https://doi.org/10.2352/EI.2024.36.3.MOBMU-318

The Open Source Intelligence (OSINT) in the Electricity Sector: Balancing Utility and Responsibility

Mert Ilhan Ecevit[1,2], Muhammad Hasban Pervez[1,2], Hasan Dag[1,2], Reiner Creutzburg[3,4]

[1] Cyber Security and Critical Infrastructure Research Center, Kadir Has University, 610101-Istanbul, Turkey
Email: mert.ecevit@stu.khas.edu.tr, muhammadhasban.pervez@stu.khas.edu.tr, hasan.dag@khas.edu.tr

[2] Management Information Systems, Kadir Has University, 610101-Istanbul, Turkey
Email: mert.ecevit@stu.khas.edu.tr, muhammadhasban.pervez@stu.khas.edu.tr, hasan.dag@khas.edu.tr

[3] SRH Berlin University of Technology, Berlin School of Technology, Ernst-Reuter-Platz 10, D-10587 Berlin, Germany
Email: reiner.creutzburg@srh.de

[4] Technische Hochschule Brandenburg, Department of Informatics and Media, Magdeburger Str. 50, D-14770 Brandenburg, Germany
Email: creutzburg@th-brandenburg.de

Keywords: OSINT, Open Source Intelligence, SOCMINT, Social Media Intelligence, Critical Infrastructure, Critical Infrastructure Protection, Intelligence Cycle, Cyber Security, Homeland Security

Abstract

Critical infrastructure is the backbone of modern societies, and protecting this infrastructure is essential to ensure the stability of societies and economies. The electricity sector is one of the most critical infrastructures, and any disruption can have significant consequences. The threat landscape in this sector is constantly evolving. With the increasing sophistication of cyber-attacks and other threats, it has become essential to use innovative technologies to identify and mitigate them. Open Source Intelligence (OSINT) technologies have emerged and offer valuable tools for identifying and mitigating these threats. This article presents an in-depth overview of OSINT technologies and their applications in the protection of critical infrastructure, with an emphasis on the electricity sector. It discusses the vulnerabilities of the electricity sector, the types of OSINT technologies, and the benefits they provide. Case studies of successful applications of OSINT technologies in the electricity sector are presented to illustrate their effectiveness. This article also examines organizations' challenges in implementing OSINT technologies, including technological, legal, and financial challenges. Finally, the article concludes by offering recommendations for successfully implementing OSINT technologies to protect critical infrastructure, particularly in the electricity sector. The insights offered in this article will be helpful for policymakers, security professionals, and anyone interested in protecting critical infrastructure.

Introduction

Background

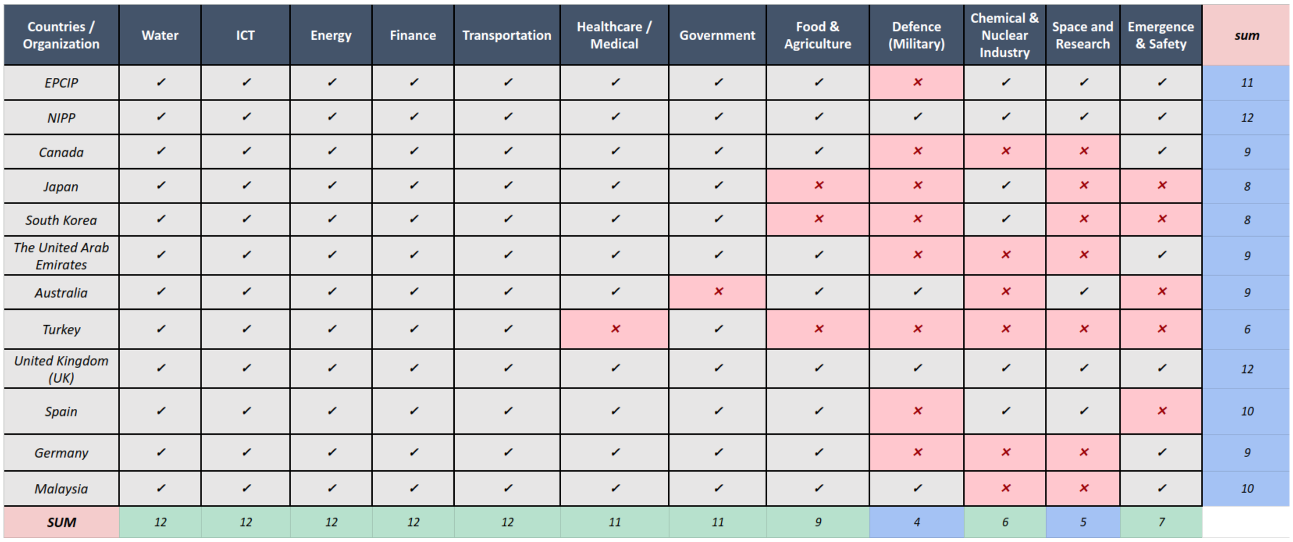
Critical infrastructure serves as the foundation for modern societies and economies, delivering essential services that enable the daily functioning of communities [53, 62]. The conceptualization of critical infrastructure varies across nations and institutions, as evidenced by Figures 1 and 2. These variations in definition predominantly stem from the specific political, economic, or social priorities influencing the defining entity at any given time.

Among these foundational services, the electricity sector is of paramount importance, given that any disruption in power supply can cascade into significant adverse impacts, affecting multiple facets of society and the economy [53, 62, 37, 18, 37, 52, 44]. When Figure 1 is analyzed, we can see classifications made by the USA on the definition of critical infrastructure. It is visible that without energy-critical infrastructure, the continuity of others will be disturbed. This puts the electricity sector as an energy infrastructure at a critical point where its security affects all other critical infrastructures.

Critical infrastructure protection is traditionally focused on defending physical assets against environmental threats. However, the evolving landscape of threats, particularly the emergence of sophisticated cyber-attacks, has necessitated a shift in this traditional perspective [53, 44, 37]. This change is even more critical considering that many of these critical systems were not designed initially with robust cybersecurity measures, transitioning from primarily analog, manual operations to more digital and automated configurations [37, 52]. As a result, new vulnerabilities have been introduced that could potentially be exploited to compromise infrastructure control systems [53, 37, 52].

Given the complexity and variability of threats, there is no one-size-fits-all solution for protecting these vital assets. Instead, a diverse array of adaptive strategies and technologies, such as wireless sensor networks for monitoring and metrics for assessing security posture, should be considered based on the unique risks associated with each sector [53, 44, 52, 37].

In conclusion, protecting critical infrastructure is an ever-evolving challenge that demands ongoing attention and investment. An integrated, defense-in-depth approach addressing both



Countries / Organization	Water	ICT	Energy	Finance	Transportation	Healthcare / Medical	Government	Food & Agriculture	Defence (Military)	Chemical & Nuclear Industry	Space and Research	Emergence & Safety	sum
EPCIP	✓	✓	✓	✓	✓	✓	✓	✓	✗	✓	✓	✓	11
NIPP	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	12
Canada	✓	✓	✓	✓	✓	✓	✓	✓	✗	✗	✗	✓	9
Japan	✓	✓	✓	✓	✓	✓	✓	✗	✗	✓	✗	✗	8
South Korea	✓	✓	✓	✓	✓	✓	✓	✗	✗	✓	✗	✗	8
The United Arab Emirates	✓	✓	✓	✓	✓	✓	✓	✓	✗	✗	✗	✓	9
Australia	✓	✓	✓	✓	✓	✓	✗	✓	✓	✗	✓	✗	9
Turkey	✓	✓	✓	✓	✓	✗	✓	✗	✗	✗	✗	✗	6
United Kingdom (UK)	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	12
Spain	✓	✓	✓	✓	✓	✓	✓	✓	✗	✓	✓	✗	10
Germany	✓	✓	✓	✓	✓	✓	✓	✓	✗	✗	✗	✓	9
Malaysia	✓	✓	✓	✓	✓	✓	✓	✓	✓	✗	✗	✓	10
SUM	12	12	12	12	12	11	11	9	4	6	5	7	

Figure 1. *Critical Infrastructure classifications among different nations and institutions [6, 8, 9, 5, 7, 10, 2, 11, 4, 70, 1, 3]*

cyber and physical vulnerabilities is essential for ensuring the uninterrupted functioning of the services that are crucial for the well-being of citizens and the economy [53, 62, 18, 37, 52, 44].

