UNIVERSIDAD DE MURCIA

ESCUELA INTERNACIONAL DE DOCTORADO

TESIS DOCTORAL

Opportunities, Risks and Applications of Open Source Intelligence in Cybersecurity and Cyberdefence

Oportunidades, Riesgos y Aplicaciones de la Inteligencia de Fuentes Abiertas en la Ciberseguridad y la Ciberdefensa

D. JAVIER PASTOR GALINDO

2023

UNIVERSIDAD DE MURCIA

ESCUELA INTERNACIONAL DE DOCTORADO

TESIS DOCTORAL

Opportunities, Risks and Applications of Open Source Intelligence in Cybersecurity and Cyberdefence

Oportunidades, Riesgos y Aplicaciones de la Inteligencia de Fuentes Abiertas en la Ciberseguridad y la Ciberdefensa

Autor: Javier Pastor Galindo

Directores: Dr. Félix Gómez Mármol

Dr. Gregorio Martínez Pérez

DECLARACIÓN DE AUTORÍA Y ORIGINALIDAD DE LA TESIS PRESENTADA EN MODALIDAD DE COMPENDIO O ARTÍCULOS PARA OBTENER EL TÍTULO DE DOCTOR

Aprobado por la Comisión General de Doctorado el 19-10-2022

D./Dña. Javier Pastor Galindo

doctorando del Programa de Doctorado en

Informática

de la Escuela Internacional de Doctorado de la Universidad Murcia, como autor/a de la tesis presentada para la obtención del título de Doctor y titulada:

Opportunities, Risks and Applications of Open Source Intelligence in Cybersecurity and Cyberdefence

Oportunidades, Riesgos y Aplicaciones de la Inteligencia de Fuentes Abiertas en la Ciberseguridad y la Ciberdefensa

y dirigida por,

D./Dña. Félix Gómez Mármol
D./Dña. Gregorio Martínez Pérez
D./Dña.

DECLARO QUE:

La tesis es una obra original que no infringe los derechos de propiedad intelectual ni los derechos de propiedad industrial u otros, de acuerdo con el ordenamiento jurídico vigente, en particular, la Ley de Propiedad Intelectual (R.D. legislativo 1/1996, de 12 de abril, por el que se aprueba el texto refundido de la Ley de Propiedad Intelectual, modificado por la Ley 2/2019, de 1 de marzo, regularizando, aclarando y armonizando las disposiciones legales vigentes sobre la materia), en particular, las disposiciones referidas al derecho de cita, cuando se han utilizado sus resultados o publicaciones.

Además, al haber sido autorizada como compendio de publicaciones o, tal y como prevé el artículo 29.8 del reglamento, cuenta con:

- *La aceptación por escrito de los coautores de las publicaciones de que el doctorando las presente como parte de la tesis.*
- *En su caso, la renuncia por escrito de los coautores no doctores de dichos trabajos a presentarlos como parte de otras tesis doctorales en la Universidad de Murcia o en cualquier otra universidad.*

Del mismo modo, asumo ante la Universidad cualquier responsabilidad que pudiera derivarse de la autoría o falta de originalidad del contenido de la tesis presentada, en caso de plagio, de conformidad con el ordenamiento jurídico vigente.

En Murcia, a 11 de septiembre de 2023

Fdo.: Javier Pastor Galindo

Acknowledgements

Here ends a fabulous personal, academic and professional experience. To all those people who have been part of my life since I was born and who have contributed to being the person and professional I am today: thank you very much for your support, experiences and lessons that, in some way, are present in this PhD thesis.

Agradecimientos

Aquí finaliza una fabulosa experiencia personal, académica y profesional. A todas aquellas personas que han formado parte de mi vida desde que nací y que han contribuido a ser la persona y el profesional que soy hoy en día: muchas gracias por vuestro acompañamiento, experiencias y lecciones que, de alguna forma, están presentes en esta tesis doctoral.

Abstract

The intelligence gathering has transformed significantly in the digital age. A qualitative leap within this domain is the sophistication of Open Source Intelligence (OSINT), a paradigm that exploits publicly available information for planned and strategical objectives. Although it might seem contemporary, OSINT has an historical connection to military and diplomatic strategies, like in the World War II (1939-1945) and the Cuban Missile Crisis (1962). Nevertheless, the proliferation of information systems and the Internet has contributed new opportunities for OSINT, as it now encompasses a broad spectrum of digital sources such as social media, online databases, blogs, academic journals and other web-based resources. The resulting extensive data pool, widely known as Big Data, presents an unprecedented potential for scientific exploration and technological progress.

Current advancements in algorithms and computing power have paved the way for Artificial Intelligence (AI) as a key technology for sophisticated processing and analysis of open-source data, providing natural language processing, image and video recognition, classification tasks, identification of complex patterns, prediction capabilities or anomaly detection, among other. The combination of all these AI capabilities makes it possible to generate a new-age OSINT. Additionally, representative use cases, the different nature of the information and the variety of purposes demonstrate the potential of this paradigm, including scientists using weather databases and academic literature to track long-term global climate patterns, market researchers assessing consumer sentiments towards specific brands or products using social media and user feedback platforms, as well as healthcare researchers leveraging medical journals and patient forums for comprehensive epidemiological studies. Furthermore, OSINT is increasingly employed in law enforcement, intelligence agencies, finance, journalism, and human resources, among others.

The importance of OSINT has become even more profound in cybersecurity, a multidisciplinary field that encompasses measures and processes to safeguard digital systems and data, due to the capacity of this type of intelligence to track different types of devices and data sources, analyze feeds of information of different natures, and search for patterns and phenomena invisible to the human eye. Considering the increasing cyber threats in the digital landscape, cybersecurity analysts leverage OSINT to collect documents, media, posts, users or news residing on the public Internet to further characterize the online ecosystem, identify hostile actors and analyze suspicious behaviors. OSINT is also useful for surveillance of exposed servers, computers and Internet of Things (IoT) devices, spotting misconfigurations, data breaches, and identifying zero-days exploitable by any user connected to the network.

This set of features is pivotal, particularly for cybersecurity efforts to understand the evolving risk reality and provide Cyber Threat Intelligence (CTI).

When integrated into cyberdefence strategies, those operations planned to protect critical infrastructure, preserve state assets and support military missions, OSINT serves as a valuable support for real-time threat detection and mitigation, tracking tactics, techniques and procedures of cyberoperations, and pinpointing vulnerabilities in military tactical networks before adversaries exploit them. In national security contexts, OSINT offers key insights into potential threats from foreign entities and non-state actors, supporting policy decisions, law enforcement and diplomatic strategies. The analysis of open-source data, like social media and online news, can unmask potential terrorist activities, civil unrest or new adversary technologies. In military operations, OSINT enhances situational awareness and assists in identifying enemy activities and capabilities, including satellite imagery and social media. As a result, OSINT is instrumental in shielding society from hybrid threats, influence operations and foreign interference by identifying and combating disinformation campaigns, monitoring extremist groups and detecting attempts at public opinion manipulation. Thus, it plays a crucial role in economic security, upholding democratic values and freedom.

The main purpose of this PhD thesis is to motivate, justify and demonstrate OSINT as a reference paradigm that should complement the present and future of both civilian cybersecurity solutions and cyberdefence national and international strategies. We examine the technical opportunities, security and privacy risks, and practical applications of OSINT in cybersecurity activities and cyberdefence capabilities. In particular, our research explores the power of OSINT to enrich security and defence processes, the implications of its misuse for organizations and end users, and the employment Social Media Intelligence (SOCMINT) and Dark Web Intelligence (DARKINT) to protect society and countries against threats. Therefore, four research objectives are established for this dissertation.

The first objective of this PhD thesis concerns the critical examination and evaluation of the state of OSINT under the current digital revolution and the growth of Big Data and Artificial Intelligence (AI). This objective entails crafting a well-structured analysis of the OSINT landscape, techniques and tools, highlighting its strengths and weaknesses. Moreover, we suggest potential ways where OSINT could enhance cybersecurity alongside addressing implementation barriers. Nevertheless, some security and privacy concerns arise.

The second objective of this PhD thesis is geared toward categorizing security and privacy risks associated with OSINT. Despite the numerous benefits brought by OSINT addressed in the first objective, it is crucial to recognize that they can be exploited by cybercriminals who leverage open data to cause harm to individuals and organizations. This objective thus entails an in-depth exploration of potential threats and misuse of public data, with a particular focus on the role of AI in fueling sophisticated cyberattacks. Considering these implications, OSINT should be developed in a responsible manner for cybersecurity and cyberdefence purposes.

The third objective of this PhD thesis focuses on leveraging the OSINT advantages in practical use cases by designing and implementing OSINT techniques to counter online threats, particularly those stemming from social networks. Given the publicly available information accessible in these online spaces, OSINT, specifically SOCMINT, has become an essential resource for gathering intelligence and spotting threats. This objective aims to establish and execute OSINT methodologies capable of analyzing social media data, identifying automated accounts known as social bots, and assessing their behaviour and impact in the information environment. The effectiveness of these methodologies will be evaluated through practical case studies conducted in critical electoral contexts, contributing to the understanding of these threats to national and social integrity.

Last but not least, the fourth objective of this PhD thesis embarks on the exploration of the Dark web through the lens of OSINT. Traditionally, the Dark web remains relatively unexplored in the literature of OSINT, so it is worth extending it from Surface web use cases to this anonymous part of the Internet, which is vital in cybersecurity and cyberdefence, often constituting the hub of illicit activities. This objective aims to identify and evaluate existing techniques for discovering Tor onion addresses, those that enable the access to Dark sites hosted in the Tor network, which could facilitate the monitoring of underground sites on the Dark web, thereby bolstering DARKINT capabilities.

To achieve these appealing and challenging objectives, we follow a methodology with clearly ordered steps. Firstly, a rigorous review of the existing literature addresses the first objective, focusing on the state of OSINT, its applications, and its challenges. This serves to identify existing research gaps and establish a solid foundation for an updated view of OSINT. Consequently, a critical part of the methodology involves assessing the potential security and privacy risks that could emerge from the misuse of OSINT by cybercriminals, including using AI to enhance cyberattacks, fulfilling the second objective. Thirdly, to provide practical evidence regarding the power of OSINT, we work in a Twitter use case in the context of the 2019 Spanish general election, designing and implementing OSINT methods to understand the behaviour and impact of automated accounts. Through AI and social media analysis, this process aims to detect social bots in the wild for further behavior characterization and impact assessment, thus covering the third objective. The last effort is dedicated to the Dark web, reviewing different works in the literature related to the Tor network to identify and characterize the techniques for gathering onion addresses essential for accessing anonymous websites, completing the fourth objective. This comprehensive methodology led to the publication of five remarkable scientific papers in peer-reviewed journals, collectively forming the basis of this PhD thesis. Notably, the PhD candidate served as the primary and corresponding author for every and each of the aforementioned articles, inserted in the corpus of this document.

