Open-Source Intelligence (OSINT)-based Technologies for Online Payments in Saudi Arabia

Ahlam Alhalafi [1] and Prakash Veeraraghavan [1], Dalal Hanna [2]

La Trobe University, Computer Science & Information Technology Department.

Abstract
This research examines how open source intelligence (OSINT) applications are used to secure online payment systems. These technologies could transform digital transaction security in the face of rising cyberthreats. The research shows how AI and blockchain can automate threat detection, ensure data integrity, and enable secure, transparent transactions, offering promising solutions to online payment system issues. It also discusses implementation issues like regulatory compliance, scalability, and the need for specialized technology management knowledge. The study explains how AI and blockchain strengthen online payment systems against fraud and cyberattacks, making the digital financial landscape more secure through theoretical frameworks, case studies, and real-world applications. The study also places its findings in the context of Saudi Arabia's Vision 2030 initiative to digitize the economy and integrate cutting-edge technologies across sectors, including finance. It discusses Saudi challenges and opportunities, such as the need for tailored blockchain solutions and the strategic importance of developing a skilled workforce to support AI adoption. The research helps policymakers, industry practitioners, and academics understand the potential impacts, ethical concerns, and practical challenges of using AI and blockchain to improve payment security. It emphasizes strategic planning, cross-sector collaboration, and ongoing innovation in using these technologies to protect Saudi Arabian and international online payment systems.

Keywords:
Open source intelligence (OSINT), online payment, Saudi Arabia

1. Open Source Intelligence (OSINT)

The term *"Open Source Intelligence"* (OSINT) originally defined a specific intelligence collection method. In general, intelligence sources collect initial data. As outlined by the Office of the Director of National Intelligence in 2011, this data can be processed through the six intelligence cycle phases to gain meaningful insights. OSINT generates intelligence from public sources. The Office of the Director of National Intelligence (2011) defines this as collecting, using, and quickly distributing information to meet an intelligence need. Data and information have enriched intelligence, with artificial intelligence changing traditional practices (Mei, 2020). OSINT has grown in popularity among intelligence communities and academics. OSINT has grown from a niche activity to a collaborative, networked effort (Hong, Zhu & Jiang, 2020). However, China's intelligence efforts are hampered by disorganized operational processes, inefficient intelligence gathering, and questions about intelligence output reliability. To address these challenges, open-source intelligence capabilities, intelligence operations structure, intelligence personnel expertise, and communication and collaboration must be improved (Mao & Yu, 2021).

Scholarly research on OSINT focuses on its definition, processes, and applications (Liu et al., 2023; Mei, 2020). According to the CIA, OSINT comes from media, commercial databases, and other processed data (Ma, Gen & Wang, 2017). Only legally gathered intelligence from publicly licensed sources is considered open-source by NATO. Ding (2017), a Chinese academic, suggests two perspectives on open-source intelligence: a narrower view emphasizes the source's transparency, maintaining some secrecy over the content, while a broader view emphasizes the intelligence process's openness, allowing public participation and intelligence sharing. This paper follows Ding's broad interpretation of open-source intelligence as a model with a feedback loop, transparent information sources, and participatory intelligence work but reserves the intelligence for designated recipients. Despite presentation, open-source intelligence comes from transparent and accessible sources (Mei, 2020).

Studies estimate that 70–90% of modern intelligence material comes from OSINT, which is publicly available (Unver, 2018, p. 5). The growth of open-source information and computer science, data science, and statistics advances have made its collection and analysis more efficient. OSINT analysts' effectiveness is closely tied to the sophistication of their technological tools, as AI systems have improved this process. Thus, the growth of these technologies raises important governance issues in academic and practical contexts (Liu et al., 2023). Addressing the legal, ethical, and regulatory issues arising from the growing complexity of AI interactions throughout

Manuscript received August 5, 2025
Manuscript revised August 20, 2025
https://doi.org/10.22937/IJCSNS.2025.25.8.7

the OSINT process—direction, collection, processing, analysis, dissemination, integration, and feedback—is crucial.

AI algorithms have been tested for OSINT analysis (Evangelista et al., 2021), and the GDPR has been discussed about OSINT (Shere, 2020). The Governance, Ethical, Legal, and Social Implications (GELSI) framework for OSINT needs further study. This research provides a systematic review of OSINT literature within the GELSI framework, as defined by Grant and Booth (2009, p. 102), by searching and analyzing relevant studies. This work collects OSINT-related articles and filters them to highlight those that address the GELSI framework to summarize existing research and suggest future research.

1.1 OSINT history and background

Numerous writers have placed the origins of OSINT on the eve of World War II, citing the BBC Monitoring Service in the United Kingdom in 1939 and the Foreign Broadcast Monitoring Service (FBMS) in the United States in 1941 (Colquhoun, 2016). These initiatives, which arose in response to the emergence of radio as a burgeoning technology, are frequently cited as seminal, structured efforts to collect and analyze data from publicly available sources. Conversely, this manuscript contends that OSINT has a much longer history and is rooted in a rich institutional tradition. Colquhoun (2016) credits William Donovan with founding OSINT. During World War II, Donovan helped found the Office of Strategic Services, which would become the CIA, the US Foreign Intelligence Service. This agency had a division that analyzed public information. This division collected international newspapers, magazines, and radio broadcasts. According to Colquhoun (2016), Donovan believed that a careful observer could reveal a nation's secrets through publicly controlled media.

OSINT has risen to prominence in recent decades, largely thanks to the digital revolution (Block, 2023). The proliferation of the internet and digital methods for creating and storing data has drastically altered the landscape and availability of public information. These developments have significantly improved the intelligence community's ability to gather and use open-source data (Larsen, 2022). This era of technological advancement has also resulted in increased academic interest in open sources in the field of intelligence studies. Steele (1990) introduced the term 'OSINT' and the acronym 'OSINT' to the literature. In a significant development, a 1993 special edition of the American Intelligence Journal dedicated itself to OSINT, compiling contributions from the first-ever open-source intelligence conference held in 1992 (Steele, 1993).

Despite the recent emphasis on open-source data collection and analysis, the strategic value of publicly available information has long been recognized. For example, William Donovan's seminal publication in 1946 highlighted the invaluable role of open sources during World War II, providing illuminating examples of their utility (Bagnall, 1958; Becker, 1957; Croom, 1969). Classic literature by figures such as Kent and Dulles have emphasized the importance of 'overt information' or 'overt intelligence' within the intelligence framework (Donovan, 1946). Nonetheless, the term 'OSINT' did not become popular until the 1990s, and widespread adoption in intelligence circles took another couple of decades (Dulles, 1963; Kent, 1949).

Some scholars argue that practices similar to today's open-source intelligence date back millennia. Westcott, for example, notes that ancient communities such as Viking explorers, Roman legionnaires, and Silk Road merchants practiced primitive forms of OSINT by closely observing and sharing information about their surroundings (Evangelista et al., 2020). Echoing this sentiment, Schaurer and Storger (2013) argue that using publicly available information for intelligence dates back to the origins of intelligence as a governmental support tool (Westcott, 2019). They acknowledge, however, that a systematic, institutional approach to exploiting foreign media for intelligence only emerged once the United States pioneered the formation of the FBMS, which set the stage for the formal establishment and professionalization of OSINT (Schaurer & Storger, 2013).