Objectives

The primary objective of this paper is to provide a comprehensive overview of Open Source Intelligence (OSINT) technologies as they apply to the protection of critical infrastructure, with a particular focus on the electricity sector. It aims to delineate the types of OSINT technologies available, discuss their benefits, and explore real-world applications and case studies where these technologies have proven effective.

Scope

This article confines itself to OSINT technologies targeting enhancing the electricity sector's security posture. Although OSINT applications are vast, spanning from social media analysis to geopolitical intelligence, the scope of this article is deliberately narrowed to focus on critical infrastructure protection.

Structure of the Paper

The paper is structured as follows: Section 2 outlines the vulnerabilities inherent in the electricity sector, including physical and cyber aspects. Section 3 provides an overview of OSINT technologies, elaborating on their types and benefits. Section 4 dives into specific applications of OSINT technologies in the electricity sector, supplemented by relevant case studies. Section 5 discusses the challenges organizations face in implementing these technologies. Section 6 offers actionable recommendations, and Section 7 concludes the paper.

Vulnerabilities in the Electricity Sector

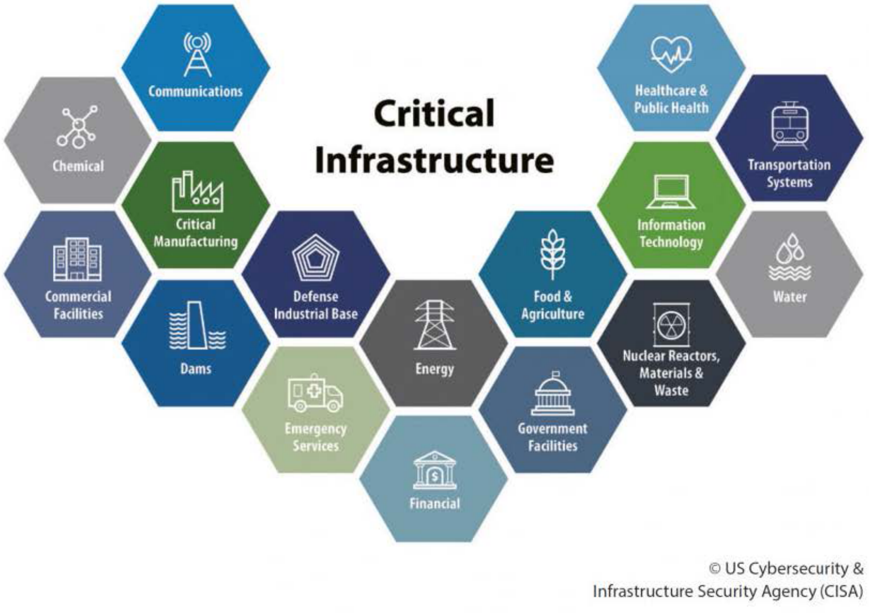
Physical Vulnerabilities

The electricity sector's critical infrastructure is susceptible to physical and digital threats, which could result in severe repercussions. Components such as transformers and transmission towers are at risk of physical assault, and their replacement could require significant time. Likewise, control systems are prone to cyber risks like hacking, terrorism, or malware, though quantifying these risks remains a challenge [13]. Technological advances like phasor measurement units (PMUs) and phasor data concentrators (PDCs) offer better monitoring but also come with vulnerabilities. These technologies often fall short of security measures such as encryption and strong password policies, exposing them to various types of cyber risks [30].

While advancements in information technology have enhanced the efficiency of electrical grids, they have also created alarming cyber vulnerabilities. These cyber risks can disrupt critical services and significantly wreak havoc on economies. Eliminating risks is unfeasible, but international cooperation is essential for risk mitigation [63]. Historically prioritizing reliability and cost, the industry now needs to focus on security. Regulatory reforms and technological innovations have both introduced new vulnerabilities and increased interdependence. Presently, the cyber risks appear to outweigh the physical risks. Regulatory efforts to manage these risks must find a balance among security, cost, and reliability [79].

For practical risk assessment, test beds are essential to evaluate the vulnerabilities in industrial control systems without putting critical infrastructure at risk. One test bed identified weaknesses in PLCs, relays, and SCADA systems commonly used in critical infrastructure. Remedial strategies were subsequently formulated and communicated to the manufacturers. Work is underway to create a library of exploits and payloads aimed at similar systems [54].

Ownership of critical infrastructure by the private sector presents additional challenges as governments must depend on systems beyond their control. Despite their global reach, operators of interconnected systems often lack a comprehensive understanding of their infrastructure's scope and interconnectedness. These knowledge gaps could potentially enable international attacks affecting multiple countries. Strategies to manage risks associated with private ownership are thus imperative [78].



© US Cybersecurity & Infrastructure Security Agency (CISA)

***Figure 2.** Critical Infrastructure Classification in the USA [67]*

Emerging electrical cyber-physical systems, which merge computing and communication technologies with power grids, are prone to chain reactions of failures in the event of cyber-attacks. Algorithms for detection and protection can act as preventive measures. Techniques like load balancing can alleviate issues related to fragmented infrastructures. A multifaceted vulnerability assessment should encompass robustness, cost, potential damage, equipment, and possible failure points. Solutions should incorporate cyber and physical infrastructure dimensions [77].

Control systems are vulnerable to cyber threats that interrupt electricity supply, thus affecting security and economic stability. Ensuring compliance with established standards such as NERC CIP is challenging due to the complexity of the infrastructure. A comprehensive framework for securing control systems could include monitoring, detection, analysis, and mitigation. Tools like attack tree models can evaluate vulnerabilities across different system levels. Quantitative metrics and indices may serve as a guide for enhancing security measures. Therefore, solutions must consider the cyber and physical facets of critical infrastructure [71].

Cyber Vulnerabilities

The increasing reliance on Information and Communication Technologies (ICT) in the electricity sector has heightened the system's vulnerability to cyber threats, introducing new forms of risks like system breakdowns, data breaches, and cyber-attacks that endanger the stability of energy supply [80]. The threats to the energy sector's cybersecurity have been widely studied. For instance, Jha et al. (2023) revealed that India's electricity distribution systems show insufficient preparedness for cybersecurity, emphasizing challenges related to the absence of robust policies, standards, and specialized personnel [47]. Aarland (2022) undertook a systematic review of existing literature, concluding that there is a scarcity of research focusing on digital supply chain risks in critical infrastructure and suggesting more comprehensive risk management strategies [14].

Samikannu, Kumar, and Venkatachary, in their 2018 studies, reviewed various cyber threats such as malware, DoS attacks, and data breaches that specifically target the energy sector. They argued that these cyber threats could lead to operational disruptions, equipment damage, data theft, and risks to public safety. Hence, global collaboration and investments are essential for mitigation [63, 75]. Ten (2010) proposed an analytical framework involving attack-tree methodology for monitoring, detecting, and mitigating cyber threats in critical systems, enabling the measurement of system vulnerabilities based on existing security conditions [71]. Furthermore, Ani (2017) discussed the increased cybersecurity risks by adopting Industry 4.0 and IoT trends in manufacturing sectors. He suggested an integrated security strategy encompassing human skills, processes, and technologies [19].

In summary, these studies collectively indicate the growing cybersecurity vulnerabilities in the electricity sector due to the increased use of ICT and automation [47, 14, 63, 75]. They call for a holistic approach to risk management, advocating for international collaborations and investments in cybersecurity frameworks and expertise [71, 19]. In light of this, proactively addressing these cybersecurity risks becomes crucial for maintaining a secure and reliable electricity infrastructure [80, 79].

Threat Landscape

The increasing digitization and interconnectivity of critical electrical systems have escalated cybersecurity concerns. Various academic contributions have explored this complex landscape of risks and remedies. Samikannu et al. (2018) underline that the enhanced interconnectivity in sectors like energy opens up avenues for cyber-attacks, which could have significant economic and psychological repercussions [63]. Coutinho et al. (2008) suggest employing anomaly detection methods and rule extraction to recognize cyber-attacks, contributing a methodology for the same [31].

Amin (2002) categorizes threats to power systems into three types: direct attacks, attacks aimed at other infrastructures through the power system, and attacks that spread through the power system from other sectors. They argue that complete defense is improbable due to the systems' intricate nature and interconnectedness [17]. Sun et al. (2018) offer a panoramic view of the state-of-the-art intelligent grid technologies while outlining cybersecurity solutions and areas still requiring research [68].