As a result of this thesis, our exploration of OSINT highlights its critical role in a broad range of sectors such as marketing, political campaigning, disaster management, human resources recruitment and journalism. Furthermore, the ability to monitor threats in social media via SOCMINT and detect cybercrime on the Dark web through DARKINT is also noteworthy. OSINT tools can spot illicit activities, recover suspicious traces and significantly aid in cybersecurity and cyberdefence by facilitating activities such as footprinting, forensic analysis, crime attribution, and social engineering prevention. However, challenges such as data complexity, handling unstructured information and dealing with misinformation pose noteworthy obstacles for analysts. Additional complications arise due to the reliability of data sources and the need to comply with ethical and legal frameworks, such as the European General Data Protection Regulation (GDPR). Nonetheless, the value and contribution of OSINT in the various mentioned sectors remain undeniable.

Secondly, we identify and characterize significant security and privacy risks associated with OSINT, particularly those arising from the misuse of Personally Identifiable Information (PII) found in open sources. Our research shows that cybercriminals can exploit PII to launch OSINT-based attacks, classified into three primary threat dimensions: deception, blackmail, and expansion. In deception-based attacks, open data is manipulated to mislead victims or systems, such as in social engineering attacks, phishing, spear-phishing or impersonation attacks. In blackmail, open data is used to coerce victims, typical of extortion attacks. Then, expansion-based attacks employ open data to gather additional sensitive information, broadening the potential attack surface. In all these categories, advanced analytics can enhance the severity of threats by facilitating activities such as password cracking in brute-force attacks, creating deep-fake videos for impersonation attacks, and automating the collection of personal details for profiling attacks. This thesis proposes some recommendations for users and service providers to combat these threats, including measures to reduce personal data exposure, implement restrictive privacy settings and prioritize privacy in the early stages of project design.

Regarding the third objective of practical nature, the potential of OSINT for defensive purposes is investigated by analyzing the behaviour of social bots in Twitter during the 2019 Spanish general election of November 10th, 2019. The resulting dataset comprised over 5.8 million tweets, revealing that social bots accounted for about 5% of traffic volumes. A detailed examination of bot interactions revealed that the bots frequently retweeted human content, possibly aiming for virality. Bots were further classified with AI according to their political alignment, revealing an increased bot activity in those days with important national events. To further understand the influence of bots, a second experimental use case in the same context is designed. With an augmented dataset, the retweet network was inspected with a data-driven framework incorporating statistical, network, robustness, influence, structure, temporal, content, and virality analysis. Experimental results on the extended version of the previous elections dataset, with 7,9M retweets and 1,3M associated users, unveils that social bots seem to alter the social network but failed to achieve substantial influence. Notably, semi-automated bots had a more significant impact than fully automated ones.

In the extension to the Dark web, our investigation into the techniques for harvesting Tor onion addresses identifies five main methods, namely: repositories, Tor crawling, onion search engines, relay injection, and generic search engines, each having unique strengths and weaknesses. The review of methods reveals that Tor crawling and repositories are the most commonly used collection techniques. However, the effectiveness varied among techniques, with relay injection, repositories, and Tor crawling yielding the highest number of onion addresses discovered daily. We show that there is a lack of tailored onion-gathering techniques, bias in collection procedures, a narrow variety of discovered onion services, and limited search spaces.

As a result, a series of recommendations are proposed for improving onion address discovery: amplify the combination of techniques, employing both the Surface web and Dark web for searching, implementing a continuous gathering process in fresh data sources due to the dynamic nature of onion services, guiding gathering strategically rather than relying on brute-force methods, leveraging alternative search paths beyond crawling by exploiting correlations and pivoting through the cyberspace, and evaluating gathering effectiveness and representativeness to improve the outcomes over time.

As main conclusions, this PhD thesis underlines the immense potential of OSINT as a strategic tool for problem-solving across many sectors. In the age of Big Data and AI, OSINT aids in deriving insights from vast, complex information sources such as social networks, online documents, web pages and even the corners of the Deep and Dark web. However, an effective OSINT application requires more than data analysis and it calls for strategic planning and understanding of the specific context or sector being studied. The choice of technologies, analytical methods, and visualizations must be justified, and scalable and efficient designs are indispensable.

The practical use cases developed in this PhD thesis evidence that the incorporation of OSINT into cybersecurity and cyberdefence is increasingly valuable. SOCMINT helps to characterize social bots in disinformation contexts, which in conjunction with AI returns sophisticated results, such as the sentiment of organic content generated in social media or the political alignment of automated accounts. On the other hand, the DARKINT enables the gathering of the links of anonymous Dark web sites.

Nevertheless, a multidisciplinary approach would significantly enhance the effectiveness of OSINT activities. While the role of computer science, information technology, and data science is undeniable, the input from social sciences such as sociology and psychology can offer indispensable insights into human behavior, social trends and cultural contexts. The adoption of ethical practices is also important, considering the potential adverse outcomes of using OSINT. Furthermore, legal professionals must collaborate with computer scientists to design systems that align with laws and standards.

Moreover, we also expose that the development of OSINT carries its share of risks. Open data can be exploited for social engineering, spear-phishing, profiling, deception, blackmail, spreading disinformation or launching personalized attacks. Hence, implementing adequate security measures of secure data storage, controlled access and regular audits is crucial to augment our protection levels.

Finally, this dissertation paves the way for some promising future directions in the field of OSINT research. Future research could study the disinformation phenomena in detail, assessing the effects of different manipulative attacks, evaluating potential countermeasures to combat them, and exploring the use of Generative Artificial Intelligence (GenAI) for agent-based realistic simulations. Another appealing direction is the research on cyber situational awareness from the information and cognitive perspective. It could include developing a framework with collection, fusion, analysis and visualization of information in the cyberspace to provide a real-time clear view for decision-making, early detection and effective reactions. This exposes technical challenges related to information visualization, data flow tracking, malicious content identification, and the evaluation of cognitive, emotional and vulnerability status of users. The last proposal of future work of this PhD thesis is the exploration of the ethical and legal limits of OSINT, which could enable the collaboration with law experts to interpret compliance frameworks, like GDP, and consider ethical guidelines for paradigm fueled with public data.

Resumen

La recolección de inteligencia ha sufrido una transformación significativa durante la era digital. En particular, podemos destacar el auge y sofisticicación de la Inteligencia de Fuentes Abiertas (OSINT, por sus siglas en inglés de *Open Source Intelligence*), paradigma que recolecta y analiza la información públicamente disponible para objetivos estratégicos y planificados. Aunque pueda parecer contemporáneo, el OSINT ya tenía originalmente protagonismo en estrategias militares y diplomáticas, por ejemplo, durante la Segunda Guerra Mundial (1939-1945) o en la Crisis de los Misiles de Cuba (1962). Sin embargo, la proliferación de los sistemas de información e Internet ha generado nuevas oportunidades para este tipo de inteligencia, abarcando un creciente espectro de recursos tales como las redes sociales, bases de datos online, blogs, revistas académicas u otros recursos web. La extensa cantidad de datos resultante, conocido ampliamente como Big Data, presenta un potencial sin precedentes para la exploración científica y el progreso tecnológico.

Los avances actuales en algoritmos y potencia de cálculo han propiciado el desarrollo de la Inteligencia Artificial (IA), tecnología clave para el procesamiento y análisis de datos, proporcionando procesamiento del lenguaje natural (NLP, por sus siglas en inglés de *Natural Language Processing*), reconocimiento de imágenes y videos, tareas de clasificación, identificación de patrones complejos, capacidades de predicción o detección de anomalías, entre otros. La combinación de todas estas capacidades de IA posibilita una OSINT de nueva generación. Además, los diferentes casos de uso, la diversa naturaleza de la información y la variedad de propósitos demuestran el potencial de este paradigma, incluyendo científicos que utilizan bases de datos meteorológicas y literatura académica para rastrear patrones climáticos globales a largo plazo, investigadores de mercado evaluando las percepciones de los consumidores hacia marcas o productos específicos utilizando redes sociales o plataformas de comentarios de usuarios, así como trabajadores de la salud que aprovechan revistas médicas y foros de pacientes para estudios epidemiológicos integrales. Además, el OSINT es cada vez más empleado en los cuerpos de seguridad, agencias de inteligencia, finanzas, periodismo y recursos humanos, entre otros.

La importancia de OSINT es muy evidente en el campo de la ciberseguridad, área multidisciplinar que abarca medidas y procesos para proteger sistemas digitales y datos, debido a la capacidad que tiene este tipo de inteligencia para rastrear diferentes tipos de dispositivos y fuentes de datos, analizar flujos de información, o buscar patrones y fenómenos invisibles para el ojo humano. Considerando el aumento de ciberataques en la actualidad, los analistas de ciberseguridad utilizan OSINT para recopilar documentos, medios, publicaciones, usuarios o noticias presentes en

Internet para caracterizar el entorno online digital, identificar actores hostiles y analizar comportamientos sospechosos. El OSINT también es útil para la vigilancia de servidores expuestos, ordenadores y dispositivos del Internet de las Cosas (IoT, por sus siglas en inglés de *Internet of Things*), detectando configuraciones incorrectas, brechas de datos y vulnerabilidades explotables por cualquier usuario hostil conectado a la red. Además, este conjunto de capacidades permiten analizar el riesgo y proveer de inteligencia de ciberamenazas (CTI, por sus siglas en inglés *Cyber Threat Intelligence*).

Cuando se integra en estrategias de ciberdefensa, aquellas operaciones planificadas para proteger infraestructuras críticas, preservar activos estatales y apoyar misiones militares, el OSINT es una herramienta potente para la detección y mitigación de amenazas en tiempo real, rastreando tácticas, técnicas y procedimientos de ciberoperaciones, y señalando vulnerabilidades en redes tácticas militares antes de que los adversarios las exploten. En contextos de seguridad nacional, el OSINT puede revelar posibles amenazas extranjeras y de actores no estatales, y apoyar a la toma de decisiones y aplicación de la ley. El análisis de la información públicamente accesible, como la existente en redes sociales y noticias en línea, puede desenmascarar posibles actividades terroristas, riesgos civiles o nuevas tecnologías enemigas. En operaciones militares, el OSINT mejora la conciencia situacional (CSA, por sus siglas en inglés *Cyber Situational Awareness*) y ayuda a identificar actividades y capacidades enemigas, incluyendo imágenes satelitales y redes sociales. Como resultado, el OSINT es estratégico para proteger a la sociedad de las amenazas híbridas, operaciones de influencia e interferencias extranjeras, pudiendo identificar y combatir campañas de desinformación, monitorear grupos extremistas y detectar intentos de manipulación de la opinión pública. Por lo tanto, juega un papel crucial en la seguridad económica, defendiendo así valores democráticos y la libertad.