1.2 Understanding the role and usages of OSINT.

It is essential to distinguish intelligence from data or information by identifying its sources. Military intelligence is usually divided into HUMINT and TECHINT (Stenslie et al., 2019). Technological sources enable intelligence gathering through signals, imagery, measurements and signatures, geographic information, and open sources ‘OSINT’. These methods are intelligence disciplines. A knowledge requirement (IR) is the first step in any intelligence activity. An IR includes any information needed to understand a scenario (UK Ministry of Defence, 2011) and may arise from informational gaps or direct requests from intelligence users (Forsvaret, 2021). The intelligence-gathering entity must choose the best intelligence discipline based on the IR (Liska, 2014, p. 24). With the digitalization of the world, OSINT has expanded to use the vast amount of publicly available information (Pastor-Galindo et al., 2020). In the 1990s, OSINT focused on translating foreign press. In cybersecurity, open-source information is crucial for preparedness (Williams & Blum, 2018). In recent years, social media and other online resources have made open sources a rich source of potentially valuable information.

OSINT is interpreted differently by military agencies, technical operations centers, and large corporations due to its diverse user base. The name OSINT implies that OSINT is intelligence gathered from public sources. What constitutes *"open sources"* is debatable. Pastor-Galindo et al. (2020, p. 10282) define open source information (OSIF) as *"mass media, social networks, forums and blogs, public government records, publications, or commercial data,"* while Williams and Blum (2018, p. 10) define it as material that the public can legally request, purchase, or observe. This thesis defines OSINT as legally sourced material from publicly available sources, whether manually or automatically, and via internal or external (third-party) systems. However, OSINT must be distinguished from OSINF, information without intelligence value. These terms should intersect since OSINT collects information from many sources. Williams and Blum (2018) offer a diagram (Figure 1) showing how these disciplines interact, adding to the discussion on OSINT's definition and role as a process and product. According to Williams and Blum (2018), our perception of OSINT as a distinct discipline affects how the intelligence community prioritizes intelligence output from single or multiple sources.

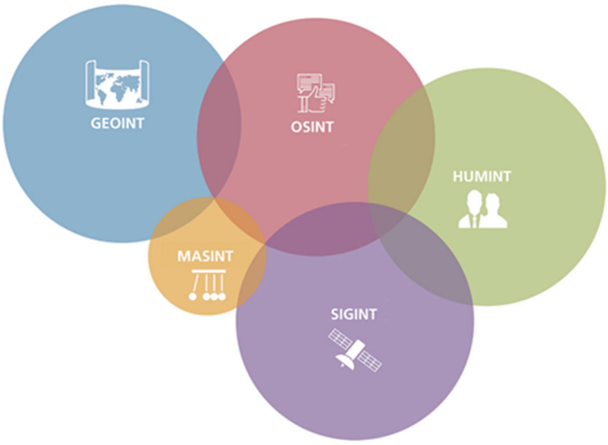

Figure 1. Overlapping of intelligence systems (Williams & Blum, 2018, p. 9)

1.3 Exploring the relationship between OSINT and security.

In a cyber-attack, quick and cautious decision-making is essential. A complete situational awareness before a cyber-threat can improve decision-making. During an attack, defenders and opponents compete for superiority and must make informed decisions (Crowe et al., 2021). Crowe et al. (2021, p. 233) define *Cyber Situational Awareness (CSA)* as *"gathering and analyzing information from diverse sources to equip security analysts with the precise data needed for making informed decisions about potential security risks."* In a systematic review, Pai Yogish and Krishna Prasad (2021) examine how OSINT advances cybersecurity technologies.

Understanding the importance of cyber situational awareness in decision-making emphasizes the need for accurate and relevant data in the cybersecurity threat environment. Cyber Threat Intelligence (CTI), including OSINT, can improve decision-making and defenses without planning for every weakness (Tundis et al., 2022). Despite cyber threats, organizational preparedness is being boosted. Shin and Lowry (2020) criticize this strategy for failing to address the growing complexity of cyber threats. They compare it to Baskerville et al. (2014) prevention paradigm, which views threats as constant and quantifiable, suggesting a continuous link between threats and countermeasures. This suggests that organizational defenses are static and reactive to evolving and sophisticated cyber threats. Shin and Lowry (2020) suggest adopting Baskerville et al. (2014) response paradigm, which promotes a proactive defense mechanism. After this reactive-to-proactive shift, OSINT can gather actionable intelligence to inform strategic decisions. Gibson (2016) notes that OSINT can be used reactively or preemptively to gather intelligence on a cyber-incident or potential cyber event.

Understanding the threat landscape before an attack helps identify attacker methods and tools (Crowe et al., 2021). According to Tundis et al. (2022), security experts can use their CSA to more easily identify anomalies that may indicate a cyber-attack by using open-source intelligence. This could involve monitoring for new threat campaigns or vulnerabilities attackers could exploit. OSINT also helps digital forensics track threat actors in a compromised network (Qusef & Alkilani, 2022). Data integrity in OSINT tool repositories is crucial. Integrity means maintaining data consistency and accuracy to prevent unauthorized changes (Alkhudhayr et al., 2019; Barona & Anita, 2017). Unauthorized access and modification of public data can damage its credibility. This may lead users to unknowingly spread false information, laying the groundwork for cybercrimes like fake news (Tabatabaei & Wells, 2016). Thus, data integrity is essential to OSINT. Protecting data integrity is crucial for national security because attackers often use OSINT data for evil. Financial crimes and cyber terrorism, including network and DoS attacks, can result from OSINT data exploitation (Yeboah-Ofori & Brimicombe, 2018). Thus, user authentication and access controls are necessary to protect sensitive and critical OSINT data.

OSINT in security can prevent cyberattacks and terrorism. Research is underway to use OSINT to defend against cyberattacks (Wells, 2016). The U.S. Office of Homeland Security reports that OSINT data is used for general intelligence gathering, warnings, domestic counterterrorism, critical infrastructure (cyberspace), and managing emergencies related to primary national security missions (Tabatabaei & Wells, 2016). Thus, OSINT-derived data governance is crucial to cybersecurity. Intelligence, security, and public safety agencies must collect various data, including terrorism and cybersecurity threats. This data must be refined into actionable intelligence using OSINT and managed with strict security protocols to maintain integrity and confidentiality (Chen, Chiang & Storey, 2012). Therefore, there is a strong relationship between the security and OSINT.