Jarmakiewicz et al. (2017) outline an approach to designing cybersecurity solutions for power grid control systems, using a domestic grid system analysis to spotlight key security components [46]. Baggott and Santos (2020) introduce a framework for risk analysis aimed at bolstering the cybersecurity of the U.S. electrical grid. They claim that past studies have paid more attention to natural disasters rather than cyber threats [22].

Zhang (2011) argues for a comprehensive cybersecurity policy for the electricity sector, identifying current regulatory shortcomings and suggesting changes that include leadership roles, data sharing, and international cooperation [84]. Boeding et al. (2022) survey governance, risks, and countermeasures in power grid cybersecurity. They pinpoint unique threats and priorities in Operational Technology (OT) systems as compared to Information Technology (IT) systems [27].

In conclusion, the scholarly works collectively highlight a rapidly evolving cybersecurity threat landscape targeting critical electricity infrastructures. As these systems grow increasingly digital and interconnected, the window of vulnerability expands, presenting challenges ranging from direct cyber-attacks to complex threats that could affect other sectors [63, 17]. Despite advancements in anomaly detection and rule extraction methods for identifying threats [31], and even comprehensive frameworks for risk analysis [22], there remains a pressing need for integrated solutions. The current regulatory frameworks and policies are inadequate to meet these complex challenges, necessitating revamped governance, more robust risk assessments, and multi-layered defensive measures [84, 27].

Overview of OSINT Technologies

Definition of OSINT

Open Source Intelligence, commonly known as OSINT, involves collecting and analyzing information from public sources to generate actionable insights. While OSINT has traditionally served as a supplementary source of information for governments and militaries, its importance has gained renewed recognition, prompting calls for more systematic collection and analysis. The United States has responded by establishing specific roles and centers for OSINT, like the Assistant Director of National Intelligence for Open Source and the National Open Source Center. The types of information OSINT uses can be diverse, ranging from traditional media like newspapers and television to modern platforms like the Internet. Extracting actionable intelligence from the vast, unstructured data on the Internet necessitates the use of specialized tools [24].

As shown in Figure 3, OSINT is not limited to military uses; it has grown to encompass areas like politics, economy, society, and cybersecurity. It can be employed to acquire valuable information and counter various threats, including cybercrime [57]. AI and machine learning advances have created new methods for gathering and interpreting OSINT. Research in this area is focused on various applications, such as detecting cyber threats and analyzing public sentiment. Most of this research is concentrated in the U.S. and Europe, and the field is attracting increasing interest [34].

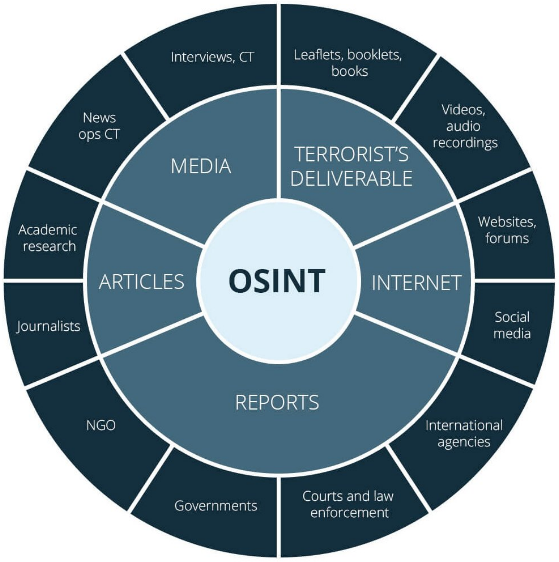


Figure 3. Use of OSINT Technologies in different domains [12]

In the private sector, OSINT is particularly useful for gathering information from social media, although privacy settings can create obstacles. Methods have been proposed to establish connections between private profiles on social media platforms more efficiently [42]. Some argue that the availability of OSINT can fundamentally change problem-solving approaches by providing access to a broader range of information, enhancing fluid intelligence later in life. However, there are concerns that this could undermine cultural intelligence, posing a risk to social harmony [38].

While OSINT is a continually evolving field with abundant potential, it also has limitations. Its applications in cybersecurity and by governments require complex tools and techniques to sift through extensive volumes of unstructured information [57]. Overall, OSINT offers novel problem-solving approaches that cross cultural boundaries, but we must be cautious of its societal implications.

Types of OSINT Technologies

Open Source Intelligence (OSINT) involves collecting and evaluating publicly accessible information to generate valuable insights [57]. While OSINT has historical roots, its importance has surged due to the proliferation of the Internet and social media platforms.

Social Media Intelligence

This form of intelligence focuses on extracting data from social networking sites such as Twitter, Facebook, and YouTube. It is used to gain various insights, such as detecting online radicalization and forecasting civil disturbances [15].

Web Intelligence

Web intelligence involves gleaning data from websites, search engines, and the deep web. An example application is to aid law enforcement in criminal investigations by accumulating data with minimal human interaction [72].

Media Intelligence

In this category, traditional media channels like television, radio, newspapers, etc., are analyzed. Baldini (2007) outlined a system that can scrutinize media in different languages [23].

Tools and Techniques

Various methods and tools are deployed for OSINT, such as data mining, machine learning, geolocation, and network analysis [59]. These processes can be automated through web scraping, Application Programming Interfaces (APIs), and specific algorithms [15, 76, 59]. Nevertheless, human intervention is essential for contextualization and ensuring the ethical utilization of the collected information [28, 59].

Applications and Ethical Considerations

OSINT has a wide range of applications including but not limited to cybersecurity, business intelligence, and criminal investigations [28, 57, 72]. It has been argued that OSINT can significantly improve cybersecurity by identifying system vulnerabilities [82]. However, it poses ethical questions about privacy, as OSINT can inadvertently disclose sensitive information about individuals and entities [28]. Regulatory frameworks aim to balance the advantages of OSINT and the need to protect privacy [28].

In summary, OSINT leverages an array of publicly available data sources and employs both automated and manual techniques for analysis. While it offers numerous applications, ethical issues related to privacy must be diligently managed through proper regulations. When judiciously implemented and regulated, OSINT is a crucial intelligence asset in the digital era.

The Advantages and Limitations of OSINT

Open Source Intelligence (OSINT) is the process of collecting intelligence from publicly accessible sources [45]. OSINT has several advantages, such as ease of availability, low costs, and covering a broad range of subjects [45]. Despite these strengths, OSINT is also plagued by data inconsistency, lack of proper validation, and the risk of encountering false information [45].

Untapped Potential and Modern Applications

OSINT is often described as an untapped ”goldmine” of information if utilized correctly [57]. Technology advancements have contributed to the rapid evolution of OSINT, making it an invaluable asset in various sectors like politics, business, society, and cybersecurity [57].

Strengths of OSINT

The strengths of OSINT lie in its capability to identify events, assist in decision-making, perform risk assessments and due diligence, monitor communications, and manage reputations [57]. It can facilitate effective investigations and trustworthy web searches [72]. For instance, investigators can benefit from OSINT by having more accessible access to relevant information, thereby conserving time and resources [72]. Businesses can also leverage OSINT for objectives such as client information discovery and brand monitoring [72].

Multilingual Capabilities

A multilingual OSINT platform can handle large and geographically diverse datasets [23]. This is particularly advantageous for language-independent searches, as a critical asset for military and governmental applications [23].

OSINT for Organizational Benefits

OSINT can bolster an organization’s brand and competitive edge [35]. It is a comprehensive tool to enhance decision-making, risk evaluation, due diligence, and communication [35].

Limitations and Concerns

However, there are also inherent limitations and challenges, such as privacy risks and legal considerations [28]. One significant downside is the susceptibility to disinformation [43]. The open nature of OSINT makes it prone to manipulation, but when utilized with expert oversight, it can yield credible outcomes [43].

In conclusion, OSINT offers a wealth of advantages when used judiciously, ranging from accessibility and cost-effectiveness to specialized uses in event identification, decision-making, risk analysis, and more [45, 57, 72, 23, 35, 28, 43]. Yet, it lacks significant drawbacks like data inconsistency, validation issues, disinformation, and ethical considerations [45, 28, 43]. Expertise is essential to navigate these challenges and make the most of OSINT [43].

Applications of OSINT in the Electricity Critical Infrastructure

Surveillance and Monitoring

The literature demonstrates that Open Source Intelligence (OSINT) plays a vital role in understanding and securing electricity critical infrastructure. Keliris et al. delve into how OSINT can be employed to build comprehensive models of power systems, pinpointing their vital components [49]. Their work includes a case study, showcasing the depth of analysis achieved through public data while also cautioning against the hazards of releasing sensitive information.