El cometido principal de esta tesis doctoral es motivar, justificar y demostrar que OSINT es un paradigma de referencia para complementar el presente y futuro de las soluciones de ciberseguridad civiles y las estrategias de ciberdefensa nacionales e internacionales. Examinamos las oportunidades técnicas, los riesgos de seguridad y privacidad, y las aplicaciones prácticas de OSINT en actividades de ciberseguridad y capacidades de ciberdefensa. En particular, nuestra investigación explora el poder de OSINT para enriquecer procesos de seguridad y defensa, las implicaciones de su mal uso para organizaciones y usuarios finales, y el empleo de Inteligencia de Redes Sociales (SOCMINT, por sus siglas en inglés *Social Media Intelligence*) e Inteligencia de la Web Oscura (DARKINT, por sus siglas en inglés *Dark Web Intelligence*) para proteger a la sociedad y a los países contra amenazas. Por lo tanto, se establecen cuatro objetivos de investigación para esta disertación.

El primer objetivo de esta tesis doctoral es examinar y evaluar el estado de OSINT en el contexto actual de revolución digital y crecimiento del Big Data y la IA. Este objetivo implica crear un análisis bien estructurado del paradigma, identificando sus técnicas, herramientas, fortalezas y debilidades. Además, sugerimos aproximaciones en las que OSINT podría superar las barreras de implementación y mejorar la ciberseguridad. Sin embargo, surgen algunas preocupaciones de seguridad y privacidad.

El segundo objetivo de esta tesis doctoral está orientado a categorizar los riesgos de seguridad y privacidad asociados con OSINT. A pesar de los numerosos beneficios abordados en el primer objetivo, es crucial reconocer que pueden ser explotados por ciberdelincuentes que aprovechan los datos abiertos para causar daño a individuos y organizaciones. Este objetivo, por lo tanto, implica una exploración profunda de las posibles amenazas y mal uso de datos públicos, con un enfoque particular en el papel de la IA en alimentar ciberataques sofisticados. Considerando estas implicaciones, OSINT debere desarrollarse de una manera responsable para propósitos de ciberseguridad y ciberdefensa.

El tercer objetivo de esta tesis doctoral se centra en aprovechar las ventajas de OSINT en casos de uso prácticos, diseñando e implementando técnicas de OSINT para contrarrestar amenazas online, particularmente aquellas provenientes de las redes sociales. Dada la información públicamente accessible, el OSINT, y específicamente el SOCMINT, se han convertido en un recurso esencial para recopilar inteligencia y detectar amenazas. En particular, este objetivo busca establecer y ejecutar metodologías de OSINT capaces de analizar datos de redes sociales, identificar cuentas automatizadas conocidas como bots sociales y evaluar su comportamiento e impacto en el entorno digital. La efectividad de estas metodologías se evaluará a través de estudios de caso prácticos llevados a cabo en contextos electorales, contribuyendo a la comprensión de estas amenazas en defensa de la integridad social y nacional.

Por último, pero no menos importante, el cuarto objetivo de esta tesis doctoral es explorar la Dark web desde la perspectiva de OSINT. Tradicionalmente, la Dark web no es estudiada en la literatura por su naturaleza anónima, por lo que es interés de esta tesis doctoral adentrarse en ella. Además, las redes anónimas que componen la Dark web tienen implicaciones en ciberseguridad y ciberdefensa, constituyendo a menudo el centro de actividades ilícitas. En particular, en este objetivo buscamos identificar y evaluar técnicas existentes para descubrir las direcciones aleatorias de las páginas alojadas en la red Tor (actualmente conocidos como "*onion services*"), lo que podría facilitar la monitorización de sitios maliciosos en la Dark web, fortaleciendo así las capacidades DARKINT.

Para alcanzar estos objetivos seguimos una metodología con pasos claramente ordenados. En primer lugar, para abordar el primer objetivo, realizamos una revisión rigurosa de la literatura existente, centrándonos en el estado de OSINT, sus aplicaciones y sus desafíos. Esto sirve para identificar oportunidades de investigación existentes y establecer una sólida base de visión actualizada de OSINT. A continuación, en relación con el segundo objetivo, evaluamos los posibles riesgos de seguridad y privacidad que podrían surgir del mal uso de OSINT por parte de ciberdelincuentes, incluido el uso de IA para mejorar los ciberataques. En tercer lugar, para proporcionar evidencia práctica sobre el poder de OSINT, trabajamos en un caso de uso de Twitter en el contexto de las elecciones generales españolas de 2019, diseñando e implementando métodos de OSINT para entender el comportamiento y el impacto de las cuentas automatizadas. A través de la IA y el análisis de redes sociales, buscamos detectar bots sociales en Twitter para una posterior caracterización del comportamiento y evaluación del impacto, cubriendo así el tercer objetivo. Luego, dedicamos otra parte de la tesis al cuarto objetivo relacionado con la Dark web, revisando diferentes trabajos en la literatura de la red Tor para identificar y caracterizar las técnicas para recopilar direcciones onion, esenciales para acceder a sitios web anónimos de la red Tor. Esta metodología llevó a la publicación de cinco destacados artículos científicos en revistas revisadas por pares, formando colectivamente la base de esta tesis doctoral. El autor de esta tesis doctoral es, a su vez, autor principal para cada uno de los cinco artículos mencionados anteriormente, disponibles en el cuerpo de este documento.

A partir de los pasos metodológicos que cubren cada uno de los objetivos obtenemos los resultados de esta tesis. La exploración de la literatura destaca el importante rol de OSINT en una amplia gama de sectores como marketing, campañas políticas, gestión de desastres, reclutamiento de recursos humanos y periodismo. Además, se motiva la capacidad de monitorear amenazas en redes sociales a través de SOCMINT y detectar ciberdelitos en la web oscura mediante DARKINT. Las herramientas de OSINT pueden detectar actividades ilícitas, recuperar rastros sospechosos y ayudar significativamente en ciberseguridad y ciberdefensa, siendo empleado en footprinting, análisis forense, atribución de crímenes y prevención de ingeniería social. También se identifican desafíos para los analistas, como la complejidad de los datos, el manejo de información no estructurada y lidiar con la desinformación representan obstáculos notables. Se presentan obstáculos adicionales debido a la fiabilidad de las fuentes de datos y la necesidad de cumplir con marcos éticos y legales, como el Reglamento General de Protección de Datos (RGPD) de Europa. En cualquier caso, el valor y la contribución de OSINT en los diversos sectores mencionados siguen siendo innegables.

En cuanto a los riesgos de seguridad y privacidad asociados con OSINT, particularmente aquellos que surgen del mal uso de la información de identificación personal (PII, por sus siglas en inglés *Personally Identifiable Information*) encontrada en fuentes abiertas. Nuestra investigación muestra que los ciberdelincuentes pueden explotar la PII para lanzar ataques clasificados en tres dimensiones: engaño, chantaje y expansión. En los ataques basados en engaño, como la ingeniería social, phishing, spear-phishing o suplantación de identidad, los datos se emplean para manipular a las víctimas o sistemas. En el chantaje, los datos abiertos se utilizan para coaccionar a las víctimas y propiciar amenazas de extorsión. Finalmente, los ataques basados en expansión emplean datos abiertos para recopilar información sensible adicional, ampliando la superficie de ataque potencial. En todas estas categorías, la IA puede intensificar la gravedad de las amenazas facilitando actividades como el cracking de contraseñas en ataques de fuerza bruta, creando vídeos deepfake para ataques de suplantación de identidad y automatizando la recopilación de detalles personales para ataques de perfilado. Esta tesis propone recomendaciones para usuarios y proveedores de servicios para combatir estas amenazas, incluyendo medidas para reducir la exposición de datos personales, implementar configuraciones de privacidad restrictivas y priorizar la privacidad en las etapas tempranas del diseño de proyectos.

En relación al tercer objectivo, que tiene un prisma práctico, se investiga el potencial de OSINT en el análisis del comportamiento de bots automatizados en Twitter durante las elecciones generales españolas del 10 de noviembre de 2019. El conjunto de datos recolectado resultante tenía más de 5.8 millones de tweets, revelando que los bots representaban alrededor del 5% del volumen de tráfico. Un examen detallado de las interacciones de los bots reveló que frecuentemente retweeteaban contenido humano, posiblemente buscando viralidad. Los bots se clasificaron con IA según su alineación política, observando el aumento de actividad bot aquellos días en los que había eventos nacionales importantes. Para entender mejor la influencia de los bots, se diseñó un segundo caso de uso experimental en el mismo contexto. Con un conjunto de datos ampliado, se inspeccionó la red de retweets a través de un conjunto de análisis estadísticos, de red, de robustez, de influencia, de estructura, temporal, de contenido y de viralidad. Los resultados experimentales en la versión extendida del conjunto de datos de elecciones anteriores, con 7,9 millones de retweets y 1,3 millones de usuarios asociados, revelan que los bots sociales parecen alterar la red social pero no lograron una influencia sustancial. En particular, los bots semi-automatizados tuvieron un impacto más significativo en las dinámicas de Twitter que los completamente automatizados.

En cuanto al cuarto objetivo en torno a la Dark web, nuestra investigación sobre las técnicas para recolectar direcciones Tor onion identifica cinco métodos principales: repositorios, crawling en Tor, motores de búsqueda especializados, inyección de relays y motores de búsqueda genéricos, cada uno con puntos fuertes y débiles. La revisión de estos revela que el crawling en Tor y los repositorios son las técnicas de recolección más comúnmente utilizadas. Sin embargo, la eficacia varía entre las técnicas, siendo la inyección de relay, los repositorios y el crawling en Tor los que producen el mayor número de direcciones onion descubiertas diariamente. Demostramos la falta de técnicas especializadas en recopilar direcciones onion, sesgo en los procedimientos de búsqueda y recolección, poca variedad de servicios ocultos descubiertos, y espacios de búsqueda limitados. En consecuencia, proponemos una serie de recomendaciones para mejorar el descubrimiento de direcciones onion: ampliar la combinación de técnicas, emplear tanto la Surface web como la Dark web para la búsqueda, implementar un proceso de recolección continua en fuentes de datos actualizados debido a la naturaleza dinámica de los servicios ocultos, guiar la recolección estratégicamente en lugar de depender de métodos de fuerza bruta, aprovechar rutas de búsqueda alternativas más allá del rastreo mediante la explotación de correlaciones y pivotando a través del ciberespacio, y evaluar la efectividad y representatividad de la recolección para mejorar los resultados con el tiempo.

Como principales conclusiones, esta tesis doctoral subraya el inmenso potencial de OSINT como herramienta estratégica para resolver problemas en muchos sectores. En la era de Big Data e IA, OSINT extrae conocimiento a partir de grandes y complejas fuentes de información en abierto como redes sociales, documentos online, páginas web, e incluso en la Deep y Dark web. Sin embargo, una aplicación efectiva de OSINT requiere más que un análisis de datos y precisa una planificación estratégica y comprensión del contexto o sector específico que se está estudiando. La elección de tecnologías, métodos analíticos y visualizaciones debe ser jusitificada, y los diseños deben ser escalables y eficientes.