1.4 How Artificial Intelligence (AI) leverages OSINT for data gathering.

Starting the intelligence cycle with a well-defined question requires gathering, processing, and analyzing massive amounts of publicly available data, which requires automation for efficiency. Tools and techniques can improve the collection phase. Given the specialized nature of many and the ever-changing landscape of external tools, cataloging these tools is challenging. Developers often discontinue their tools, as Bazzell (2021) did when he retired his popular interactive online tools (Bazzell, 2021) or made resources like search. Facebook and Instagram actively disrupt OSINT tools and methods, including web service blocking, frequent source code updates, and limiting features (Bazzell, 2021). Instagram embeds particular character encoding in website source code to obscure direct URL extraction.

OSINT has adapted to these challenges by refining and updating its methods. Thus, any list of tools and techniques is temporary and may need to be updated. Category and review of these tools and techniques are attempted. The OSINT Framework (Nordine, 2021) is a well-organized resource that helps find OSINT tools for specific search queries. Its tree structure has identifiers at the root and potential tools as branches. User-friendliness is another highlight of Michael tool list. According to Bazzell (2021), these tools are well-documented, updated, maintained, and accessible via virtual machines. OSINT is essential for data collection, penetration testing, and other IT tasks. Search engines, especially Google Hacking (Long, 2005), are a good starting point for OSINT investigations. Several tools, such as human activity tracking tools, are designed to probe IT systems. Many tools can aid detailed searches, depending on the criteria. A company's website can be examined for technologies (BuiltWith, 2021) and security vulnerabilities. Tools can also find websites with the same Google Analytics ID (Reverse analytics id 0000) or view a website's history in an internet archive.

With a domain name search, tools can reveal ownership (WhoIs Online Service, 2021), subdomains (Aboul-Ela 0000), and open ports using specialized search engines that index pre-scanned data. Some services offer active port scanning (Nmap 0000) and unpatched security vulnerability data (Cyberscan, 2021). Analysts may search job ads and employee profiles on social media for skill mentions to learn about a company's IT landscape and its technologies and systems. Use spiderSilk (Spidersilk, 2021) or compare the versions of identified technologies to databases of known vulnerabilities to analyze this data.

Researchers are studying OSINT more and more. An influential 2022 study (Hwang et al., 2022) examined OSINT and its role alongside traditional intelligence methods. Hwang et al. (2022) examined OSINT's cyberspace role and its pros and cons. Lee, Park, and Park (2022) showed that OSINT can find much information, but processing it is difficult. It stressed the importance of verifying OSINT data sources before concluding. Tabatabaei and Wells (2016) also examined OSINT's military use for information breach detection. The researchers tried different tools and military keyword searches to find relevant data. Such investigations demonstrate the value of OSINT for specific goals but also highlight the need to integrate these tools into cyber attack and defense strategies. This paper critically evaluates many cutting-edge OSINT tools from an offensive and defensive perspective.

The study uses the Lockheed Martin (2014) *Cyber Kill Chain framework* to classify OSINT tools across cyber aggression and defense phases. The Cyber Kill Chain model organizes defensive strategies against active threats by describing the attack's stages. The need to sift through massive security data has highlighted the intersection of OSINT tool use and AI techniques in detecting malicious cyber activity (Branco, 2017). AI is used to automate public information analysis to identify cyber threats. Social media has exponentially increased intelligence operatives' data analysis. As technology increases intelligence data, the challenge becomes turning it into actionable intelligence. This deluge of Big Data requires advanced data processing. AI methods are increasingly recognized for managing Big Data, especially OSINT's unstructured data. Today's intelligence analysts face unstructured data, highlighting the need for advanced tools to navigate open-source intelligence gathering.

2. OSINT and Security Analysis

Digital tools benefit progress and connectivity but are also used for crime, terrorism, and other harm. To combat these threats, the military, security agencies, and law enforcement have had to innovate and adopt new strategies (Hassan & Hijazi, 2018). Privacy-conscious people also adopt OSINT methods due to concerns about online data exposure and security. They monitor their online presence with these methods to protect their privacy (Hwang et al., 2022). API keys are needed to complete Recon-ng reconnaissance. These keys help enumerate server-side technologies, detect vulnerabilities and configurations, assess physical security flaws, and find exposed credentials (Dodd, 2015). Therefore, OSINT is now working with applications and systems to watch the security and privacy issues.

2.1 Examining the advantages of OSINT in security.

OSINT's context, non-intrusiveness, exploration, and cost-effectiveness make it a better intelligence-gathering method. According to Pastor-Galindo et al.

(2020), OSINT is the best way to establish context in fields like economics, crime, environmental studies, psychology, and national security. OSINT helps understand a topic by providing a broader perspective than covert secrets. Scholars who have spent years in their fields often provide deep, contextual knowledge to this broad view (Steele, 2001, p. 48). Foreign intelligence and military operations require context, as open sources provide cultural, socio-economic, geospatial, and strategic information (Olaru, 2015). The CIA's focus on Al-Qaeda overshadowed other terrorist groups in the 2012 Benghazi attack (Hensley, 2016). This shows how OSINT can help intelligence agencies detect early warnings and online radicalization, preventing terrorism and extremism (Staniforth, 2017).

The second benefit of OSINT is its low intrusiveness, which meets public demands for more accountable intelligence services. OSINT is the most legally and ethically sound method, making it appealing to the public despite its challenges (Steele, 2001). By defining known and unknown areas, OSINT efficiently guides secretive operations as a precursor to covert intelligence activities, proving its exploratory value. Secretive methods are impractical when open sources are sufficient (Gibson, 2014). Another benefit is cost efficiency, with OSINT yielding high returns on low money or time investments. OSINT and digital technologies increase intelligence processing speed, which is crucial for military operations by reducing observation and command time (Ashwell, 2017). Open-source analysis is fast, but data organization is laborious. Automated analyses can identify social media bots (Pastor-Galindo et al., 2020; Sferrella & Conger, 2020). Free secondary sources help OSINT reduce costs by providing external expertise (Steele, 1995), making it the most efficient input-output technique (Gibson, 2014).

Beyond these benefits, OSINT's utility extends to the vast amounts of online data, from social media feeds to deep web content that no other intelligence-gathering method can match. It can also reveal hidden details, as in the case of an Australian researcher who discovered a major Indonesian counterinsurgency operation in an Indonesian museum (Packer, 2006). OSINT allows for analyzing events in distant nations where HUMINT agents are impractical (Steele, 2001). OSINT's low risk makes it a responsible choice for data sharing between intelligence agencies and private entities. However, its classification as unclassified information is debatable (Holland, 2012). OSINT can also inspire analysts to think creatively, identify adversaries' weaknesses, and find strategic advantages (Benes, 2013). Forecasting requires imagination to anticipate and prepare for new threats, improving risk assessment.

