Brass, S. Baum, D. Farber, J. Fischer, D. Garcia, T. McPhearson, D. Jimenez, B. King, P. Larcey, and K. Levy, "Artificial intelligence, systemic risks, and sustainability," *Technol. Soc.*, vol. 67, Nov. 2021, Art. no. 101741.

[98] R. Eitel-Porter, "Beyond the promise: Implementing ethical AI," *AI Ethics*, vol. 1, no. 1, pp. 73–80, Feb. 2021.

[99] Z. Stanley-Lockman, "Military AI cooperation toolbox," Center Secur. Emerg. Technol., Washington, DC, USA, Tech. Rep., Aug. 2021. [Online]. Available: https://cset.georgetown.edu/wp-content/uploads/CSET-Military-AI-Cooperation-Toolbox.pdf

[100] M. Imran, F. Ofli, D. Caragea, and A. Torralba, "Using AI and social media multimodal content for disaster response and management: Opportunities, challenges, and future directions," *Inf. Process. Manage.*, vol. 57, no. 5, Sep. 2020, Art. no. 102261.

[101] A. Capatina, M. Kachour, J. Lichy, A. Micu, A.-E. Micu, and F. Codignola, "Matching the future capabilities of an artificial intelligence-based software for social media marketing with potential users' expectations," *Technol. Forecasting Social Change*, vol. 151, Feb. 2020, Art. no. 119794.

[102] T. Gillespie, "Content moderation, AI, and the question of scale," *Big Data Soc.*, vol. 7, no. 2, Aug. 2020, Art. no. 2053951720943234.

[103] R. Radu, "Steering the governance of artificial intelligence: National strategies in perspective," *Policy Soc.*, vol. 40, no. 2, pp. 178–193, Apr. 2021.

[104] Z. Zhong, L. Jin, and S. Huang, "DeepText: A new approach for text proposal generation and text detection in natural images," in *Proc. IEEE Int. Conf. Acoust., Speech Signal Process. (ICASSP)*, Mar. 2017, pp. 1208–1212.

[105] A. Mackenzie, "From API to AI: Platforms and their opacities," *Inf., Commun. Soc.*, vol. 22, no. 13, pp. 1989–2006, Nov. 2019.

[106] Y. Zhuang, "Emotional analysis of sentences based on machine learning," in *Proc. Int. Conf. Big Data Anal. Cyber-Physical-Syst.* Singapore: Springer, 2019, pp. 813–820, doi: 10.1007/978-981-15-2568-1.

[107] K. S. Kumar, D. E. Geetha, and P. R. Sahoo, "A methodology to handle heterogeneous data generated in online social networks," *J. Comput. Theor. Nanosci.*, vol. 17, no. 9, pp. 4098–4102, Jul. 2020.

[108] K. Khalil, U. Asgher, Y. Ayaz, R. Ahmad, J. A. Ruiz, N. Oka, S. Ali, and M. Sajid, "Cognitive computing for human-machine interaction: An IBM watson implementation," in *Proc. Int. Conf. Appl. Hum. Factors Ergonom.* Cham, Switzerland: Springer, 2020, pp. 400–406, doi: 10.1007/978-3-030-51041-1.

[109] J. P. Gujjar and P. K. HR, "Sentiment analysis: Textblob for decision making," *Int. J. Sci. Res. Eng. Trends*, vol. 7, no. 2, pp. 1097–1099, 2021.

[110] M. M. Haider, M. A. Hossin, H. R. Mahi, and H. Arif, "Automatic text summarization using gensim Word2Vec and K-means clustering algorithm," in *Proc. IEEE Region 10th Symp. (TENSYMP)*, Jun. 2020, pp. 283–286.

[111] Z. Zeng, R. Islam, K. N. Keya, J. Foulds, Y. Song, and S. Pan, "Fair representation learning for heterogeneous information networks," 2021, *arXiv:2104.08769*.

[112] M. Saqib and R. Zarine, "Evaluating customer relationship management (CRM) as a business knowledge and intelligence management tool," *iRASD J. Manage.*, vol. 3, no. 2, pp. 171–184, Sep. 2021.

[113] N. Zierau, K. Flock, A. Janson, M. Söllner, and J. M. Leimeister, "The influence of AI-based chatbots and their design on users' trust and information sharing in online loan applications," in *Proc. Hawaii Int. Conf. Syst. Sci. (HICSS)*, Koloa, HI, USA, 2021.

[114] D. S. Mishra, A. Agarwal, B. P. Swathi, and K. C. Akshay, "Natural language query formalization to SPARQL for querying knowledge bases using rasa," *Prog. Artif. Intell.*, pp. 1–14, Dec. 2021, doi: 10.1007/s13748-021-00271-1.

MOHAMMED NASSER AL-SUQRI received the bachelor's degree in library and information science from the Department of Library and Information Science, Sultan Qaboos University, Oman, the master's degree in library and information science from the School of Information and Library Science, Pratt Institute, New York, USA, and the Ph.D. degree in library and information management from the School of Library and Information Management, Emporia State University, USA. He is currently an Associate Professor and the Dean of Postgraduate Studies at Sultan Qaboos University. He is the Editor-in-Chief of the *Arts and Social Sciences* journal (Oman), an Associate Editor of several journals, including "Evidence" a *Journal of Information Science*, *Journal of Applied Information Science* (Nigeria), *Journal of Socio-Informatics*, and *Social and Human Sciences Review* (SHSR) (Algeria). He is also a Reviewer of several journals and research organizations, including the *Journal of Library and Information Sciences* (Algeria), Research Council (Oman), and Qatar National Research Foundation (Qatar). He has published several articles in ISI and SCOPUS indexed, edited books and chapters published by renowned international publishers, and conference proceedings. His research interests include the area of user studies, knowledge management and sharing, technology adoption theories and models, research methodology, information industries, and the impact of new technology on academic libraries. He has been awarded the Best Researcher Award, in 2014, and the Best Academic Award, in 2018.

MARYAM GILLANI received the B.S. degree in software engineering and Computer Sciences from the Forman Christian College (FCCU), Lahore, and the M.S. degree in computer software engineering from the NUST College of Electrical and Mechanical Engineering (CEME), Islamabad, Pakistan. She is currently pursuing the Ph.D. degree in machine learning and artificial neural networks with University College Dublin (UCD), Ireland. Her other research interests include data collection and communication protocols for VANETs, intelligent transport systems, rapid software development, and information handling & security.