Por otro lado, los casos prácticos desarrollados evidencian que la incorporación de OSINT en ciberseguridad y ciberdefensa es cada vez más valiosa. El SOCMINT ayuda a caracterizar bots sociales en contextos de desinformación, que junto a la IA retorna resultados tan sofisticados como el sentimiento del contenido orgánico generado en una red social o el alineamiento político de una cuenta automatizada.

El DARKINT, por su parte, permite recopilar enlaces de sitios anónimos de la Dark web.

Además, un enfoque multidisciplinario potenciaría significativamente la eficacia de las actividades de OSINT. Si bien el rol de la informática y la ciencia de datos es indiscutible, las aportaciones de ciencias sociales, tales como la sociología y la psicología, pueden ofrecer perspectivas complementarias sobre el comportamiento humano, tendencias sociales y contextos culturales. La adopción de prácticas éticas también es importante, teniendo en cuenta los potenciales resultados adversos de usar OSINT. Además, juristas y desarrolladores deben colaborar para diseñar sistemas que se alineen con leyes y estándares.

Como última conclusión exponemos que el desarrollo de OSINT lleva consigo una serie de riesgos. Los datos abiertos pueden ser explotados para ingeniería social, spear-phishing, perfilado, engaño, chantaje, difusión de desinformación o lanzamiento de ataques personalizados. Por lo tanto, implementar medidas de seguridad adecuadas, incluyendo almacenamiento de datos seguro, acceso controlado y auditorías regulares, es crucial para aumentar nuestros niveles de protección.

Finalmente, esta tesis doctoral abre el camino para diversas direcciones futuras prometedoras en el campo de OSINT. En particular, trabajos venideras podrían estudiar el fenómeno de la desinformación en detalle, evaluar los efectos de diferentes ataques manipulativos, valorar las posibles contramedidas para combatirlos y explorar el uso de Inteligencia Artificial Generativa (GenAI, por sus siglas en inglés *Generative AI*) para construir simulaciones basadas en agentes realistas. Otra dirección sería investigar en ciberconciencia situacional desde el punto de vista informativo y cognitivo. Esto podría incluir el desarrollo de metodologías para la recolección, fusión, análisis y visualización de la información en el ciberespacio para proporcionar una visión clara en tiempo real, facilitando la toma de decisiones, detección temprana y reacciones efectivas. Esto llevaría consigo desafíos técnicos relacionados con la visualización de información, el seguimiento de diversos flujo de datos, la identificación de contenido malicioso, o la evaluación del estado cognitivo, emocional y de vulnerabilidad de los usuarios. La última propuesta de trabajo futuro recogida en este documento es la exploración de los límites éticos y legales de OSINT, donde se podría colaborar con juristas para interpretar los marcos de cumplimiento legales, como el RGPD, y pautas éticas en este paradigma que trabaja con datos públicos.

Contents

1 Introduction **25**

2 Objectives **29**

3 Methodology **33**

4 Results **37**

5 Publications **43**

1 Opportunities, challenges and trends of OSINT 45

2 Security and privacy risks of OSINT 47

3 Behaviour of bots in electoral contexts 49

4 Impact of bots in social media 51

5 Identification of Dark web sites 53

6 Conclusions and future directions **55**

Bibliography **61**

Chapter 1

Introduction

Intelligence gathering, a practice with roots in military strategies of ancient civilizations, has evolved dramatically in the digital age. One principal evolution is the rise of Open Source Intelligence (OSINT), collecting and analyzing publicly accessible information for intelligence purposes [1]. While OSINT might seem novel, it has long historical antecedents for military and diplomatic strategies. The value of this type of intelligence was demonstrated during World War II when open radio broadcasts and newspapers served as rich sources of intelligence [2]. In the Cold War, the Cuban Missile Crisis (1962) saw extensive OSINT use, with the U.S. intelligence community analyzing public photographs, newspapers, and other unclassified sources to monitor Soviet and Cuban activities [3]. These historical events underline OSINT longstanding role in strategic defence activities.

In the current information-driven era, OSINT significance and complexity have grown exponentially, evolving to include many digital sources like social media, websites, blogs, databases, academic journals, and other online resources [4]. This vast pool of data, known as Big Data, offers unprecedented opportunities for scientific research and technological advancements [5]. Advanced analytics, Machine Learning (ML) and Artificial Intelligence (AI), under the recent progress in computing capabilities, have emerged as essential tools for processing and making sense of this huge amount of open data, allowing us to identify patterns and trends that were previously undiscoverable [6].

Climate scientists employ OSINT from weather databases and academic publications to trace century-long global climate patterns [7]. Market researchers, on the other hand, utilize OSINT from social media and consumer feedback platforms to gauge customer sentiments towards specific brands or products [8]. Healthcare researchers deploy OSINT from medical journals and patient forums for comprehensive epidemiological studies, like tracking the COVID-19 spread [9] or gauging vaccine sentiment during the pandemic [10]. OSINT is also a crucial tool for law enforcement and intelligence agencies, aiding in predicting crime trends, finding persons of interest, and forestalling threats through the analysis of data from social media, public records, and news [11]. In finance, OSINT from financial databases and social media guides investment firms in understanding market trends, spotting investment opportunities, and assessing risks, exemplified by the use of sentiment analysis to predict stock market fluctuations [12]. In journalism, OSINT aids in information gathering and fact-checking, with investigative journalists often relying on it to expose illicit activities or represent public opinion [13]. In human resources, OSINT is a crucial tool for gaining deeper insights into job applicants by assessing their online presence, aiding in comprehensive and objective hiring decisions [14]. Therefore, the influence of OSINT now reaches far beyond geopolitical or security contexts, stretching into knowledge for understanding real-world dynamics and supporting decision-making.

In a digital landscape with an increasing prevalence of complex and sophisticated cyberthreats, the value of OSINT becomes even more apparent [15]. These dangers cause significant global damage, impacting individuals, disrupting critical infrastructures, stealing sensitive information and disrupting democratic processes. In this high-stakes environment, effective understanding and use of OSINT techniques contribute and enhance methodologies for surveillance, identifying vulnerabilities and zero-days, spotting data leaks, providing cyber threat intelligence, tracking threat actors, predicting their strategies, and gaining insights into the evolving risk landscape [16]. This forms a cornerstone of proactive security, where threats are identified, shared and mitigated before they can inflict damage.

OSINT can also be integrated into cyberdefence strategies, potentially protecting society against digital threats, influence operations and foreign interference [17]. This protection transcends immediate economic impacts and is crucial for safeguarding democracy and freedom and generating a competitive advantage to the adversary [18]. OSINT fuels situational awareness to identify social weaknesses and prevent the spread of disinformation [19], but also orients strategic communications to maintain the integrity of elections and preserve public trust in institutions [20]. Furthermore, as we approach a future where cyberwarfare and hybrid warfare might supersede traditional warfare with the recent advances in Generative AI [21], the role of OSINT in cyberdefence is expected to grow even further in the strategic, information and cognitive domains [22].

Despite the opportunities OSINT presents in different areas such as security, defence, sociology, business, politics, marketing, journalism, disaster management, healthcare, human rights, finances, and investment or academic research, there are some ethical considerations and critical challenges along with its development [23]. The misuse of OSINT can lead to significant security offences and privacy violations, including cybercrime, stalking and harassment, disinformation campaigns, social profiling, corporate espionage, political manipulation or bullying [24], [25]. The situation is further complicated as more individuals share personally identifiable information (PII) online, increasing their vulnerability to tailored threats like impersonation or social engineering attacks against society [26] or military [27].

In this PhD thesis, we explore OSINT from a contemporary perspective to motivate, justify and demonstrate its potential to enrich cybersecurity and cyberdefence activities. We discuss the opportunities that OSINT presents, the existing tools and techniques, as well as the risks associated with its misuse by cybercriminals. Given the high technical component of this intelligence and the absence of academic references to show OSINT advantages, particularly in the context of social networks in Spain or related to the Dark web, practical applications of Social Media Intelligence (SOCMINT) in the Spanish general election of 2019, and Dark Web Intelligence (DARKINT) to identify sites of the anonymous Tor network are elaborated. These hands-on case studies demonstrate the importance of OSINT in addressing current and future challenges related to protecting society and democracy against threats.

This research is validated through a series of peer-reviewed articles that jointly build this PhD Thesis in compilation, being the PhD candidate the main author in all of them:

1. Javier Pastor Galindo, Pantaleone Nespoli, Félix Gómez Mármol and Gregorio Martínez Pérez, "**The not yet exploited goldmine of OSINT: Opportunities, open challenges and future trends**", *IEEE Access*, vol. 8, pp. 10282-10304, 2020, 10.1109/ACCESS.2020.2965257 [28]

2. Javier Pastor Galindo, Félix Gómez Mármol and Gregorio Martínez Pérez, "**Nothing to hide? On the security and privacy threats beyond open data**", *IEEE Internet Computing*, vol. 25, no. 4, pp. 58-66, 2021, 10.1109/MIC.2021.3088335 [29]

3. Javier Pastor Galindo, Mattia Zago, Pantaleone Nespoli, Sergio López Bernal, Alberto Huertas Celdrán, Manuel Gil Pérez, José A. Ruipérez Valiente, Gregorio Martínez Pérez and Félix Gómez Mármol, "**Spotting political social bots in Twitter: A use case of the 2019 Spanish general election**", *IEEE Transactions on Network and Service Management*, vol. 17, no. 4, pp. 2156-2170, 2020, 10.1109/TNSM.2020.3031573 [30]

4. Javier Pastor Galindo, Félix Gómez Mármol and Gregorio Martínez Pérez, "**Profiling users and bots in Twitter through social media analysis**", *Information Sciences*, vol. 613, pp. 161-183, 2022, 10.1016/j.ins.2022.09.046 [31]

5. Javier Pastor Galindo, Félix Gómez Mármol and Gregorio Martínez Pérez, "**On the gathering of Tor onion addresses**", *Future Generation Computer Systems*, vol. 145, pp. 12-26, 2023, 10.1016/j.future.2023.02.024 [32]

OSINT is poised to be pivotal in shaping the present and the future of cybersecurity and cyberdefence. Its capabilities in detecting, predicting, and mitigating cyberthreats could be the key to protecting our digital society and preserving democracy and freedom against an increasing tide of cyberthreats, particularly cognitive offences and influence operations.

Chapter 2

Objectives

The primary motivation of this PhD thesis is to highlight and illustrate Open Source Intelligence (OSINT) as a reference model to enhance civilian cybersecurity measures for protecting digital systems and data, and to boost the development of mature cyberdefence capabilities for preserving state assets and supporting military operations. In this sense, this dissertation seeks to expand our understanding of the paradigm of OSINT, focusing on its various applications, intrinsic challenges, and consequential impacts on cybersecurity and cyberdefence. This study is oriented around the following appealing research objectives:

O1. Review the current state of OSINT

The OSINT paradigm, originally utilized in military contexts, has garnered increasing attention in response to the widespread adoption of digital services and social platforms. The advent of the Big Data era and the subsequent rise of Artificial Intelligence (AI) offers unique opportunities for data utilization, yielding critical insights. However, updated discourse on the present state of OSINT in this rapidly changing environment is noticeably lacking.