2.2 Examining the disadvantages of OSINT in security.

Although OSINT has a few disadvantages in security and analysis, it can hinder its effectiveness. The main concerns with OSINT are legal and ethical. OSINT may include sensitive unclassified data despite being derived from open sources (Hu, 2016). This calls into question the use of public domain private data. OSINT researchers must consider privacy issues and follow EU regulations like the GDPR (Ten, 2020). Open sources present three major ethical issues (Hu, 2016). Information sensitivity comes first. OSINT often contains sensitive personal information (PSI) such as sexual preferences, political views, birth dates, parents' names, and identification numbers (Eijkman & Weggemans, 2012). The second challenge is information provenance, especially the ethical dilemma of considering leaked classified data public. Some call this NOSINT ('N' denoting 'NOT') because it is based on classified material (Hassan & Hijazi, 2018,), complicating whistleblowing. Whistleblowing has revealed illegal government actions (Dunn, 2016), but its motivations and effects can vary, exposing unnecessary information. The third issue is dependability. Unvetted public information may spread false information that harms individuals or groups.

OSINT activities on social media often occur without subjects' knowledge or consent, raising ethical concerns and requiring stricter permissions. Social media content downloads are irreversible, so users lose control over their data privacy settings (Ten Hulsen, 2020). Data usage may not worry social media users, but context misuse does (Eijkman & Weggemans, 2012). The legal doctrine of a "reasonable expectation of privacy" diminishes once information is shared online, so individuals must carefully manage their data sharing (Ssclegacy.com, 2021; Ten Hulsen, 2020). However, this ignores public ignorance of data exploitation risks and third-party data sharing, such as photo tagging (Edwards & Urquhart, 2016). Social media intelligence gathering may require "directed covert surveillance" authorizations under the Regulation of Investigatory Powers Act (RIPA) in the UK (Edwards & Urquhart, 2016). Private OSINT practitioners must protect privacy and prove their findings in court (Ssclegacy.com, 2021).

The use of advanced OSINT technologies also presents challenges. Technology cannot only partially replicate human intelligence analysts' nuanced analytical skills, which are essential for interpreting data, formulating hypotheses, and making decisions. While beneficial, technology dependence creates vulnerabilities, mainly as OSINT relies more on analytical software and vast online data collections, potentially neglecting traditional intelligence sources. While beneficial, OSINT's volume of data, or *"noise,"* can overwhelm analysts, complicating speed and cost-efficiency (Expert.ai, 2017). This issue will worsen with 5G internet (Hassan & Hijazi, 2018). The *"echo"* effect, where multiple sources repeat a news story, complicates source verification and truth assessment (Best and Cumming, 2008). Misinformation is a significant risk for OSINT, primarily online, where it is hard to tell fact from fiction, emphasizing the need for source validation. Finally, when secret information is needed, OSINT often only scratches the surface of hidden issues, especially when dealing with wary and secretive subjects (Pallaris, 2008). OSINT has many benefits. However, it can only replace some-source analysis (Holland, 2012).

2.3 Cases how attackers exploit OSINT for targeted and untargeted attacks

The study examines different case studies from the US, Germany, the Netherlands and Saudi Arabia to better understand OSINT attacks. These cases draw from literature and archival research. These case studies are important because they show how early OSINT efforts shaped modern intelligence practices.

2.3.1 OSINT during American Civil War

In *"Yankee Reporters and Southern Secrets,"* Fuhlhage examines the unprecedented rise in journalistic information collection during the Civil War. He believes this surge expanded civilian and military threat intelligence (Fuhlhage, 2019). According to Fuhlhage, the partisan media landscape of that era acted as a vast surveillance apparatus (Fuhlhage, 2019). According to him, Union sympathizers used cover stories, disguises, ciphers, and countermeasures to avoid detection. Fuhlhage also shows that both sides used newspaper information, regardless of who gathered it. Fuhlhage examined 18 newspapers from December 13–28, 1860. He found 3,079 secession-related articles, with 1,423 containing actionable information. This data was divided into political, economic, military, cultural, and technological categories. Most intelligence-worthy information was about political developments, especially secession conventions. Second in importance was military data like troop deployments and organizational structures. His findings provided economic insights, including currency shortages and trade disruptions, as well as cultural and technological insights.

Maslowski, like Fuhlhage, recognized the significance of systematically acquiring opposing newspapers for their valuable information (Maslowski, 1988). Such military force and strategy information could be operational intelligence. Fuhlhage emphasizes that both parties were aware of strategic intelligence, including philosophical doctrines, goals, and planned actions (Fuhlhage, 2019). He studied how newspaper information affected decision-making and early intelligence organizations' development. In 1863, the Army of the Potomac established the Bureau of Military Information, starting systematic press information exploitation. In 1864, this bureau regularly briefed on Confederate press content, influencing decision-making increasingly. Fuhlhage's findings show that both sides used newspaper information during the Civil War. They went beyond information curiosity to assess enemy military capabilities and strategic intentions. This practice captures the essence of OSINT, showing its roots in the US before modern intelligence agencies. As we examine early 20th-century European intelligence practice, we expect similar patterns.

2.3.2 OSINT cases from Germany

Established in 1889, the German military's intelligence division (officially Sektion IIIb and colloquially Nachrichtendienst was a vital part of the General Staff's structure (Pöhlmann, 2005, p. 27). Its main role during peacetime was gathering information, while other General Staff departments focused on specific geographical areas performed analytical duties. Sektion IIIb's intelligence collection was guided by these departments based on their informational needs (Foley, 2005; Schmidt, 2005). Section IIIb used four main intelligence gathering methods (Foley, 2005). These included military attachés, agents, and encouraging German army officers to travel abroad for leisure. Many Sektion IIIb personnel, from 22 in 1914 to 83 in 1918, focused on 'Zeitungsrecherche' or newspaper research. Systematic collection and analysis of foreign newspapers was used.

Open sources like military publications and international newspapers were vital intelligence sources before World War I, according to Pöhlmann. These sources illuminated military doctrines, armament developments, and strategic policy. Wartime censorship reduced the availability and usefulness of these sources (Pöhlmann, 2005). However, German military intelligence history shows that open-source intelligence was effective throughout the conflict. In spring 1915, Sektion IIIb began publishing biweekly reports called 'Eindrucke aus der Auslandspresse,' or 'Impressions from the Foreign Press.' Segmented reports on military, political, and economic aspects were distributed to German army supreme command units and selected intelligence officers (Schmidt, 2005). Systematic collection of French and Russian newspapers enabled this dissemination. In Sektion IIIb, 24 Russian newspapers were selected for government, economic, industrial, and general news coverage (Schmidt, 2005). Schmidt notes that these publications provide valuable intelligence on political assessments, Russian military and bureaucratic personnel changes, mobilization efforts, and economic indicators like raw material prices. Press disclosures, even accidental, provided intelligence on Russian troop movements, similar to the Civil War era's newspaper use for intelligence.

Pöhlmann highlights that Sektion IIIb's intelligence efforts in France relied heavily on Swiss intermediaries, with the military attaché in Berne playing a crucial role in cooperation (Pöhlmann, 2005). A 1918

Gendarmerie manual noted Swiss entities' suspicious interest in subscribing to French newspapers, indicating French awareness of this activity. Despite censorship, newspapers could accidentally reveal enemy-valued information, the manual warned. Foley found that German Nachrichtendienst reports on France identified French military tactics as vulnerable and strategic, considering political influences, demographic trends, and societal shifts (Foley, 2005). German intelligence used public sources, focusing on French military expenditures to infer wartime intentions. Revue militaire générale, Sciences militaire, Le Temps, and Écho de Paris were crucial. Analysts estimated that France's governance style led to increased press leaks of sensitive information, demonstrating the strategic use of open sources in German military intelligence (Foley, 2005).