Syamsiana et al. introduce an Energy Monitoring System built upon the Internet of Things (IoT), which can keep track of power quality and flag potential cyber-attacks targeting strategic installations [69]. The system focuses on parameters such as voltage, current, and harmonics to aid in the early detection and remediation of threats.

A platform that monitors the security of electrical information systems in real-time is presented by Yu et al. [83]. This system keeps tabs on IT hardware, software, networks, and network boundaries, enabling a swift reaction to and defense against security threats.

Similarly, a proposal for an IoT-based monitoring system for electricity substations is put forward by Pankajavalli et al., which allows remote tracking of transformers, capacitors, and reactors to detect issues before they escalate [56].

Arduini et al. offer a methodology tailored to assess the importance of energy infrastructure about Intentional Electromagnetic Interference (IEMI) threats [20]. The framework is designed to assist grid operators in identifying and mitigating security risks, and its application is demonstrated in a transmission substation.

Jiang et al. propose a testing model to evaluate the security protocols of electric Industrial Control Systems (ICS) [48]. The paper describes a three-layer model covering typical ICS components and provides a process for executing security assessments to bolster protection.

Lastly, Piat et al. discuss a platform that integrates models of electrical distribution networks, IT infrastructure, and telecommunications to understand better the interdependencies and security implications among these critical infrastructures [58].

To sum up, the body of work discusses using OSINT, coupled with IoT and monitoring systems (Figure 4), to collect intelligence for evaluating the security state of electricity critical infrastructure. The papers focus on early threat detection — from cyberattacks or IEMI — and propose integrated systems and methodologies for a comprehensive view of infrastructure security.

Threat Identification and Mitigation

OSINT is a valuable resource for mining publicly accessible information to spot cyber threats. Various research studies confirm its utility in identifying risks to essential infrastructure. For instance, Lee's work [51] introduces an OSINT-grounded framework tailored for scrutinizing cyber threats to crucial infrastructures. Similarly, Cartagena et al. [29] designed a framework employing OSINT, albeit with privacy concerns, for evaluating risks associated with critical infrastructures. Moreover, Keliris et al. [49] illustrate the capability of OSINT in collecting data about power systems and discerning their weak points.

Despite its potential, OSINT faces several limitations, as pointed out by Govardhan et al. [39]. They highlight challenges related to data quality, volume, integration, analysis, and ethical concerns, suggesting potential remedies such as enhanced analytical tools, the use of AI, and adopting ethical data practices.

OSINT may be beneficial but may not be wholly adequate by itself for threat detection. Kostopoulos et al. [50] advocate for an approach that melds OSINT with real-time analytics and alert systems to anticipate better, identify, and mitigate threats. Additionally, Vacas et al. [73] crafted an intrusion detection system based on OSINT that can recognize real-time threats such as botnets and brute force attacks. Pakizeh [55] put forth a multi-layered framework focused on understanding cyber attacks on cyber-physical systems, a class of systems often vital for critical infrastructure.

Case Studies

The 2007 Estonian Cyber Attacks: Demonstrating the Multifaceted Role of OSINT in Cyber Resilience

The 2007 cyber attacks on Estonia are a poignant example of modern cyber warfare's increasing complexity and scope. Initiated by political tensions, these attacks crippled Estonia's critical digital infrastructures, such as government websites and the banking sector. This case illuminates the potential of Open Source Intelligence (OSINT) in preemptive defense and real-time response. OSINT could have provided early warnings through monitoring online forums and social media, enabling preemptive actions like firewall fortification. Real-time OSINT could have offered tactical benefits by identifying attack patterns and origins during the attack. The incident also reinvigorated policy dialogues around collective cyber defense, where OSINT can offer data-driven insights into potential aggressors' capabilities [33].

The 2013 Metcalf Substation Sniper Attack: Utilizing OSINT for Comprehensive Grid Security

The 2013 sniper attack on the Metcalf substation was a pivotal moment in recognizing the potential for physical threats against critical electrical infrastructure in the U.S. The event led to $15.4 million in damages and underlined the vulnerabilities in the electricity grid's transmission and distribution aspects. This case argues that Open Source Intelligence (OSINT) can be essential in securing the grid against diverse threats, including physical attacks. Strategic OSINT practices can offer early warnings by monitoring unusual activities or patterns in open sources, such as social media and online marketplaces, facilitating preventative action. Additionally, real-time OSINT tools can provide automated alerts for quick responses, filling gaps traditional security measures may overlook [66, 32].

The 2015 Ukraine Power System Cyberattack: The Crucial Role of OSINT in Securing Critical Infrastructure

The 2015 cyberattack on Ukraine's power distribution service, Kyivoblenergo, was a wake-up call about the vulnerabilities in critical infrastructures using digital technologies like SCADA systems. The attack led to substantial outages affecting approximately 225,000 customers across several regions. This case highlights Open Source Intelligence's (OSINT) essential role in enhancing security measures for such critical systems. Proactive monitoring of hacker forums, tracking suspicious IP addresses, and real-time alerts configured for SCADA systems are among the OSINT strategies that could have provided an early warning mechanism, potentially averting the attack or minimizing its impact [81].

Multifaceted Threats to the U.S. Power Grid During Obama's Era: The Imperative of Open Source Intelligence (OSINT)

During President Obama's administration, the U.S. power grid faced an evolving landscape of cyber and physical threats, highlighted by events such as the discovery of the Stuxnet worm and the 2013 Metcalf sniper attack. Despite policies like Executive Order 13636 aimed at enhancing cybersecurity, vulnerabilities persisted in the energy sector. Open Source Intelligence (OSINT) is an invaluable tool in this context. OSINT's capability to continuously monitor cyber activities and detect emerging threats enables a proactive, rather than reactive, security posture for both government and private sectors [40].