For this reason, *Objective 1* consists in scrutinizing and assessing existing OSINT methodologies, tools, and applications, also unveiling the limitations of the paradigm. This includes creating a well-structured overview of the current OSINT landscape, highlighting its strong points and deficiencies. Furthermore, this dissertation examines the potential benefits of OSINT and proposes various ways in which it could bolster cybersecurity. The study also addresses the limitations and hurdles of implementing OSINT, suggesting that a responsible, ethical and legal development is needed to avoid misuse and associated risks.

O2. Categorize the security and privacy risks of OSINT

Among the various applications of OSINT, it is crucial to acknowledge the existence of illicit and dangerous practices that can be employed for malicious purposes. Regrettably, cybercriminals have acknowledged the exploit of OSINT to manipulate open data, transforming it into a cyberweapon capable of threatening individuals and organization through profiling, deception and blackmail. Therefore, assessing the potential risks associated with the vast amount of publicly available data is imperative, especially in cybersecurity and cyberdefence.

Thus, *Objective 2* involves classifying and discussing potential threats and misuse of public data. Of vital importance is the assessment of Artificial Intelligence in developing innovative cyberattacks, as AI significantly influences cybercrime evolution. Through a comprehensive analysis of various offences, this dissertation aims to shed light on the security and privacy risks inherently connected with the exploitation of OSINT by cybercriminals.

O3. Develop OSINT techniques to counter online threats in social media

On a practical level, gathering intelligence from open sources has become closely intertwined with social networks in the current landscape. Unfortunately, these platforms have also become a hub for societal and military attacks, making OSINT, notably Social Media Intelligence (SOCMINT), an essential resource for analyzing the voluminous information within these online spaces. In the context of cyberdefence, OSINT solutions are increasingly necessary for situational awareness, particularly of the cyberspace layer and cyberpersonas, becoming essential for the future battlefield of cognitive and information warfare.

Therefore, *Objective 3* aims to design and implement OSINT strategies from a practical perspective. In particular, the goal is to analyze publicly accessible social media data and apply AI to identify automated accounts, and evaluate their behaviour and impact in the information environment. This PhD thesis evaluates the effectiveness of those OSINT solutions in spotting and characterizing unauthentic behavior through experimental case studies in critical electoral contexts, thus contributing to understanding these threats to national integrity widely launched by foreign states.

O4. Investigate OSINT techniques for identification of Dark web sites

The traditional Internet and OSINT have gained a significant reputation among practitioners. However, a lesser-known and unexplored anonymous part exists called the Dark web. The exploration of Dark web sites is vital in cybersecurity and cyberdefence activities to monitor data leaks, organized communities, weapon sales, hacking services, or propagandist forums, among others. However, one key challenge for analysts is discovering illicit pages and underground forums hosted on anonymous networks, such as the Tor network, commonly based on static and constrained repositories. Unfortunately, there is limited scientific knowledge on how to systematically discover Tor websites on a large scale for automated analysis to generate Dark Web Intelligence (DARKINT).

In light of this, *Objective 4* extends the possibilities of OSINT to the Dark web, dealing with the identification and evaluation of OSINT techniques for gathering Tor onion addresses, those links composed of random base32-coded characters and the ".onion" top-level domain. Analysts and researchers could implement the resulting OSINT methods for discovering the addresses in the wild and accessing them to fuel

Dark web analytic investigations. In this sense, this PhD thesis uncovers a list of techniques for collecting Tor onion addresses, their functioning and effectiveness.

By completing these objectives, this research will contribute significantly to the scholarly discourse on cybersecurity and cyberdefence, paving the way for safer, more effective utilization of OSINT in various domains.

Chapter 3

Methodology

The following chapter presents the methodology conducted to address the objectives of this PhD thesis. Our research aims to investigate the paradigm of Open Source Intelligence (OSINT) for complementing cybersecurity and cyberdefence activities, encompassing a literature review, risk assessment, data collection and analysis in social media, and the Dark web exploration, culminating in a synthesis of findings and potential areas for future research.

M1. Research question formulation

The research begins with the formulation of the central question: How can Open Source Intelligence (OSINT) be leveraged for cybersecurity and cyberdefence tasks? This question is derived from recognizing the extensive collection of publicly available data in cyberspace and the latest progress in advanced analytics, Machine Learning and Artificial Intelligence, thus suggesting potential implications for the protection of society, organizations and states.

The four objectives of the thesis, derived from the research question, entail reviewing the current state of OSINT, recognizing and categorizing the security and privacy risks associated, developing use cases in which OSINT techniques counter online threats and assist to identify Dark web sites.

M2. Literature review

A comprehensive review of the existing literature is conducted to understand the current state of Open Source Intelligence (OSINT), its applications, challenges, and future trends, addressing the *Objective O1* of this PhD thesis. This review identifies gaps in the existing research and provides a foundation for subsequent studies.

The literature review delves into a detailed analysis of recent research works in the field of OSINT, discussing the motivations behind its development, and its advantages and drawbacks, with special mention to the incorporation of advanced analytics, Machine Learning and Artificial Intelligence. It also explores the principal steps and practical workflows involved in OSINT, clearly understanding how it operates. The overview further includes an in-depth examination of OSINT-based collection techniques and services, and a comparative analysis of various OSINT tools that automate the collection and analysis of information. The potential integration of OSINT in the investigation of cyberattacks is also discussed, highlighting its significant role in enhancing internal cyberdefence operations.

This step poses open challenges regarding research in OSINT and concludes with key remarks and future research directions, being validated through the following publication, available in Section 5.1:

- Javier Pastor Galindo, Pantaleone Nespoli, Félix Gómez Mármol and Gregorio Martínez Pérez, "**The not yet exploited goldmine of OSINT: Opportunities, open challenges and future trends**", *IEEE Access*, vol. 8, pp. 10282-10304, 2020, 10.1109/ACCESS.2020.2965257 [28]

M3. Risk assessment

An integral part of the methodology is the assessment of risks associated with the misuse of OSINT by cybercriminals. This involves understanding the potential security offences and privacy violations that could arise from exploiting open data sources, giving response to the *Objective O2* of this dissertation.

In this step, we analyze the ways in which cybercriminals can exploit publicly available information to design tailored cyberattacks, including the use of Artificial Intelligence to enhance the effectiveness of these attacks. The results are validated in the following publication, available in Section 5.2:

- Javier Pastor Galindo, Félix Gómez Mármol and Gregorio Martínez Pérez, "**Nothing to hide? On the security and privacy threats beyond open data**", *IEEE Internet Computing*, vol. 25, no. 4, pp. 58-66, 2021, 10.1109/MIC.2021.3088335 [29]

M4. Experimental analysis of online threats in social media

Given the review of the strong points of OSINT, we apply this intelligence paradigm to monitor online threats in social media, as stated in the *Objective O3* of this PhD thesis. Due to the proliferation of documented interference in social media by external actors to manipulate the elections of different countries, which are simultaneously related to different OSINT risks exposed in this thesis, we carry out two hands-on studies for categorizing the behaviour and impact of social bots, those automated accounts that artificially generate, viralize or confront content in social media to have manipulative effects on people's opinion, during the previous weeks to the Spanish general election of 10th November, 2019, in Twitter.

M4.1. Characterization of the behaviour of Twitter social bots in the 2019 Spanish general election

In the first study, the main goal is to categorize the interactions social bots engage in during the weeks leading up to the general election, the political preferences shown, the emotions emitted in their content and interactions, and their activity over time. In this sense, the Twitter API was requested through the Social Feed Manager tool [33] between October 4th, 2019 and November 11th, 2019 to gather tweets (and associated users) that contained at least one of the 46 hashtags that we introduced based on the main political parties and national events.

Particularly, a multifaceted framework was designed with the Botometer tool [34] to detect potential bot accounts, and machine learning algorithms such as Decision Tree, Random Forest, Support Vector Machine, Naive Bayes, k-Nearest Neighbor, and AdaBoost to discern the political leanings of these bots based on the sentiment analysis of content and interactions. Furthermore, an unsupervised machine learning element was included to identify bot clusters based on their shared traits visually. The Gephi software enabled the illustration of an undirected graph showcasing the relationship network between the bots. The investigation, available in Section 5.3, and the associated dataset are published in the following articles:

- Javier Pastor Galindo, Mattia Zago, Pantaleone Nespoli, Sergio López Bernal, Alberto Huertas Celdrán, Manuel Gil Pérez, José A. Ruipérez Valiente, Gregorio Martínez Pérez and Félix Gómez Mármol, "**Spotting political social bots in Twitter: A use case of the 2019 Spanish general election**", *IEEE Transactions on Network and Service Management*, vol. 17, no. 4, pp. 2156-2170, 2020, `10.1109/TNSM.2020.3031573` [30]

- Javier Pastor Galindo, Mattia Zago, Pantaleone Nespoli, Sergio López Bernal, Alberto Huertas Celdrán, Manuel Gil Pérez, José A. Ruipérez Valiente, Gregorio Martínez Pérez and Félix Gómez Mármol, "**Twitter social bots: The 2019 Spanish general election data**", *Data in Brief*, vol. 32, p. 106047, 2020, `10.1016/j.dib.2020.106047` [35]

M4.2. Characterization of the impact of Twitter social bots in the 2019 Spanish general election

Despite having categorized the behaviour, sentiment and political affinity of automated accounts in this PhD thesis, we found the need to evaluate the materialized consequences of such activity in the social graph. Due to the lack of methodologies to infer the influence of bots activity, this second SOCMINT investigation of the dissertation designs measurements with quantitative and qualitative values to assess the the impact these bots. In this line, a data collection is performed again, with the same parameters as the previous study in the context of the 2019 Spanish general election, but with the premium version of the Twitter API. Therefore, the collected users were classified with a new version of the AI-based tool called BotometerLite [36] into the categories of Likely Bots, Likely Semi-Bots and Likely Humans.

For the subsequent characterization, a framework unifying seven perspectives is proposed to compare these three groups and extract the differences. In particular, the perspectives are based in related works and including network science fundamentals applied to retweet network investigations, namely: statistical analysis (number of existing accounts, the traffic generated, and the interactions between groups), network analysis (insights about social relationships and information-spreading phenomena), robustness analysis (vulnerability of the social graph by disconnecting nodes and detecting critical groups, influence analysis (role of groups in information spreading), structure analysis (contact networks and data paths in which users are involved), temporal analysis (temporal patterns or anomalies and categorize the activity of groups over time), and content and virality analysis (traces viral content and analyzes the speed of spreading, including the study of information cascades and word clouds).