2.3.3 OSINT cases from the Netherlands

The Dutch military began gathering open-source intelligence before their intelligence services were established. In the 1870s, the Army's General Staff began collecting data on 'foreign armies' using diplomatic reports and public publications (Engelen, 1999). The 1879 General Staff records analyze 'Revue Militaire d'Etranger', including summaries of articles on the Austrian-Hungarian Officer's Handbook (Schmidt, 2005). Early recognition of open-source information includes German newspaper reports on army budget discussions in 1899 and monthly summaries in the 'Militaire Spectator' from 1870, which highlighted articles from international military journals. These actions show appreciation for such information, but they do not necessarily follow current OSINT definitions. The Netherlands' first official military intelligence service was established in 1914 to organize open-source information gathering. In 1912, the Study Bureau for Foreign Armies (*'Studiebureau Vreemde Legers'*) was established as a small entity before becoming part of the General Staff as GS III on June 25, 1914. General Fabius led the bureau to a team of 23 by 1918 (NIMH, 1951).

From 1912 to 1914, GS III specialized in utilizing open sources, gaining expertise in their use. General Fabius wrote in 1921 that the press and public documents were essential to gathering actionable intelligence. He explained how analyzing German army casualty data and French obituaries revealed combat strengths of both forces (Fabius, 1921). He emphasized the importance of thorough media coverage, including major and minor publications, in understanding the structure of the British military. During World War I, GS III added intelligence collection methods, such as establishing a scout network and collaborating with military attachés (Engelen, 1999). While not part of GS III, these attachés were effectively overseen by GS III for intelligence gathering, despite being officially directed by the General Staff's head. Their reports were required to be based on direct observations, discussions, and open sources like press reports, parliamentary records, and military and economic analyses (Vinke, 1989).

Reports on naval strength and organization in the General Staff's archives were often written by naval officers and did not include GS III markings (NIMH, 1951). GS III documents made use of open sources, such as English, German, and Russian newspaper articles, as seen in a 1915 naval engagement briefing.

2.3.4 OSINT cases from Saudi Arabia

Understanding Saudi Arabia's (KSA) involvement in Yemen requires seeing its strategic motives rather than a coincidence. The Kingdom of Saudi Arabia uses soft power to promote stability and security in its foreign policy (MEPC, 2013). The conflict in Yemen presents a chance for Saudi Arabia to counter Iran's influence in the Middle East while strengthening its own influence (Hartmann, 2016). It is difficult to understand the motivations behind the KSA's actions in Yemen, as it aims to limit foreign involvement (Fenton-Harvey, 2019). Saudi Arabia's religious institutions have had a major impact on Yemen (McDonnell et al., 2017). Support for the Saudi-led coalition has grown due to this influence (McDonnell et al., 2017). Saudi Arabia entered the conflict in 2015, claiming to protect Sunni Muslims in the region (Matthiesen, 2015). Saudi clerics with large online followings have shaped conflict discourse. The prominent cleric Salman al-Awda has advocated for the intervention, arguing on social media that actions against the Houthis are religiously justified (Matthiesen, 2017). Mohamed al-Arifi advises Houthi-allied Yemenis to distance themselves to avoid supporting the "Safavid" state, referring to the historical Persian empire (Matthiesen, 2017). Ayid al-Qarni praised Yemeni opponents of the Houthis as divine warriors (Mandaville & Hamid, 2018). Religious narratives have heavily influenced public opinion by gaining Islamic support for Saudi foreign policy.

Saudi media and religious figures have portrayed the Yemeni conflict as a sectarian conflict between Sunnis and Shiites, portraying Shiites as a regional threat (Darwich, 2018). As a result of civilian casualties from military actions, the KSA has engaged with PR firms to maintain a positive image in Yemen and manage perceptions (Nasser, 2017). Public sentiment in Yemen has been impacted by these incidents, challenging Saudi Arabia's regional leadership efforts (Darwich, 2018). Saudi attempts to influence Yemeni women through religious narratives, such as television channels like Iqraa, demonstrate a multifaceted approach to influence. While the exact impact of these efforts is unknown, it suggests a strategic focus on media control to shape future outcomes. Information management is crucial to long-term goals, and this approach shows Saudi recognition of this.

2.4 Addressing the impact of OSINT security issues on online payment systems

The financial sector now refers to *"digital payments", "digital money", "electronic money", "online payment systems",* and *"mobile payments"* as *"paytech"*—a subset of fintech services that facilitate payments and financial transactions (Polasik et al., 2020). Paytech provides electronic payment methods directly or through third parties (AEFI, 2022). Additionally, Capgemini (2021) adds that digital apps and contactless wearable technology can address peer-to-peer payments and merchant services in e-commerce and traditional markets (Palmié et al., 2020). Al-Qudah et al. (2020) examined Arabic customers' opinions of Jordan's main online payment system, eFawateercom. They used three algorithms to analyze Twitter and Facebook customer feedback. Paytech is a vital and fast-growing fintech sector, especially for consumers (Belanche et al., 2022). Payments are becoming seamless, integrated, and crucial to collaborative customer experiences in this sector post-pandemic (Capgemini, 2021).

Understanding the drivers of peer-to-peer (P2P) payments is crucial as fintech firms explore their potential (Belanche et al., 2022). This "winners-take-all" market is fiercely competitive due to users' heavy use of technology and networking (Wirtz et al., 2018), necessitating research to help paytech firms dominate the P2P payment market. Liébana-Cabanillas et al. (2021) found that P2P payment systems are adopted for different reasons than smartphone-based payments, highlighting their uniqueness compared to general mobile payment solutions (Li and Xu, 2021). This emphasizes the need for targeted P2P payment adoption research.

Open-Source Intelligence (OSINT) is crucial for online payment cybersecurity, which relies on rapid information flow (Neubert, 2024). Financial institutions can monitor cybercriminals' online platforms and prepare for cyber threats and financial fraud by using OSINT to proactively analyze publicly available data. Real-time surveillance helps banks detect and mitigate financial fraud like phishing and account takeovers and stay ahead of evolving cyber threats. Banking integrity and trust depend on this proactive and vigilant approach. OSINT is crucial to fraud detection, especially when automated systems fail and require manual analysis (Yadav, Kumar & Singh, 2023). Keeping up with fraudsters' evolving tactics requires monitoring underground forums and the dark web. Identity verification, transaction credibility, and customer profile fit are analysts' main concerns.

Rajamäki (2020) examines cyber surveillance using OSINT and Big Data Analytics (BDA), focusing on privacy issues. Rajamäki (2020) examines the privacy implications of OSINT and BDA practices and how maritime surveillance agencies can build public trust in their reconnaissance. Maritime Integrated Surveillance Awareness (MARISA) privacy issues are empirically analyzed. To promote discussion about privacy violations that could limit personal freedoms and undermine trust.