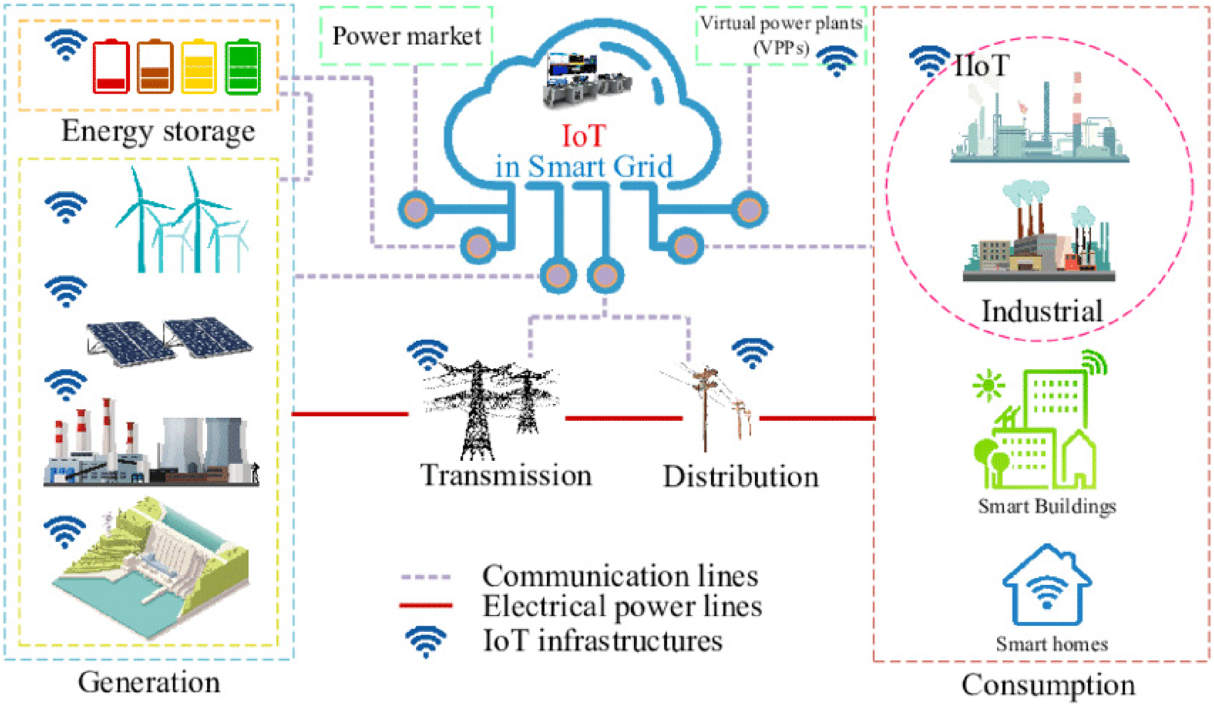


Figure 4. *Resemblance of IoT monitoring on infrastructure [65]*

Challenges in Implementing OSINT Technologies

Technological Challenges

The proliferation of the Internet and social media platforms has resulted in an abundant availability of public data, offering both pros and cons for the application of Open Source Intelligence (OSINT) technologies. Several scholarly works emphasize the untapped reservoir of information that can be obtained via OSINT [57] but also highlight the logistical challenges of processing large and diverse data sets [25]. One main obstacle is ensuring the trustworthiness and accuracy of open-source information [25]. Given the surge in disinformation and ”fake news,” OSINT practitioners are compelled to cross-verify information from diverse outlets and assess the possible biases of these sources [25]. There’s a growing need for advanced technological solutions to sort and prioritize data based on source reliability [25]. Legal and privacy concerns further complicate data acquisition from social media platforms [42]. Nevertheless, some researchers have investigated methodologies for legally accessing private social media data through network analysis [42]. Integrating open-source data with confidential information from secure channels remains another challenging aspect [36]. To effectively leverage OSINT, organizations are encouraged to formulate comprehensive strategies and tools for integration into pre-existing intelligence and decision-making systems [36].

Several studies have delved into the application of OSINT in specialized domains like disaster management [21], counterterrorism [41], and nuclear non-proliferation [41]. These studies reveal both the strengths—such as real-time disaster data [21]—and limitations, like the restricted access to encrypted terrorist networks [16]. There is a general agreement that OSINT should be methodically amassed and scrutinized by intelligence agencies [25]. Although the U.S. has established the National Open Source Center to streamline OSINT initiatives, some argue that further efforts are necessary for its complete assimilation into mainstream intelligence activities [26]. In summary, OSINT offers a rich data source, but challenges related to technology and implementation must be overcome. As new tools and strategies evolve, OSINT’s role as a crucial information source for decision-making is expected to grow.

Legal Challenges

Deploying Open Source Intelligence (OSINT) technologies presents a landscape with legal and ethical obstacles. Concerns arise about the credibility of the data, its privacy implications, and ethical considerations, as identified by Govardhan et al. (2023) [39]. The data sourced from public domains can sometimes be unreliable, and the absence of consent when using such data opens up privacy issues. Rajamäki (2018) adds another layer of complexity by emphasizing the ethical quandaries around automated data collection and its subsequent analysis [61].

On the flip side, when implemented responsibly, OSINT has significant benefits. For instance, it has proven helpful in monitoring events such as mass violence in South Africa, as shown by Senekal (2019) [64]. The use of natural language processing technologies allows OSINT to furnish real-time information. Law enforcement agencies also benefit from OSINT, provided it is utilized within legal and ethical boundaries, as stressed by Akhgar (2017) [16].

To navigate these challenges, various mitigation strategies have been proposed. Holland (2012) suggests algorithmic methods to explore connections in private social networks without infringing on privacy [42]. Furthermore, Böhm (2021) recommends that adherence to data protection laws and ethical guidelines can alleviate some of these challenges [28]. This includes classifying data entities to grasp OSINT data reliability and limitations better.

In summary, OSINT can be a robust tool for intelligence gathering, but legal and ethical constraints temper its potential. These include, but are not limited to, concerns about privacy, data reliability, and algorithmic biases. Strict compliance with legal standards, ethical protocols, and meticulous data verification can ensure OSINT technologies serve their purpose effectively and responsibly.

Financial Challenges

As several studies have noted, financial constraints pose a significant obstacle in deploying Open Source Intelligence (OSINT) technologies effectively. The very nature of OSINT involves gathering and interpreting enormous volumes of unstructured information from publicly accessible web resources, as explained by Pouchard (2009) [60]. This necessitates using sophisticated tools and systems with a substantial price tag for development and upkeep.

Moreover, the complexity of some OSINT tools compounds the financial burden. Baldini (2007) discusses a language-independent OSINT platform that can search and categorize data from open sources, illustrating the high level of investment such systems demand [23]. Fleisher (2008) corroborates that private companies also grapple with funding constraints. Even though OSINT data may be inexpensive and abundant, leveraging it for actionable intelligence still requires significant financial resources [36].

Ven (2008) adds that independent software vendors (ISVs) face challenges of their own, particularly concerning the costs of maintaining and updating open-source software platforms [74]. The situation isn't any easier for public sector bodies and government agencies. According to Holland (2012), constraints such as privacy restrictions on social media platforms necessitate further financial outlay to develop technologies capable of legal data access and analysis [42]. Schwarz (2020) contends that funding is essential for training well-equipped OSINT specialists, particularly for sensitive governmental investigations.

Yet, there are proposals to lessen these financial burdens. Holland (2012) suggests cost-effective algorithms for legal data collection from private social media [42]. Ven (2008) recommends fostering closer collaborations between open-source projects and ISVs to share costs [74]. Akhgar (2017) offers insights into low-cost tools useful for OSINT, although he acknowledges that some level of funding remains indispensable for more advanced operations [16].

To summarize, while OSINT leverages data that is often freely available, the technologies and practices to make it actionable require substantial financial investments. These financial constraints are not exclusive to any sector; they impact private companies, public organizations, and governments. Some strategies may help in cost reduction, but the financial challenges in fully unlocking the potential of OSINT remain considerable [60].

Recommendations

Policy Recommendations

Navigating the Ethical and Legal Terrain in OSINT Applications

Integrating Open Source Intelligence (OSINT) into critical infrastructure protection efforts is fraught with ethical and legal challenges that must be judiciously addressed. Within the domain of the electricity sector, OSINT applications provide a valuable means of assessing vulnerabilities and risks, yet they also pose questions of data ethics, privacy, and legality. Govardhan et al. (2023) underscore this by highlighting the persistent dilemmas surrounding data reliability and the ethics of automated collection methods [39].

In response to these issues, a comprehensive policy framework becomes indispensable for guiding organizations and governmental bodies in the responsible implementation of OSINT technologies. One approach is to design frameworks based on transparency, fairness, and inclusiveness principles. Rajamäki (2018) specifically discusses the need to critically examine automated data collection and analytics processes, calling for scrutiny of how algorithms make decisions [61].

Regulatory bodies can establish explicit boundaries for data collection and analysis for the electricity sector, which is fundamentally crucial to the security and well-being of societies. These would ensure that information gathering remains within the confines of legal and ethical frameworks, particularly when sensitive data or potentially vulnerable systems are concerned.

Enhancing Data Privacy and Reliability in OSINT Deployment

In addition to ethical and legal issues, ensuring data privacy and reliability is another high-priority concern for policymakers working on OSINT applications in the electricity sector. The intersection between OSINT and privacy rights is particularly complex, given that much of the data analyzed is public yet can be used to compromise privacy. Holland (2012) addresses this delicate balance, recommending the development of algorithms capable of identifying relationships within private social networks without violating privacy norms [42].

The electricity sector is a fertile ground for advanced OSINT applications, yet it's also a field with abundant sensitive data. In light of the significance of this sector to national security and everyday life, even seemingly innocuous data can have impactful implications if misused. Therefore, stringent guidelines are required to specify the types of OSINT methods that can be ethically and legally deployed. These could include permissions for certain types of data gathering, mandatory impact assessments for any new OSINT method introduced, and perhaps even specialized oversight bodies to monitor OSINT activities within the electricity sector.

By considering these factors, policymakers can create a robust and ethical environment for deploying OSINT technologies. This will ensure that while we are making strides in protecting our critical infrastructures, we also respect the bounds of privacy, reliability, and legality.

Technical Recommendations

Adopting Cost-Effective Tools and Algorithms in OSINT Implementation

Financing the development and deployment of Open Source Intelligence (OSINT) technologies is a substantial undertaking. As Line Framework (2009) aptly outlines, OSINT's intrinsic need to parse enormous volumes of unstructured data mandates significant financial commitments to acquire the necessary hardware and software solutions [60]. This is particularly salient in the electricity sector, where resources are often earmarked for many operational needs, from infrastructure maintenance to energy production.