As mentioned, the whole framework is applied to determine the impact that Likely Bots or Likely Semi-Bots had on the social media dynamics in comparison with Likely Humans, evidencing their influence in Twitter on the 2019 Spanish general election. This proposal and its experimental application is validated with the next publication (see Section 5.4):

- Javier Pastor Galindo, Félix Gómez Mármol and Gregorio Martínez Pérez, "**Profiling users and bots in Twitter through social media analysis**", *Information Sciences*, vol. 613, pp. 161-183, 2022, `10.1016/j.ins.2022.09.046` [31]

M5. Exploration of techniques for collection of Dark web sites

Following social media studies, the research extended its scope to include the Tor network, a significant part of the Dark web. This investigation is driven by the need to understand the broader landscape of online threats and the potential misuse of anonymous websites. This step involves the examination of 54 scholarly articles on harvesting Tor links, published between 2013 and 2022, that implemented various techniques for gathering onion addresses, which are essential for accessing anonymous websites on the Dark web, resolving the *Objective O4*.

The review identifies several challenges in gathering onion addresses and highlights the benefits of using OSINT to collect, analyze, and extract onion addresses through publicly available data. A series of recommendations for improving onion address discovery is also presented. The results are published in the following article (see Section 5.5):

- Javier Pastor Galindo, Félix Gómez Mármol and Gregorio Martínez Pérez, "**On the gathering of Tor onion addresses**", *Future Generation Computer Systems*, vol. 145, pp. 12-26, 2023, `10.1016/j.future.2023.02.024` [32]

M6. Conclusions and future work

This PhD thesis concludes with a synthesis of the findings and a discussion of their implications for cybersecurity and cyberdefence activities. The conclusion also outlined potential areas for future research, particularly in a scenario of evolving cyberthreats and the continuous growth of publicly available data.

Chapter 4

Results

In this chapter, the central findings and significant results of this PhD are meticulously presented and discussed.

R1. The current state of OSINT

The updated exploration of OSINT (*Objective O1*) through the literature review (*Step M2*) underscores its potency as a comprehensive paradigm across cyberspace. The sectors that leverage OSINT include social opinion and sentiment analysis, which encapsulates marketing, political campaigns, disaster management, human resources recruiting, and journalism. Furthermore, OSINT aids in the detection and monitoring of cybercrime and organized crime by spotting illicit activities and retrieving suspicious traces. It is also a significant force in cybersecurity and cyberdefence, where it is used in footprinting, forensic analysis, crime attribution, and social engineering prevention, among others.

Our review exposes the ascendance of OSINT in recent years is attributed to a confluence of factors, including access to a vast amount of public information, increased computing power, and advancements in Big Data and AI technologies. As a result, we find that OSINT is compatible with diverse data sources and a wide range of use cases. However, analysts leveraging OSINT also face several challenges, such as managing the complexity of data, handling unstructured information, and dealing with misinformation. Further complications arise from the reliability of data sources and the need to navigate stringent ethical and legal considerations, such as the European Union's General Data Protection Regulation (GDPR). Despite these challenges, we claim that the value of OSINT in the aforementioned applications remains considerable.

R2. Security and privacy risks of OSINT

In the context of security and privacy threats, we survey the different OSINT-based attacks that can be implemented by cybercriminals (*Objective O2*) to expose the risks associated with OSINT (*Step M3*), specifically those leveraging Personally Identifiable Information (PII). The analysis done as part of our research led to the development of a taxonomy of attacks that exploit PII, categorized into three primary threat dimensions: deception, blackmail, and expansion.

Under the deception category, data is manipulated to mislead victims or systems. This category comprises social engineering attacks like phishing, which employs PII to craft personalized messages to deceive victims into revealing sensitive data. Spear-phishing, a more sophisticated form of phishing, uses specific details about a victim to increase its chances of success. Impersonation attacks involving unauthorized use of another person's identity are often facilitated by PII sourced from open data. In the blackmail dimension, data is used to coerce or manipulate victims, typified by extortion attacks. Here, cybercriminals use the obtained data to force their victims into specific actions, often involving payment to avert the release of sensitive information. The expansion category employs data to acquire additional critical information and broaden the potential attack surface. In profiling attacks, for instance, cybercriminals use PII to assemble comprehensive profiles of their victims, while recognition attacks leverage data about network infrastructures to facilitate unauthorized access.

Across these categories, we find that AI plays a pivotal role as it may enhance the severity of these threats. It can bolster password-cracking techniques in brute-force attacks, generate deep fake videos for impersonation attacks, and automate the collection and analysis of open data for profiling attacks. This exploration of risks depicts a clear picture of how OSINT-based attacks can unfold as well as the critical role AI can play in augmenting these threats.

In order to mitigate the aforementioned negative effects, some recommendations are suggested in this thesis. For users, these include minimizing virtual friendships to only known contacts, reducing the publication of personal photos and sensitive information on social networks, deleting any personal details that are not strictly necessary to be publicly accessible, configuring restrictive rules within privacy settings of online services and web browsers, and installing complementary privacy tools such as ad-blockers and anti-tracking extensions. For service providers, recommendations include adopting privacy as a design principle at the beginning of each project, protecting the data of customers and third parties under privacy standards, reviewing the vulnerabilities of software and the exposure of AI-based services to avoid data leaks or intrusions, making employees aware of not disclosing internal details, and providing users with functionalities for the tracking, handling, and cleaning of personal data.

R3. Behaviour of social bots in the 2019 Spanish general election

Taking advantage of the OSINT benefits and techniques from the review (*R1*), which highlights the integration of Big Data and AI technologies in novel OSINT workflows, this thesis elaborates in a practical way an advanced analysis with AI to identify social bots and characterize their behaviour in Twitter. At the same time, the OSINT risks such as social engineering, monitorization or profiling are directly faced (*R2*). In this way, the behavior of these automated agents was analyzed in Twitter during the 2019 Spanish general election (*Step M4.1*), showing the potential of OSINT in a state threatening context such as a democratic election, demonstrating its usefulness for situational awareness and characterization of the threat landscape (*Objective O3*).

In this investigation, a dataset comprising 5,826,655 tweets was compiled and applied to substantiate the proposed framework [35]. Most of these tweets were retweets, making up 87.81% of the total, and the dataset yielded 783,185 distinct user accounts, of which 0.68% were disqualified due to account inactivity or suspension. The users were then segregated into three categories based on their bot scores as determined by Botometer [34], resulting in 592,909 humans (75.7%), 144,856 uncertain users (18.5%), and 40,098 bots (5.1%).

The analysis indicates that 5% of the traffic volumes was attributed to social bots, with humans predominantly retweeting content shared by these bots rather than quoting or replying to them. Interestingly, the data reveals that social bots frequently retweet human content, presumably aiming for virality. Leveraging sentiment analysis and training the models using interactions and messages from a sample of official accounts of five major political parties, the 40,098 bots were further classified. A subset of these bots appeared to have clear political alignments to one of the five political parties (*United We Can*, *Citizens*, *VOX*, *Spanish Socialist Workers Party* and *People's Party*). The study also spotlighted a distinct correlation between noteworthy real-world events and increased bot activity. Notably, bots exhibited a more positive sentiment towards messages pertaining to their aligned party and a decidedly negative sentiment with other parties.

It is worth highlighting that the results of this study had a significant media coverage at national level, being published in different media such as the newspaper El País [1].

R4. Impact of social bots in the 2019 Spanish general election

After the detailed study of the actions and nature of social bots (*R3*), the challenge of evaluating the impact on their behaviour remained active (*Objective O3*). Due to the lack of frameworks to estimate this impact by users, a data-driven framework that employs different analysis perspectives is designed for comparing users and bots, identifying their differences, and measuring the interference between them (*Step M4.2*). In particular, seven types of analysis with well-known algorithms are considered: statistical, network, robustness, influence, structure, temporal, and content and virality analysis.

The framework was applied and validated using an extended version of the Twitter dataset of the 2019 Spanish election mentioned before. The updated dataset included 39,344,305 retweets and 2,802,467 users, but a random 20% sample of 7,868,861 retweets and 1,297,975 associated users was finally used for computational reasons. The users were classified with BotometerLite [36] into three categories: 709,212 Likely Humans, 208,836 Likely Semi-Bots, and 109,257 Likely Bots. The remaining 270,670 users to complete the full sample of 1,297,975 were not classified as they represented suspended or private Twitter profiles.

Experimental findings, which utilized the seven perspectives in the framework, revealed that the network structure of the analyzed snapshot was challenging to

[1] https://elpais.com/tecnologia/2020-05-03/de-vox-a-unidas-podemos-las-cuentas-de-bots-se-reparten-entre-todos-los-partidos.html

manipulate. However, the natural dynamics of the network were altered by semi and fully-automated agents. Semi-automated accounts attracted user's attention and helped connect with the most active and popular nodes within the network. In contrast, fully automated bots were noteworthy for their proximity to all users and accessibility within the network, even drawing interactions. These bots were primarily located on the network's periphery, and their content did not significantly circulate. In conclusion, while social bots have modified the social network, they did not succeed in their influence tasks. On the other hand, semi-automated bots have a more substantial impact than their fully automated counterparts.

R5. Techniques for collection of Dark web sites

Beyond the SOCMINT works (*R3* and *R4*), the Dark web was chosen as second type of OSINT scenario to be less explored in the literature (*Objective O4*). The exploration of techniques for gathering Dark web sites (*Step M5*) revealed several challenges in collecting Tor onion addresses, including the lack of specific onion gathering techniques beyond traditional methods, bias in collecting procedures, a narrow variety of discovered onion services, and limited spaces of search.

At the same time, we identified five different methods for gathering Tor onion addresses: repositories, Tor crawling, onion search engines, relay injection, and generic search engines. Each technique possesses unique strengths and weaknesses. Repositories refer to collections of onion addresses compiled by third parties and made available for download, offering high accuracy and low delay but a medium range of the types of onion services that can be located. Tor crawling, the practice of navigating the Tor network and following links to onion services, yields medium accuracy and high delay but finds many onion services. Onion search engines index and search for onion addresses on the Tor network specifically, providing high accuracy in finding onion addresses directly and cleanly but a low variety in the types of onion services they can locate. Relay injection involves deploying Tor relays within the Tor network and waiting for them to transform into directory servers (HSDirs), capable of capturing onion addresses directly from descriptors. While offering high accuracy and low delay, this method presents a high complexity. Finally, generic search engines, which explore conventional websites, might locate onion addresses through keyword searches, offering low accuracy and medium delay but can uncover a wide range of onion services. Each of these techniques depends on extracting publicly available data, that is, all of them are clear examples of application of the OSINT concept.