3. Saudi Context and Challenges

The global shift from cash to digital payment methods like online wallets, credit and debit cards, and buy now, pay later schemes is growing. By 2025, the global digital payment sector could reach 11.95 trillion dollars. This trend is also seen in Saudi Arabia, where cash use at POS locations decreased in 2023 compared to 2019 (Statista, 2023). Saudi consumers prefer cash transactions but are increasingly using electronic payments. The growing popularity of contactless retail transactions is driving this shift, which expands the payment card market. Despite this change, OSINT faces online security issues and threats that violate the consumers. Therefore, the following sections elaborate the OSINT within Saudi Arabia.

3.1 Tailoring OSINT discussion to the Saudi context

The evolution of open-source online payment applications in Saudi Arabia has sparked significant interest from both academic and industrial sectors, with the goal of addressing the Saudi market's unique challenges and preferences. Al-Mani (2020) provides a comprehensive overview of Saudi Arabia's digital payment landscape, emphasizing consumers' preference for cash on delivery. This preference highlights the critical need for more adaptable and secure online payment solutions that can serve the local consumer base. Al-mani's research identifies a gap in the adoption of digital payment methods, implying that open-source solutions could bridge the gap by providing customizable, secure, and user-friendly payment options.

Alflayyeh et al. (2020) investigate the barriers to the adoption of online payment systems, citing a lack of satisfactory payment options as a major impediment. According to their findings, the region's e-payment growth has been hampered by a lack of versatile and reliable payment gateways. The authors argue that open-source payment applications have the potential to introduce a broader range of payment options, increasing consumer trust and willingness to conduct online transactions. They believe that such platforms can provide the flexibility and security required to overcome existing barriers, resulting in a more inclusive digital marketplace in Saudi Arabia. In an analysis of consumer behavior toward online payments, Illankoon (2020) identifies trust as a critical factor influencing the adoption of digital payment options. The study emphasizes the importance of creating open-source payment applications that prioritize security features and user privacy in order to build consumer trust. According to Illankoon, the transparency and community-driven development model of open-source platforms can help to increase user trust, encouraging a shift to digital payments in the Saudi market.

Additionally, Rehman (2019) investigates the impact of security concerns on the adoption of online payment systems, observing that Saudi consumers are concerned about credit card fraud, privacy breaches, and a lack of effective after-sales support. Rehman's study advocates for the use of open-source payment solutions that provide strong security, comprehensive privacy policies, and dependable customer support. The author contends that addressing these concerns with open-source technology can significantly increase the appeal of online payments, facilitating a shift to digital commerce in Saudi Arabia.

According to Al-mani (2020), payment upon delivery is the most common and preferred method of transaction in Saudi Arabia. Alflayyeh et al. (2020) identified a lack of satisfactory payment options as a major concern for consumers when using online shopping services. According to Illankoon (2020), changes in consumer and business preferences are critical for the evolution of commercial practices across the region. Consumers' purchasing decisions are heavily influenced by the trust factor, as they prefer brands and products that they perceive to be reliable. The hesitation to embrace online shopping in Saudi Arabia stems from internet security concerns, such as credit card fraud, limited payment methods, concerns about privacy and confidentiality, a lack of robust regulations, and inadequate customer service after the purchase. These concerns highlight the difficulties associated with online shopping, which are primarily focused on security, privacy, and the credibility of online vendors (Rehman, 2019).

3.2 Identifying current security issues and challenges in Saudi Arabia

In the digital age, security, trust, and user experience concerns make global digital payment system adoption difficult (Bandar, 2023). Digital payment benefits and conveniences must be communicated to the public. Cybercrime has increased in Saudi Arabia over the past decade. IBM found that data breaches in Dubai and Saudi Arabia cost $6.93 million each, up 6% during the pandemic (Al Zoubi, 2023). The Saudi financial sector's rapid shift to online and mobile banking and poor operational strategies have made it more vulnerable to cyberattacks. Financial institutions must establish and follow a cybersecurity governance framework that incorporates blockchain and AI, as approved by their governing bodies, to mitigate these risks (Al Zoubi, 2023).

Regner and Riener (2017) and Garman et al. (2017) highlight the difficulty of balancing consumer data protection with commercial interests in online payment security and privacy. Khalilov and Levi (2018) discuss Bitcoin's anonymity versus transparency, while Goldfeder et al. (2017) discuss blockchain technologies' challenges to cryptocurrency privacy in the face of traditional tracking. This balance is difficult across legal and regulatory landscapes. Additionally, Rajendran et al. (2017) note that countries with underdeveloped digital infrastructure face different challenges in implementing secure, privacy-focused digital payment systems than those with advanced digital economies facing sophisticated cybersecurity threats and strict data protection regulations. Balgobin et al. (2016) examine how financial privacy concerns and payment instruments affect online shopping behavior depending on the country's payment infrastructure and digital trust. Schomakers et al. (2020) suggest privacy-preserving data markets to meet consumer data protection needs, which could boost online payments growth and innovation.

Therefore, the literature review shows the changing landscape of Saudi Arabian FinTech, including its challenges and opportunities. According to World Bank (2020) and GAS (2020), FinTech firms face regulatory and market challenges (Bandar, 2023), cybersecurity issues in financial services (Al Zoubi, 2023), and economic factors affecting FinTech development. McKinsey and Company (2016) and Abiliti (2023) research on digital banking adoption and blockchain technology highlight the sector's progress and growth potential. These findings suggest that research should expand beyond Saudi Arabia due to limitations like the narrow focus on social media usage (GMI, 2019). This complex mix of technology, regulation, and market forces drives FinTech growth in Saudi Arabia and elsewhere.

3.3 Discussing how AI can mitigate Saudi-specific security challenges in online systems

AI's transformative power is reshaping the global finance sector by increasing process efficiency, automating mundane tasks, and providing deeper insights into consumer behavior. In the Kingdom of Saudi Arabia (KSA), the financial industry has seen a significant increase in the use of AI technologies. Swain and Gochhait (2022) investigate the impact of AI on Middle Eastern financial institutions, with a focus on the integration of AI, blockchain technology, cloud computing, and data security in the context of Islamic banking. Their findings show that the use of cloud computing within Islamic banks increased significantly during the pandemic and has continued to grow. Cloud computing has helped to improve the security and efficiency of data management processes in these institutions, implying that cloud technology can have a significant impact on the structural and network integrity of Islamic banks.

In response to emerging AI trends, the Saudi Monetary Authority (SAMA) established a regulatory sandbox in 2018 to allow for the testing of innovative fintech products and services in a controlled environment. This initiative seeks to promote innovation and broaden AI applications in the financial sector. The COVID-19 pandemic highlighted the importance of AI and IoT in banking, prompting an increase in the use of robotics and AI to automate banking operations by urban financial institutions and fintech companies (SAMA, 2020). The findings from this period show a decrease in cybersecurity threats among banks using AI technologies, as well as improvements in regulatory compliance. Saudi banks are increasingly using AI to improve their service offerings, incorporating technologies like customer service chatbots and AI-powered fraud detection systems. For example, the Saudi National Bank (SNB) has implemented chatbots that are available around the clock to provide immediate assistance, as well as an AI-powered system that examines customer behavior and transaction patterns to detect fraud. AlQudah and Shaalan (2020) documented several instances of AI technology adoption in the Saudi financial sector, demonstrating the use of machine learning (ML) and natural language processing (NLP) to improve customer service, automate tasks, and improve data analysis in risk management.