To make OSINT more financially attainable, Akhgar (2017) offers insights into using low-cost tools and techniques that don't compromise on the quality of intelligence gathering [16]. This could mean incorporating open-source software that offers similar capabilities to commercial solutions or leveraging cloud-based services for scalable data storage and processing, lowering initial capital expenditures.

In line with this, Ven (2008) recommends a symbiotic relationship between open source projects and Independent Software Vendors (ISVs) to create bespoke solutions that are tailored for specific use-cases in the electricity sector [74]. By pursuing these collaborative models, the industry can reduce the overall financial burden and facilitate the development of tools more aligned with sector-specific requirements.

Addressing Data Accuracy and Algorithmic Fairness in OSINT Practices

As the electricity sector faces increasingly intricate and multifaceted threats, the imperative for precise and unbiased intelligence grows concurrently. Senekal (2019) argues that the efficacy of OSINT is closely tied to the reliability and timeliness of data extraction processes [64]. Poor data accuracy can hinder threat detection and potentially direct resources from actual risks.

To counter this, rigorous quality controls should be implemented significantly as the scale and complexity of OSINT tools increase. These may include the deployment of data validation and verification mechanisms to double-check the authenticity and quality of collected data. Furthermore, real-time data integrity checks could be implemented to assess and ensure the reliability of the data as it flows into the system.

Algorithmic fairness is another facet that needs attention. As AI and machine learning algorithms become more central to OSINT applications, there's a growing need to ensure these algorithms do not inadvertently introduce biases that could skew intelligence gathering and analysis. Auditing practices for algorithmic decision-making should be instated, covering the machine learning models and the data used to train these models. Transparency in algorithmic practices can be another layer of this quality assurance, allowing for external scrutiny to verify that OSINT tools operate under ethical guidelines.

In summary, incorporating cost-effective and open-source technologies can alleviate financial constraints. At the same time, rigorous auditing and algorithmic fairness measures will contribute to the data accuracy and ethical validity of OSINT applications in the electricity sector.

Conclusion

Open Source Intelligence (OSINT) stands at a fascinating juncture—on the one hand, it offers unprecedented capabilities to bolster the security of critical infrastructure like the electricity sector. On the other hand, it presents a labyrinth of ethical, legal, and financial challenges that cannot be overlooked. The future of OSINT, particularly in safeguarding electricity infrastructures, rests on our ability to navigate this complex landscape judiciously.

First and foremost, the promise of OSINT to contribute to critical infrastructure protection is undeniable. As our in-depth analysis has revealed, OSINT technologies can help identify vulnerabilities, counter threats in real time, and augment the overall security posture of the electricity sector. These capabilities are becoming increasingly essential as threats grow more sophisticated and our societal reliance on stable electricity supplies intensifies.

However, the road to effective OSINT utilization is fraught with complications. Ethical considerations around data privacy, legal constraints tied to data collection and use, and the substantial financial resources needed for sophisticated OSINT setups are all factors that organizations must reckon with [60, 42, 74, 16]. The multifaceted challenges make it clear that deploying OSINT is not just a matter of technological implementation but a complex policy issue requiring cross-disciplinary expertise and due diligence.

Therefore, a nuanced approach that balances the utility of OSINT with its responsibilities is imperative. Policymakers and regulatory bodies must construct robust frameworks that delineate the ethical and legal boundaries of OSINT use, mainly focusing on sectors like electricity critical to national security and public welfare. The industry, from utility providers to Independent Software Vendors (ISVs), must embrace and implement these guidelines with fidelity.

Moreover, as the OSINT field evolves, ongoing monitoring and adaptability will be crucial. As new technologies and techniques emerge, the frameworks and policies must also adapt, ensuring they remain relevant and effective in addressing the day's challenges. This dynamic interplay between technology and policy must be at the forefront of any OSINT strategy in the electricity sector.

In summary, the key to unlocking the vast potential of OSINT in critical infrastructure protection lies in adopting a holistic approach that harmonizes the utility and ethical responsibilities of this powerful form of intelligence gathering. For the electricity sector, this would mean advanced, real-time threat detection and mitigation and the peace of mind from knowing these capabilities are exercised within an ethical, legal, and financially sustainable framework. It is a complex but crucial endeavor that calls for the concerted effort of policymakers, security professionals, and industry stakeholders.

Acknowledgments

This work was supported partially by the European Union in the framework of ERASMUS MUNDUS, Project CyberMACS (Project #101082683) (`https://cybermacs.eu`).

References

[1] Critical Infrastructure Protection in Germany. `https://bmi.bund.de/SharedDocs/downloads/`

EN/publikationen/2009/kritis_englisch.html;jsessionid=18C78061072A7ADE54100516B2C8EF5D.2_cid295. Accessed: 2023-12-07.

[2] Critical Infrastructure Resilience Strategy 2023. https://www.cisc.gov.au/resources-contact-information-subsite/Documents/critical-infrastructure-resilience-strategy-2023.pdf. Accessed: 2023-12-07.

[3] Critical National Information Infrastructure in Malaysia. https://www.nacsa.gov.my/cnii.php. Accessed: 2023-12-07.

[4] Critical National Infrastructure in the United Kingdom. https://www.npsa.gov.uk/critical-national-infrastructure-0. Accessed: 2023-12-07.

[5] Cybersecurity Strategy in Japan. https://www.nisc.go.jp/eng/pdf/cs_policy_cip_eng_v4.pdf. Accessed: 2023-12-07.

[6] European Programme for Critical Infrastructure Protection. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52005DC0576&from=EN. Accessed: 2023-12-07.

[7] Law Information Center - South Korea. https://www.law.go.kr/LSW/eng/engMain.do. Accessed: 2023-12-07.

[8] National Infrastructure Protection Plan. https://www.cisa.gov/sites/default/files/2022-11/national-infrastructure-protection-plan-2013-508.pdf. Accessed: 2023-12-07.

[9] Strategic Framework for Critical Infrastructure. https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/srtg-crtcl-nfrstrctr/srtg-crtcl-nfrstrctr-eng.pdf. Accessed: 2023-12-07.

[10] The United Arab Emirates' National Cybersecurity Strategy. https://tdra.gov.ae/userfiles/assets/Lw3seRUaIMd.pdf. Accessed: 2023-12-07.

[11] Turkey's National Cyber Security Strategy and Action Plan (2020-2023). https://www.itu.int/en/ITU-D/Cybersecurity/Documents/National_Strategies_Repository/(3)TURNCSS(2020-2023).pdf. Accessed: 2023-12-07.

[12] OSINT Framework CQR Lib. https://www.cqr.tools/tools/osintframework, 2023. Accessed: 04 December 2023.

[13] A. Abel, P. Parfomak, and Dana A. Shea. Electric Utility Infrastructure Vulnerabilities: Transformers, Towers, and Terrorism [April 9, 2004].

[14] Mari Aarland and Terje Gjøsæter. Digital Supply Chain Vulnerabilities in Critical Infrastructure: A Systematic Literature Review on Cybersecurity in the Energy Sector. In *Proceedings of the 8th International Conference on Information Systems Security and Privacy*. SCITEPRESS - Science and Technology Publications, 2022.

[15] Swati Agarwal, Ashish Sureka, and Vikram Goyal. *Open Source Social Media Analytics for Intelligence and Security Informatics Applications*, pages 21–37. Springer International Publishing, 2015.

[16] Babak Akhgar, P. Saskia Bayerl, and Fraser Sampson, editors. *Open Source Intelligence Investigation: From Strategy to Implementation*. Springer, 2017.

[17] Massoud Amin. Security challenges for the electricity infrastructure. *Computer*, 35(4):supl8–supl10, 2002.

[18] Peter S. Anderson. Critical infrastructure protection in the information age. In *Networking Knowledge for Information Societies: Institutions & Intervention*, 2002.

[19] Uchenna P. Daniel Ani, Hongmei (Mary) He, and Ashutosh Tiwari. Review of cybersecurity issues in industrial critical infrastructure: manufacturing in perspective. *Journal of Cyber Security Technology*, 1(1):32–74, nov 7 2016.

[20] Fernando R. Arduini, Marian Lanzrath, Thorsten Pusch, Michael Suhrke, and Heyno Garbe. A Methodology for Estimating the Criticality of Energy Infrastructures in the Context of IEMI. In *2021 IEEE International Joint EMC/SI/PI and EMC Europe Symposium*. IEEE, jul 26 2021.