Our research concludes with a series of challenges to be addressed for improving onion address discovery. Firstly, enhancing the combination of multiple techniques is essential, as most collections focus on a limited number of techniques, hindering comprehensive results. Secondly, unifying the search surface by programming processes on the Surface and Dark Web, potentially through bidirectional spiders between them. Thirdly, maintaining an updated gathering process is paramount due to the dynamic nature of onion services, integrating non-static data sources and continuous intelligent searching. Fourthly, guiding gathering strategically, rather than relying on brute-force methods, can lead to more fruitful outcomes, possibly by targeting hub web pages. Fifthly, alternative search paths should be leveraged for broader coverage beyond traditional techniques, using correlations and pivoting through the cyberspace. Lastly, evaluating gathering effectiveness and representativeness through metrics like gathering rate and proportion of collected onion addresses in relation to the Tor network's size remains crucial for gauging research impact and progress over time.

Chapter 5

Publications

1 Opportunities, challenges and trends of OSINT

Title

The not yet exploited goldmine of OSINT:
Opportunities, open challenges and future trends

Authors

Javier Pastor Galindo[1], Pantaleone Nespoli[1],
Félix Gómez Mármol[1], Gregorio Martínez Pérez[1]

[1] *Department of Information and Communications Engineering,
University of Murcia, Spain*

Publication details

Journal	IEEE Access	**Publisher**	IEEE
Volume	8	**Number**	–
Pages	10282-10304	**Year**	2020
JIF	3.367	**Rank**	Q2
Status	Published	**DOI**	10.1109/ACCESS.2020.2965257

Abstract

The amount of data generated by the current interconnected world is immeasurable, and a large part of such data is publicly available, which means that it is accessible by any user, at any time, from anywhere in the Internet. In this respect, Open Source Intelligence (OSINT) is a type of intelligence that actually benefits from that open nature by collecting, processing and correlating points of the whole cyberspace to generate knowledge. In fact, recent advances in technology are causing OSINT to currently evolve at a dizzying rate, providing innovative data-driven and AI-powered applications for politics, economy or society, but also offering new lines of action against cyberthreats and cybercrime. The paper at hand describes the current state of OSINT and makes a comprehensive review of the paradigm, focusing on the services and techniques enhancing the cybersecurity field. On the one hand, we analyze the strong points of this methodology and propose numerous ways to apply it to cybersecurity. On the other hand, we cover the limitations when adopting it. Considering there is a lot left to explore in this ample field, we also enumerate some open challenges to be addressed in the future. Additionally, we study the role of OSINT in the public sphere of governments, which constitute an ideal landscape to exploit open data.

IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

2 Security and privacy risks of OSINT

Title

Nothing to hide? On the security and privacy threats beyond open data

Authors

Javier Pastor Galindo[1], Félix Gómez Mármol[1], Gregorio Martínez Pérez[1]

[1] *Department of Information and Communications Engineering,*
University of Murcia, Spain

Publication details

Journal	IEEE Internet Computing	**Publisher**	IEEE
Volume	25	**Number**	4
Pages	58-66	**Year**	2021
JIF	2.680	**Rank**	Q2
Status	Published	**DOI**	`10.1109/MIC.2021.3088335`

Abstract

People's online activity continuously dumps personally identifiable information on the web. Alarmingly, this public information becomes a dangerous cyberweapon in the era of finely targeted cyberattacks. This article explores today's cyberthreats around open data, from traditional ones to AI empowering, thus unveiling a range of vulnerabilities to which end-users are exposed.

3 Behaviour of bots in electoral contexts

Title

Spotting political social bots in Twitter:
A use case of the 2019 Spanish general election

Authors

Javier Pastor Galindo[1], Mattia Zago[1], Pantaleone Nespoli[1], Sergio López Bernal[1], Alberto Huertas Celdrán[2], Manuel Gil Pérez[1], José A. Ruipérez Valiente[1], Gregorio Martínez Pérez[1], Félix Gómez Mármol[1]

[1] *Department of Information and Communications Engineering, University of Murcia, Spain*
[2] *Communication Systems Group, University of Zürich (UZH), Switzerland*

Publication details

Journal	IEEE Transactions on Network and Service Management	**Publisher**	IEEE
Volume	17	**Number**	4
Pages	2156-2170	**Year**	2020
JIF	4.195	**Rank**	Q2
Status	Published	**DOI**	10.1109/TNSM.2020.3031573

Abstract

While social media has been proved as an exceptionally useful tool to interact with other people and massively and quickly spread helpful information, its great potential has been ill-intentionally leveraged as well to distort political elections and manipulate constituents. In this article at hand, we analyzed the presence and behavior of social bots on Twitter in the context of the November 2019 Spanish general election. Throughout our study, we classified involved users as social bots or humans, and examined their interactions from a quantitative (i.e., amount of traffic generated and existing relations) and qualitative (i.e., user's political affinity and sentiment towards the most important parties) perspectives. Results demonstrated that a non-negligible amount of those bots actively participated in the election, supporting each of the five principal political parties.

IEEE TRANSACTIONS ON
NETWORK AND
SERVICE MANAGEMENT
A PUBLICATION OF THE IEEE COMMUNICATIONS SOCIETY
IEEE ComSoc
IEEE Communications Society

4 Impact of bots in social media

Title

Profiling users and bots in Twitter through social media analysis

Authors

Javier Pastor Galindo[1], Félix Gómez Mármol[1], Gregorio Martínez Pérez[1]

[1] *Department of Information and Communications Engineering,*
University of Murcia, Spain

Publication details

Journal	Information Sciences	**Publisher**	Elsevier
Volume	613	**Number**	–
Pages	161-183	**Year**	2022
JIF	8.1	**Rank**	D1
Status	Published	**DOI**	`10.1016/j.ins.2022.09.046`

Abstract

Social networks were designed to connect people online but have also been exploited to launch influence operations for manipulating society. The deployment of social bots has proven to be one of the most effective enablers to polarize and destabilize platforms. While automatic tools have been developed for their detection, the way to characterize these accounts and measure their impact is heterogeneous in the literature. In this work, we select metrics and algorithms from existing efforts to ensemble a data-driven methodology to profile groups of users and bots of Twitter from seven perspectives. We apply the framework to a dataset of Twitter retweets before the 10 November 2019 Spanish elections to characterize potential interferences. In this case study, Likely Bots (fully automated accounts) and Likely Semi-Bots (partially automated accounts) interacted with the same tendencies as Likely Humans (non-automated users), generating similar virality (information cascades) over time and without compromising the network connectivity. However, Likely Bots particularly stood out as close, visible, and reachable to other users. Likely Semi-Bots attracted particular attention, created proportionally more retweets, and were placed in strategically key positions in the core of the network. Results suggest that semi-automated accounts would be more threatening than fully automated ones.

INFORMATION
SCIENCES
Informatics and Computer Science
Intelligent Systems
Applications
AN INTERNATIONAL JOURNAL

5 Identification of Dark web sites

Title

On the gathering of Tor onion addresses

Authors

Javier Pastor Galindo[1], Félix Gómez Mármol[1], Gregorio Martínez Pérez[1]

[1] *Department of Information and Communications Engineering,*
University of Murcia, Spain

Publication details

Journal	Future Generation Computer Systems	**Publisher**	Elsevier
Volume	145	**Number**	–
Pages	12-26	**Year**	2023
JIF	7.5	**Rank**	D1
Status	Published	**DOI**	`10.1016/j.future.2023.02.024`

Abstract

Exploring the Tor network requires acquiring onion addresses, which are crucial for accessing anonymous websites. However, the Tor protocol presents a challenge, as it lacks a standard method for finding these complex links composed of either 16 or 56 base32-coded characters and featuring the unique ".onion" top-level domain. This study delves into the existing literature analyzing onion services and categorizes the various strategies employed to gather their addresses. The success of each approach is measured by the number of addresses obtained, while the relevancy of the work is evaluated by comparing the number of services uncovered to Tor's official count. The results indicate that the most used techniques are Tor crawling and repositories, whereas the most effective methods are relay injection, repositories, and Tor crawling. This paper also estimates the representativeness of literature collections, revealing that most past works explored a small portion of the Tor network. The study also uncovers the limitations of onion gathering and sheds light on the challenges for future research to provide more representative datasets for dark web exploration.

Chapter 6

Conclusions and future directions

The completion of this PhD thesis and the results derived from its associated research unveil a number of conclusions deserving to be highlighted.

C1. The importance of a strategic application of OSINT for problem-solving

This PhD thesis evidences that OSINT is a powerful tool for extracting valuable knowledge from a vast pool of information. The data can be gathered from various sources, including social networks, public government documents, online multimedia content, and the Deep and Dark web, as revealed in the result *R1*. Additionally, the evolution of computer architecture, coupled with the spread of data analysis and machine learning techniques, has amplified the potential of OSINT. These advancements enable the processing and interpretation of large data volumes and the identification of intricate, often unexpected, correlations. However, as evidenced in the experimental use cases of this PhD thesis (*R3* and *R4*), these opportunities require more than just data collection and analysis, demanding strategic planning, comprehensive study, and accurate interpretation to fulfill the needs and provide solutions to the analyst.

Moreover, OSINT is not only technical, and understanding the specific context or business sector of the use case where to apply it is a critical part. As the OSINT application spans various sectors, from politics and economics to society and defence, tailoring its usage to specific objectives aids in selecting relevant data sources and determining the most fitting analytical methods. Nevertheless, technical knowledge is vital to choose the right technologies, analytical algorithms, and visualizations to meet strategic objectives. Particularly in the era of Big Data, developing a scalable and efficient design is pivotal.

C2. The increasing value of OSINT for cybersecurity and cyberdefence

The intelligence generated from open sources reinforces cybersecurity measures and fortifies cyberdefence strategies. By integrating OSINT into existing methodologies, it is possible to characterize the threat landscape, track suspicious users, provide situational awareness or identify vulnerabilities, as evidenced in the result

R1. Moreover, monitoring online spaces contributes significantly to national and international security and societal integrity, raising early warnings of hybrid threats and influence operations.

The application of OSINT is particularly evident in the context of social media platforms such as Twitter, leading to SOCMINT, as shown in the results *R3* and *R4*. For instance, the analysis of social bots on Twitter can yield valuable insights into potential threats and vulnerabilities to which a huge part of users are exposed daily. These bots, capable of operating at a much higher pace than human users, can be exploited to disseminate misleading information and manipulate public opinion, thereby posing significant threats to our society. In this scenario, the appropriate OSINT solutions enable the identification and tailored description of these automated agents, effectively mitigating their potential impact. This PhD thesis particularly evidences that the integration of OSINT with Artificial Intelligence (AI) can further enhance the efficiency and effectiveness of these processes. For example, Machine Learning algorithms helped to profile the behavior of users and bots on social media platforms, aiding in identifying patterns that may signal malicious activities and measuring their influence.