However, the path to full AI integration in the financial sector faces challenges, such as a scarcity of skilled AI professionals and the need for comprehensive regulatory frameworks to guide ethical AI use, as highlighted by Al-Ghamdi and Al-Shehri (2020). According to Vijayakumar Bharathi et al. (2022), optimism about technology is critical in the willingness to use AI and robotic tools for financial investments, whereas reservations about technology can discourage their use. Overcoming these challenges, including a shortage of skilled personnel and the establishment of ethical guidelines, is critical to realizing AI's full potential in the Saudi financial market.

The Kingdom of Saudi Arabia has announced an ambitious agenda known as 'Saudi Vision 2030', which aims for a comprehensive digital overhaul that includes the adoption of groundbreaking technologies such as the Internet of Things (IoT), artificial intelligence (AI), the development of smart cities, and the use of blockchain technology (Gyan Consulting, 2023). During the recent Saudi Vision 2030 summit in Riyadh, a group of key stakeholders, including industry pioneers, scholarly figures, and officials from Saudi government-affiliated entities, discussed how blockchain technology could play a critical role in propelling the country's digital shift. The event, which lasted two days, was organized by the BSV International Association, a non-profit organization, and ThinkTech, a venture under the Saudi Ministry of Communications and Information Technology aimed at encouraging digital innovation.

Alasmary emphasizes the importance of Saudi Arabia developing and implementing blockchain-based solutions that are tailored to the country's specific digital transformation challenges. These blockchain solutions are viewed as critical accelerators for the digital transformation, with the potential to significantly improve the operational efficacy of both the government and commercial sectors. The use of blockchain technology is deemed critical for Saudi Arabia's digital transformation. This stems from the need for a wide range of distributed solutions across multiple applications. Identifying these applications is critical to the successful implementation of blockchain in the country's digital strategy.

4. Conclusion and Next Steps

After in-depth analysis of OSNIT applications and systems, the study concludes the findings:

4.1 Summarizing key points and insights.

Saudi Arabia's ambitions and challenges in digitalization across sectors are reflected in discussions about open-source intelligence (OSINT), digital transformation, and the integration of advanced technologies like AI and blockchain.

First, Vision 2030 calls for digital transformation using IoT, AI, smart cities, and blockchain to diversify and strengthen Saudi Arabia's economy. Industry leaders, government entities, and academic experts collaborate to explore blockchain's potential to enhance digital transformation in the kingdom, showing their commitment to such technologies. Customized blockchain solutions are needed to solve specific digital problems, highlighting the need for customized approaches in the country's technological evolution.

OSINT has benefits and drawbacks in security analysis. OSINT's cost-effectiveness, non-intrusiveness, and broad contextual understanding benefit national security and economics. However, ethical and legal issues like privacy and misinformation pose major obstacles. To ensure security and decision-making, technological reliance must be balanced with human analytical skills.

The dual-edged nature of information gathering is shown by historical and contemporary case studies of attackers using OSINT for targeted and untargeted attacks. It shows how OSINT-driven intelligence practices have changed over time, emphasizing the need for ethical and regulatory compliance in the digital age. Addressing OSINT's impact on online payment systems shows that the financial sector's shift toward digitalization, called 'paytech', requires vigilant cybersecurity. OSINT's monitoring and mitigation of cyber threats and financial fraud is crucial to banking trust and integrity.

Finally, Saudi Arabia's digital transformation and cybersecurity challenges and opportunities are unique. The kingdom's Vision 2030 initiative emphasizes a digital economy powered by AI and blockchain. The need for skilled AI professionals, ethical and regulatory frameworks, and the balance between privacy and security remain major issues. To achieve its digital goals, Saudi Arabia must focus on tailored solutions and strategic adoption of emerging technologies.

In the next chapter, we discuss how AI and blockchain can improve online payment system security. This exploration takes place as digital financial transactions become more common and cyber threats target them. AI and blockchain technology can detect and prevent unauthorized access, improve data integrity, and ensure transactional confidentiality, making them promising fraud fighters. In detail, the chapter will show how these technologies can be used together to create a robust security infrastructure that anticipates and mitigates cyber threats and adapts to digital fraud.

The chapter will also discuss the practicalities of integrating AI and blockchain into online payment frameworks. This covers regulatory compliance, scalability, and the need for a skilled workforce to manage and advance these technological solutions. Case studies and real-world examples will show how AI and blockchain can improve payment security, providing best practices and lessons learned. The chapter aims to explain how these technologies can revolutionize security measures to protect the future of online payments, aligning with global trends toward a more secure, efficient, and transparent digital economy.

References

[1] Yeboah-Ofori, A., & Brimicombe, A. (2018). Cyber intelligence and OSINT: Developing mitigation techniques against cybercrime threats on social media. *International Journal of Cyber-Security and Digital Forensics*, 7(1), 87–98.

[2] Agarwal, S., & Zhang, J. (2020). FinTech, lending and payment innovation: A review. *Asia-Pacific Journal of Financial Studies*, 49(3), 353–367.

[3] Alflayyeh, S., Haseebullah, S., & Belhaj, F. A. (2020). The impact of coronavirus (COVID-19) pandemic on retail business in Saudi Arabia: A theoretical review. *European Journal of Molecular & Clinical Medicine*, 7, 3547–3554.

[4] Al-Ghamdi, R. A., & Al-Shehri, M. T. (2020). The role of artificial intelligence in enhancing the quality of financial services: The case of Saudi Arabia. *Journal of Financial Services Marketing*, 25, 1–12.

[5] Al-mani, K. (2020). The Impact of E-commerce on the Development of Entrepreneurship in Saudi Arabia. *Journal of International Technology and Information Management*, 28, 28–62.

[6] Al-Qudah, D. A., Al-Zoubi, A. M., Castillo-Valdivieso, P. A., & Faris, H. (2020). Sentiment analysis for e-payment service providers using evolutionary extreme gradient boosting. *IEEE Access*, 8, 189930–189944. https://doi.org/10.1109/ACCESS.2020.3032216

[7] AlQudah, Z., & Shaalan, K. (2020). The adoption of artificial intelligence in the banking sector in Saudi Arabia: An exploratory study. *Journal of Financial Services Marketing*, 25, 145–156.

[8] McDonnell, A., Burbridge, H., & Sallum, Y. Z. (2017). Addressing Jihadi-Salafism in Yemen. *International Center for Religion and Diplomacy*.

[9] Ashwell, M. L. (2017). The digital transformation of intelligence analysis. *Journal of Financial Crime*, 24(3), 1–32.