[21] Gerhard Backfried, Christian Schmidt, Mark Pfeiffer, Gerald Quirchmayr, Markus Glanzer, and Karin Rainer. Open Source Intelligence in Disaster Management. In *2012 European Intelligence and Security Informatics Conference*. IEEE, 8 2012.

[22] Sean S. Baggott and Joost R. Santos. A Risk Analysis Framework for Cyber Security and Critical Infrastructure Protection of the U.S. Electric Power Grid. *Risk Analysis*, 40(9):1744–1761, jun 15 2020.

[23] N. Baldini, F. Neri, and M. Pettoni. A multilanguage platform for Open Source Intelligence. In *WIT Transactions on Information and Communication Technologies, Vol 38*. WIT Press, jun 14 2007.

[24] Clive Best. Open source intelligence. In *Mining Massive Data Sets for Security: Advances in Data Mining, Search, Social Networks and Text Mining, and Their Applications to Security*, pages 331–343. F. Fogelman-Soulié, 2008.

[25] Clive Best. Challenges in Open Source Intelligence. In *2011 European Intelligence and Security Informatics Conference*. IEEE, 9 2011.

[26] Richard A. Best Jr and Alfred Cumming. Open source intelligence (osint): Issues for congress. Technical Report 28, December 2007.

[27] Matthew Boeding, Kelly Boswell, Michael Hempel, Hamid Sharif, Juan Lopez, Jr., and Kalyan Perumalla. Survey of Cybersecurity Governance, Threats, and Countermeasures for the Power Grid. *Energies*, 15(22):8692, nov 19 2022.

[28] Isabelle Böhm and Samuel Lolagar. Open source intelligence. *International Cybersecurity Law Review*, 2(2):317–337, nov 24 2021.

[29] Adrian Cartagena, Gerald Rimmer, Thomas van Dalsen, Lanier Watkins, William H. Robinson, and Aviel Rubin. Privacy Violating Opensource Intelligence Threat Evaluation Framework: A Security Assessment Framework For Critical Infrastructure Owners. In *2020 10th Annual Computing and Communication Workshop and Conference (CCWC)*. IEEE, 1 2020.

[30] Luigi Coppolino, Salvatore DAntonio, and Luigi Romano. Exposing vulnerabilities in electric power grids: An experimental approach. *International Journal of Critical Infrastructure Protection*, 7(1):51–60, 3 2014.

[31] Maurilio Pereira Coutinho, Germano Lambert-Torres, Luiz Eduardo Borges da Silva, Jonas Guedes Borges da Silva, Jose Cabral Neto, and Horst Lazarek. Improving a methodology to extract rules to identify attacks in

power system critical infrastructure: New results. In *2008 IEEE/PES Transmission and Distribution Conference and Exposition*. IEEE, 4 2008.

[32] H. Davarikia, M. Barati, M. Al-Assad, and Y. Chan. A novel approach in strategic planning of power networks against physical attacks. *Electric Power Systems Research*, 180, 2020.

[33] J. Davis. Hackers take down the most wired country in europe. `https://www.wired.com/2007/08/ff-estonia/`, 2007. Accessed: 14 September 2023.

[34] João Rafael Gonçalves Evangelista, Renato José Sassi, Márcio Romero, and Domingos Napolitano. Systematic Literature Review to Investigate the Application of Open Source Intelligence (OSINT) with Artificial Intelligence. *Journal of Applied Security Research*, 16(3):345–369, may 7 2020.

[35] Stefania Fantinelli and Domenico Franco Sivilli. Open Source Intelligence's Methodology Applied to Organizational Communication. *Mediterranean Journal of Social Sciences*, mar 1 2015.

[36] Craig S. Fleisher. Using open source data in developing competitive and marketing intelligence. *European Journal of Marketing*, 42(7/8):852–866, jul 25 2008.

[37] Guillermo A. Francia III and Xavier P. Francia. *Critical Infrastructure Protection and Security Benchmarks*, pages 4267–4278. IGI Global, jul 31 2014.

[38] Michael Glassman and Min Ju Kang. Intelligence in the internet age: The emergence and evolution of Open Source Intelligence (OSINT). *Computers in Human Behavior*, 28(2):673–682, 3 2012.

[39] Devu Govardhan, Grandhi Guna Sai Hari Krishna, V. Charan, Sribhashyam Venkata Anantha Sai, and Radhika Rani Chintala. Key Challenges and Limitations of the OSINT Framework in the Context of Cybersecurity. In *2023 2nd International Conference on Edge Computing and Applications (ICECAA)*. IEEE, jul 19 2023.

[40] Darren Hayes. Using open source intelligence for risk assessment to the u.s. power grid. In *e-Society 2017*. Pace University, April 2017.

[41] Christopher Hobbs, Matthew Moran, and Daniel Salisbury, editors. *Open Source Intelligence in the Twenty-First Century*. Palgrave Macmillan UK, 2014.

[42] Benjamin Robert Holland. *Enabling Open Source Intelligence (OSINT) in Private Social Networks*. Phd dissertation, Iowa State University, 2012.

[43] Arthur S. Hulnick. The Downside of Open Source Intelligence. *International Journal of Intelligence and CounterIntelligence*, 15(4):565–579, 11 2002.

[44] William Hurst, Madjid Merabti, and Paul Fergus. *A Survey of Critical Infrastructure Security*, pages 127–138. Springer International Publishing, 2014.

[45] Tomislav Ivanjko and Tomislav Dokman. Open source intelligence (osint): Issues and trends. In *INFuture 2019: Knowledge in the Digital Age*, pages 191–196, 2019.

[46] Jacek Jarmakiewicz, Krzysztof Parobczak, and Krzysztof Maślanka. Cybersecurity protection for power grid control infrastructures. *International Journal of Critical Infrastructure Protection*, 18:20–33, 9 2017.

[47] Praveer Kumar Jha, Falti Teotia, and A K Saxena. Cyber Security in the Indian Electricity Distribution System: A Review. In *2023 5th International Conference on Energy, Power and Environment: Towards Flexible Green Energy Technologies (ICEPE)*. IEEE, jun 15 2023.

[48] Cheng Zhi Jiang, Ting Ting Liu, and Xing Chuan Bao. A Security Test and Evaluation Model for Electric Industrial Control Systems. *Applied Mechanics and Materials*, 519-520:1385–1389, 2 2014.

[49] Anastasis Keliris, Charalambos Konstantinou, Marios Sazos, and Michail Maniatakos. *Open Source Intelligence for Energy Sector Cyberattacks*, pages 261–281. Springer International Publishing, 2019.

[50] Dimitris Kostopoulos, Vasilis Tsoulkas, George Leventakis, Prokopios Drogkaris, and Vasiliki Politopoulou. *Real Time Threat Prediction, Identification and Mitigation for Critical Infrastructure Protection Using Semantics, Event Processing and Sequential Analysis*, pages 133–141. Springer International Publishing, 2013.

[51] Seokcheol Lee and Taeshik Shon. Open source intelligence base cyber threat inspection framework for critical infrastructures. In *2016 Future Technologies Conference (FTC)*. IEEE, 12 2016.

[52] Javier Lopez, Cristina Alcaraz, and Rodrigo Roman. On the protection and technologies of critical information infrastructures. In *International School on Foundations of Security Analysis and Design*, pages 160–182. Springer Berlin Heidelberg, 2006.

[53] J. Mbowe and G. Oreku. Critical infrastructure protection. In *Proceedings of the International Conference on Digital Security and Forensics*, pages 33–39, June 2014.

[54] Rohit Negi, Parvin Kumar, Shibashis Ghosh, Sandeep K. Shukla, and Ashish Gahlot. Vulnerability Assessment and Mitigation for Industrial Critical Infrastructures with Cyber Physical Test Bed. In *2019 IEEE International Conference on Industrial Cyber Physical Systems (ICPS)*. IEEE, 5 2019.

[55] Morteza Pakizeh. Threat Identifying Cyber Physical Systems Security. *International Journal of Electrical and Power Engineering*, 13(1-4):5–11, dec 20 2019.

[56] P.B. Pankajavalli, G.S. Karthick, M. Sridhar, and A. Muniyappan. A system for monitoring the electricity substation using internet of things. *International Journal of Advance Research in Science and Engineering*, 6(12), December 2017.

[57] Javier Pastor-Galindo, Pantaleone Nespoli, Felix Gomez Marmol, and Gregorio Martinez Perez. The Not Yet Exploited Goldmine of OSINT: Opportunities, Open Challenges and Future Trends. *IEEE Access*, 8:10282–10304, 2020.