[10] Bagnall, J. (1958). The Exploitation of Russian Scientific Literature for Intelligence Purposes. *Studies in Intelligence*, 2(3), 45–49.

[11] Balgobin, Y., Bounie, D., Quinn, M., & Waelbroeck, P. (2016). Payment instruments, financial privacy and online purchases. *Review of Network Economics*, 15(3), 147–168.

[12] Baskerville, R., Spagnoletti, P., & Kim, J. (2014). Incident-centered information security: Managing a strategic balance between prevention and response. *Information and Management*, 51(1), 138–151. https://doi.org/10.1016/J.IM.2013.11.004

[13] Bazzell, M. (2021). Open source intelligence techniques: Resources for searching and analyzing online information (8th ed.). Self-published.

[14] Becker, J. (1957). Comparative Survey of Soviet and US Access to Published Information. *Studies in Intelligence*, 1(4), 35–46.

[15] Belanche, D., Guinalíu, M., & Albás, P. (2022). Customer adoption of p2p mobile payment systems: The role of perceived risk. *Telematics and Informatics*, 72, 101851. https://doi.org/10.1016/J.TELE.2022.101851

[16] Benes, L. (2013). OSINT, New Technologies, Education: Expanding Opportunities and Threats. A New Paradigm. *Journal of Strategic Security*, 6(3), 22–37.

[17] Best, R., & Cumming, A. (2008). Open source intelligence: Issues for Congress. In T. M. Paulson (Ed.), *Intelligence Issues and Developments* (pp. 75–97). Nova Science Publishers.

[18] Block, L. (2023). The long history of OSINT. *Journal of Intelligence History*, 1–15.

[19] Branco, E. P. (2017). Cyberthreat Discovery in Open Source Intelligence Using Deep Learning Techniques (Doctoral dissertation). Universidade de Lisboa, Portugal.

[20] BuiltWith. (n.d.). https://builtwith.com/
Capgemini. (2021). World payments report 2021. Retrieved from https://www.capgemini.com/es-es/news/world-payments-report-de-capgemini/

[21] Croom, H. (1969). The Exploitation of Foreign Open Sources. *Studies in Intelligence*, 13, 129–130.

[22] Crowe, S., Pournouri, S., & Ibbotson, G. (2021). Use of classification techniques to predict targets of cyber attacks for improving cyber situational awareness during the COVID-19 pandemic. https://doi.org/10.1007/978-3-Wells, D. (2016). Taking stock of subjective narratives surrounding modern OSINT. In *Open Source Intelligence Investigation* (pp. 57–65).

[23] Ding, B. T. (2017). Promoting the transformation of intelligence agencies and strengthening strategic intelligence services-Reflections on the development of science and technology intelligence agencies under the perspective of innovation strategy. *Intelligence Theory and Practice*, 40(5), 15–18. https://doi.org/10.16353/j.cnki.1000-7490.2017.05.003

[24] Donovan, W. (1946). Intelligence. *Life Magazine*, 30(September), 108–121.

[25] Dulles, A. (1963). *The Craft of Intelligence*. Boulder, CO: Westview Press.

[26] Dunn, A. (2016). Responsible data leaks and whistleblowing. Retrieved June 4, 2021, from https://www.theengineroom.org/responsible-data-leaks-and-whistleblowing/

[27] Edwards, L., & Urquhart, L. (2016). Privacy in public spaces: What expectations of privacy do we have in social media intelligence? *International Journal of Law and Information Technology*, 24(3), 279–310.

[28] Eijkman, Q., & Weggemans, D. (2012). Open source intelligence and privacy dilemmas: Is it time to reassess state accountability. *Security & Human Rights*, 23(1), 285–296.

[29] Engelen, D. (1999). *De Militaire Inlichtingendienst 1914–2000*.

[30] Evangelista, J. R. G., Sassi, R. J., Romero, M., & Napolitano, D. (2020). Systematic literature review to investigate the application of open source intelligence (OSINT) with artificial intelligence. *Journal of Applied Security Research*, 16(3), 345–369.

[31] Expert.ai. (2017). Advantages and disadvantages of open source intelligence. Retrieved March 22, 2021, from https://www.expert.ai/blog/advantages-disadvantages-open-source-intelligence/

[32] Alkhudhayr, F., Alfarraj, S., Aljameeli, B., & Elkhdiri, S. (2019). Information security: A review of information security issues and techniques. In *Proceedings of the 2019 2nd International Conference on Computer Applications & Information Security (ICCAIS)* (pp. 1–6). Riyadh, Saudi Arabia.

[33] Tabatabaei, F., & Wells, D. (2016). OSINT in the context of cybersecurity. In B. Akhgar, P. S. Bayerl, & F. Sampson (Eds.), *Open Source Intelligence Investigation: From Strategy to Implementation* (pp. 213–231). Springer.

[34] Fabius, H. (1921). De Inlichtingendienst bij den Generalen Staf. *Militaire Spectator*, 90(8), 402.

[35] Foley, R. (2005). Easy Target or Invincible Enemy? German Intelligence Assessments of France Before the Great War. *Journal of Intelligence History*, 5(2), 1–24.

[36] Forsvaret. (2021). *Forsvarets etterretningsdoktrine* [Tech. rep.]. Retrieved from https://www.etterretningstjenesten.no/publikasjoner/etterretningsdoktrinen/Etterretningsdoktrine_2021_Web_LoRes_02.pdf/_/attachment/inline/633b7840-43de-42af-bb89-243d81076208:edd1367bd55a434b4489162637336d7d632d42a0/Etterretningsdoktrine_2021%20-%20Web_LoRes%2002%20(PROD).pdf

[37] Fuhlhage, M. (2019). *Yankee Reporters and Southern Secrets: Journalism, Open Source Intelligence and the Coming of the Civil War*. Peter Lang.

[38] Garman, C., Green, M., & Miers, I. (2017). Accountable privacy for decentralized anonymous payments. In *Financial Cryptography and Data Security: 20th International Conference, FC 2016, Christ Church, Barbados, February 22–26, 2016, Revised Selected Papers 20* (pp. 81-98). Springer Berlin Heidelberg.

[39] General Authority for Statistics (GAS). (2020). Fixed and mobile broadband services and Internet penetration rate. Retrieved August 15, 2020, from https://www.stats.gov.sa/en/6390

[40] Gibson, H. (2016). Acquisition and preparation of data for OSINT investigations. https://doi.org/10.1007/978-3-319-47671-16

[41] Gibson, S. D. (2014). Exploring the role and value of open source intelligence. In C. Hobbs et al. (Eds.), *Open Source Intelligence in the Twenty-First Century: New Approaches and Opportunities* (pp. 9-23). Hampshire: Palgrave Macmillan.

[42] Global Media Insight (GMI). (2019). Saudi Arabia social media statistics 2019 (Infographics) - GMI Blog. Retrieved September 15, 2020, from https://www.globalmediainsight.com/blog/saudi-arabia-social-media-statistics/