[58] Henri Piat et al. Implementation of interdependent critical infrastructures for electricity supply. In *WSSC 2013-Workshop Interdisciplinaire sur la sécurité globale*, 2013.

[59] Agate M. Ponder-Sutton. *The Automating of Open Source Intelligence*, pages 1–20. Elsevier, 2016.

[60] Line C. Pouchard, Jonathan D. Dobson, and Joseph P. Trien. A framework for the systematic collection of open source intelligence. In *AAAI Spring Symposium: Technosocial Predictive Analytics*, 2009.

[61] Jyri Rajamäki, Sari Sarlio-Siintola, and Jussi Simola. The ethics of open source intelligence applied by maritime law

enforcement authorities. In *ECCWS 2018 17th European Conference on Cyber Warfare and Security*. Academic Conferences and publishing limited, 2018.

[62] Józef Sadowski. The critical infrastructure protection. The genesis. *AUTOBUSY – Technika, Eksploatacja, Systemy Transportowe*, 19(6):1237–1241, jun 30 2018.

[63] Ravi Samikannu, Venkatachary Sampath Kumar, and Jagdish Prasad. A critical review of cyber security and cyber terrorism - threats to critical infrastructure in the energy sector. *International Journal of Critical Infrastructures*, 14(2):101, 2018.

[64] Burgert Senekal and Eduan Kotzé. Open source intelligence (OSINT) for conflict monitoring in contemporary South Africa: Challenges and opportunities in a big data context. *African Security Review*, 28(1):19–37, jan 2 2019.

[65] Hossein Shahinzadeh, Jalal Moradi, Gevork B. Gharehpetian, Hamed Nafisi, and Mehrdad Abedi. Iot architecture for smart grids. pages 22–30, 01 2019.

[66] Rebecca Smith. Assault on california power station raises alarm on potential for terrorism. *Wall Street Journal*, 5(4), 2014.

[67] R. Srivathsav. Cybered #16 types of cybersecurity? `https://medium.com/coinmonks/cybered-16-types-of-cybersecurity-1062dc33e16a`, 2022. Accessed: 16 December 2023.

[68] Chih-Che Sun, Adam Hahn, and Chen-Ching Liu. Cyber security of a power grid: State-of-the-art. *International Journal of Electrical Power amp; Energy Systems*, 99:45–56, 7 2018.

[69] Ika Noer Syamsiana, Arwin Datumaya Wahyudi Sumari, Sigi Syah Wibowo, and Awan Setiawan. Energy Monitoring System for Strategic Facilities Protection from Cyberattacks. In *2019 IEEE 6th Asian Conference on Defence Technology (ACDT)*. IEEE, 11 2019.

[70] Fernando J. Sánchez Gómez and Miguel Ángel Abad Arranz. The need for the protection of critical national infrastructures. In *ISSE 2008 Securing Electronic Business Processes: Highlights of the Information Security Solutions Europe 2008 Conference*. Vieweg+ Teubner, 2009.

[71] Chee-Wooi Ten, Govindarasu Manimaran, and Chen-Ching Liu. Cybersecurity for Critical Infrastructures: Attack and Defense Modeling. *IEEE Transactions on Systems, Man, and Cybernetics - Part A: Systems and Humans*, 40(4):853–865, 7 2010.

[72] Shiva Tiwari, Ravi Verma, Janvi Jaiswal, and Bipin Kumar Rai. *Open Source Intelligence Initiating Efficient Investigation and Reliable Web Searching*, pages 151–163. Springer Singapore, 2020.

[73] Ivo Vacas, Iberia Medeiros, and Nuno Neves. Detecting Network Threats using OSINT Knowledge-Based IDS. In *2018 14th European Dependable Computing Conference (EDCC)*. IEEE, 9 2018.

[74] Kris Ven and Herwig Mannaert. Challenges and strategies in the use of Open Source Software by Independent Software Vendors. *Information and Software Technology*, 50(9-10):991–1002, 8 2008.

[75] Sampath Kumar Venkatachary, Jagdish Prasad, and Ravi Samikannu. Cybersecurity and cyber terrorism - in energy sector – a review. *Journal of Cyber Security Technology*, 2(3-4):111–130, oct 2 2018.

[76] Vinay Kumar Kureel, Manav Arya, Aditya Kini, Suraj Maurya, and Rajesh Gaikwad. Osint Automation Application. *International Journal of Scientific Research in Computer Science, Engineering and Information Technology*, pages 377–381, apr 5 2023.

[77] Yinan Wang, Gangfeng Yan, and Ronghao Zheng. Vulnerability Assessment of Electrical Cyber-Physical Systems against Cyber Attacks. *Applied Sciences*, 8(5):768, may 11 2018.

[78] Douglas Warfield. Critical Infrastructures: It Security and Threats from Private Sector Ownership. *Information Security Journal: A Global Perspective*, 21(3):127–136, 1 2012.

[79] David Watts. Security and vulnerability in electric power systems. In *Proceedings of the 35th North American Power Symposium*, volume 2, 2003.

[80] Margot P.C. Weijnen et al. *Securing Electricity Supply in the Cyber Age: Exploring the Risks of Information and Communication Technology in Tomorrow's Electricity Infrastructure*, volume 15. SECURING ELECTRICITY SUPPLY IN THE CYBER AGE, 2010.

[81] David E. Whitehead et al. Ukraine cyber-induced power outage: Analysis and practical mitigation strategies. In *2017 70th Annual Conference for Protective Relay Engineers (CPRE)*. IEEE, 2017.

[82] Onurhan Yılmaz. *Cyber Security and Open Source Intelligence Techniques*, pages 68–86. IGI Global, 2019.

[83] Ran Yu, Jiao Jiao Zhang, Hong Fei Xu, and Shen Jin. An Integrated Electricity Information Security Monitoring Platform. *Applied Mechanics and Materials*, 701-702:947–951, 12 2014.

[84] Zhen Zhang. Cybersecurity policy for the electricity sector: The first step to protecting our critical infrastructure from cyber threats. *BUJ Sci. & Tech. L.*, 19:319, 2013.

Author Biography

Mert İlhan Ecevit is a Ph.D. candidate in Management Information Systems at Kadir Has University, where he also works as a research assistant. He earned his undergraduate and master's degrees from FMV Işık University in MIS and Information Technologies. His research focuses on critical infrastructure protection through cybersecurity and OSINT methods. Additionally, Mert manages the Center for Cybersecurity and Critical Infrastructure Protection (CCIP) at Kadir Has University, primarily focusing on threat detection, OSINT, and cybersecurity in IT and OT environments.

Mohammad Hasban Pervez is pursuing a master's degree in management information systems while working as a researcher for KHAS CCIP (Kadir Has University Research Center on Cybersecurity and Critical Infrastructure Protection). He received his undergraduate degree in Telecommunications Engineering from N.E.D University of Engineering and Technology in Karachi, Pakistan, and has over two years of network experience.

Hasan Dağ is the Vice-Rector at Kadir Has University, Istanbul, Turkey, and an academic Management Information Systems Department member. His academic background includes a B.Sc. in Electrical Engineering from Istanbul Technical University and an M.Sc. and Ph.D. in Electrical and Computer Engi-

neering from the University of Wisconsin-Madison, USA. Hasan Dağ has contributed to power systems, information technologies, and computational science. He is also the Programme Coordinator and Chair of the Executive Board for the CyberMACS Erasmus Mundus, demonstrating his involvement in international academic collaborations. His research interests include power transmission systems, SCADA, fault analysis, and information system design. Prof. Dağ has supervised numerous theses, published widely, and held various administrative positions, contributing significantly to the academic and engineering communities.

Reiner Creutzburg is a Retired Professor for Applied Computer Science at the Technische Hochschule Brandenburg in Brandenburg, Germany. Since 2019, he has been a Professor of IT Security at the SRH Berlin University of Applied Sciences, Berlin School of Technology. He is a member of the IEEE and SPIE and chairman of the Multimedia on Mobile Device (MOBMU) Conference at the Electronic Imaging conferences since 2005. In 2019, he was elected a member of the Leibniz Society of Sciences to Berlin e.V. His research interest is focused on Cybersecurity, Digital Forensics, Open Source Intelligence (OSINT), Multimedia Signal Processing, eLearning, Parallel Memory Architectures, and Modern Digital Media and Imaging Applications.