The Dark web, often linked with illicit activities, represents another domain where OSINT can significantly contribute to cybersecurity and cyberdefence via DARKINT, as seen in the result *R5*. This anonymous segment of the Internet can be monitored at a large scale with automated systems to gain valuable insights into potential threats and vulnerabilities. This PhD thesis highlighted the ways to obtain the addresses of Tor sites in open sources, thus enabling access to assist in detecting propagandist information, organized crime groups, data leaks or illegal marketplaces of stolen data, drugs, weapons and counterfeits. Through OSINT, patterns and trends indicative of malicious activities can be identified, thus enabling a more proactive and effective approach to cybersecurity and cyberdefence strategies.

C3. The risky implications of OSINT development

OSINT is a powerful paradigm to feed cybersecurity processes and cyberdefence activities, but it can also represent a double-edged sword in the context of cybercrime and cyberwarfare, as shown in the result *R2*. The same data used to protect an organization can be exploited by adversaries if not properly managed and secured.

The potential risks of OSINT range from social engineering and spear-phishing to more sophisticated AI-powered threats. Cybercriminals can exploit open data to identify sensitive information and launch advanced adversary profiling to design tailored cyberattacks. The knowledge acquired from open sources enables deception or blackmail threats. In cyberdefence, OSINT can fuel information and cognitive warfare and enable the spread of tailored disinformation, manipulate targeted opinion, spread false information, and even influence political campaigns by knowing target preferences and weaknesses. Moreover, adversaries can use OSINT to launch personalized attacks, leveraging the wealth of open data to target specific individuals or units within the military.

With the development of OSINT, the associated security and privacy measures should be implemented to counter the misuse of this paradigm. This includes secure data storage, controlled access, and regular audits to ensure compliance with security protocols. Understanding the different dimensions of these threats and developing effective strategies to mitigate them is crucial.

C4. The need for multidisciplinary contribution to OSINT activities

While OSINT is often associated with computer science, its true potential is actually unlocked through a multidisciplinary approach due to the diversity of fields that can be applied to (*R1*). The tools and techniques developed by computer science and information technology are undoubtedly crucial for data collection and analysis. Simultaneously, data science plays a significant role in managing large volumes of data and extracting meaningful insights. However, the power of OSINT extends beyond these technical fields and more effort is needed for multidisciplinary collaboration.

Social networks, online webpages or Dark web forums are examples of rich sources of information about the daily lives, interests and activities of individuals and organizations, as demonstrated by the results *R1*, *R3* and *R4*. In order to understand the associated human behavior, social trends, and cultural contexts, the raw or processed data is not enough and the insights derived from social sciences, including sociology and psychology, are highly valuable for interpretation and discussion. In the context of this PhD thesis, such social views would have complemented the challenging task of understanding social network dynamics and measuring the influence of activity from social bots.

The ethical aspect should also be deepened and included in OSINT methodologies to mitigate possible malicious uses or adverse outcomes (*R2*). In this sense, solutions and use cases must be carefully analyzed to avoid any damage to systems, processes, people or organizations. Moreover, multidisciplinarity shall be extended when an effective collaboration between legal professionals and computer scientists is required to design systems that comply with relevant laws and standards.

From this PhD thesis, its results and conclusions, three clear avenues are opened to explore as a continuation of this OSINT research line.

F1. Study of disinformation effects and evaluation of countermeasures

The SOCMINT use cases of this dissertation unveil the behavior and impact that social bots can have in an electoral context (*C2*), directly related to the threatening spread of disinformation (*C3*). To extend the understanding of this worrying phenomena, future work could focus on assessing the effects of different disinformation attacks and evaluating potential countermeasures.

Commonly, disinformation centers around the theoretical modeling of fake news propagation and leveraging social media data for detection, like the experiments within this PhD thesis. This field grapples with several issues, including the complexity of scrutinizing incidents where there is no truth baseline to affirm the objectives, tactics, and actors involved in influence campaigns, the lack of labeled datasets for various manipulation efforts, the infeasibility of testing technical countermeasures in third-party platforms or the necessity of human involvement to measure the cognitive impact of deceptive activities.

In order to face the traditional challenges of social media research, the recent rise of Generative Artificial Intelligence (GenAI) invites us to create agent-based social systems that simulate the interactions and behaviors of individuals within a social context. In this sense, we could use a simulated agent-based sandbox to explore the potential of generative models as an innovative method for comprehending, simulating, and evaluating disinformation within controlled experimental settings. Moreover, various variables, such as techniques, intensity, and nature of manipulative operations, alongside agent attributes and context, can be adjusted and tracked. By employing suitable frameworks and models (*C1*) and the expertise from social sciences (*C4*), it would be possible to estimate the effectiveness of particular disinformation strategies. Additionally, the influence of variables like agent profile or scenario context can be scrutinized. Finally, technical countermeasures against disinformation can be simulated and configured independently, without reliance on large companies.

F2. Research on cyber situational awareness for a real-time information and cognitive picture

Another line of future work of this PhD thesis is the research and prototyping of methods and technologies for cyber situational awareness in the context of cognitive and information operations. As seen in the SOCMINT and DARKINT use cases (*C2*), threats in the Surface and Dark web are rising, and the post-analysis is helpful to understand but not enough to tackle these risks at an early stage. Due to the different attacks in the online ecosystem (*C3*), it is important to monitor the status of cyberspace in real time, identify influence operations or malicious activities that may be deployed and evaluate the cognitive status of users and society.

Based on OSINT fundamentals (*C1*), a framework with collection, fusion and analysis techniques could be explored to provide an abstract representation of the information ecosystem (social media, forums, webpages, Dark web, etc.). In this sense, the result would be a real-time visualization of social trends, online sites, information propagation, important nodes and potential threats in a clear view, supporting decision-making and protecting actions. There are technical challenges to face such as the visualization of information assets, tracking of data flows, identification of malicious content, management of unstructured and never-seen data, or the evaluation of cognitive, emotional and vulnerability status of users.

The novel development of advanced cyber situational awareness would enable new cybersecurity and cyberdefence capabilities for early detection and reaction to manipulative efforts, social engineering and cybercrime. At the same time, this line of work has to be under ethical and legal rules that preserve the privacy of the individuals, as specifically related in the following future direction.

F3. Exploration of the ethical and legal limits of OSINT

As mentioned in this thesis, OSINT is based on publicly available data, yet it is incorrect to assume that anything can be done because it is based on open and public data. OSINT practitioners must exercise vigilance to align their objectives with legitimate purposes and avoid transgressions of individual privacy rights. This includes an ethical mandate that OSINT should not be misused to invade privacy in unacceptable ways, engage in stalking or harassment of individuals, infer personal beliefs, or facilitate unethical activities such as cyberattacks.

On the other hand, the study of legal considerations in collaboration with law experts (*C4*) is needed for OSINT applications to ensure that the collection and use of information respect individual privacy rights and comply with all relevant laws and regulations, such as the European General Data Protection Regulation (GDPR). For example, the latter imposes stringent requirements on the processing of personal data, emphasizing the principles of data minimization, purpose limitation, and the protection of sensitive data. These regulations necessitate an acceptable use case for data collection and usage, obtaining necessary permissions, anonymizing data when feasible, and maintaining transparency around data usage and storage practices. Additionally, compliance with GDPR often requires explicit consent from data subjects to collect and process their personal data.

Despite all this, today, it is difficult to ensure that existing OSINT solutions meet these requirements. Therefore, from a technical point of view, it is important to evaluate ethical challenges, know legal limits, and integrate OSINT solutions in the appropriate ethical and legal frameworks.

Bibliography

[1] H. J. Williams and I. Blum, “Defining second generation open source intelligence (osint) for the defense enterprise”, RAND Corporation, Tech. Rep., 2018. DOI: 10.7249/RR1964.

[2] M. Glassman and M. J. Kang, “Intelligence in the internet age: The emergence and evolution of open source intelligence (osint)”, *Computers in Human Behavior*, vol. 28, no. 2, pp. 673–682, 2012, ISSN: 0747-5632. DOI: 10.1016/j.chb.2011.11.014.

[3] S. C. Mercado, “Sailing the sea of osint in the information age”, *Studies in Intelligence*, vol. 48, no. 3, pp. 45–55, 2009.

[4] F.-Y. Wang, K. M. Carley, D. Zeng, and W. Mao, “Social computing: From social informatics to social intelligence”, *IEEE Intelligent systems*, vol. 22, no. 2, pp. 79–83, 2007. DOI: 10.1109/MIS.2007.41.

[5] C. Eldridge, C. Hobbs, and M. Moran, “Fusing algorithms and analysts: Open-source intelligence in the age of ‘big data’”, *Intelligence and National Security*, vol. 33, no. 3, pp. 391–406, 2018. DOI: 10.1080/02684527.2017.1406677.

[6] J. R. G. Evangelista, R. J. Sassi, M. Romero, and D. Napolitano, “Systematic literature review to investigate the application of open source intelligence (osint) with artificial intelligence”, *Journal of Applied Security Research*, vol. 16, no. 3, pp. 345–369, 2021. DOI: 10.1080/19361610.2020.1761737.

[7] Q. Sun, C. Miao, Q. Duan, H. Ashouri, S. Sorooshian, and K.-L. Hsu, “A review of global precipitation data sets: Data sources, estimation, and intercomparisons”, *Reviews of Geophysics*, vol. 56, no. 1, pp. 79–107, 2018. DOI: 10.1002/2017RG000574.

[8] C. S. Fleisher, “Using open source data in developing competitive and marketing intelligence”, *European Journal of Marketing*, vol. 42, no. 7/8, pp. 852–866, 2008. DOI: 10.1108/03090560810877196.

[9] E. T. Martínez Beltrán, M. Quiles Pérez, J. Pastor-Galindo, P. Nespoli, F. J. García Clemente, and F. Gómez Mármol, “Convida: Covid-19 multidisciplinary data collection and dashboard”, *Journal of Biomedical Informatics*, vol. 117, p. 103 760, 2021, ISSN: 1532-0464. DOI: 10.1016/j.jbi.2021.103760.

[10] E. Chen, K. Lerman, and E. Ferrara, “Tracking social media discourse about the covid-19 pandemic: Development of a public coronavirus twitter data set”, *JMIR Public Health and Surveillance*, vol. 6, no. 2, e19273, 2020. DOI: 10.2196/19273.

[11] A. Yeboah-Ofori and A. Brimicombe, “Cyber intelligence and osint: Developing mitigation techniques against cybercrime threats on social media”, *International Journal of Cyber-Security and Digital Forensics*, vol. 7, no. 1, pp. 87–98, 2018. DOI: 10.17781/P002378.

[12] R. P. Schumaker, Y. Zhang, C.-N. Huang, and H. Chen, “Evaluating sentiment in financial news articles”, *Decision Support Systems*, vol. 53, no. 3, pp. 458–464, 2012, ISSN: 0167-9236. DOI: 10.1016/j.dss.2012.03.001.

[13] S. C. McGregor, “Social media as public opinion: How journalists use social media to represent public opinion”, *Journalism*, vol. 20, no. 8, pp. 1070–1086, 2019. DOI: 10.1177/1464884919845458.

[14] D. R. Hayes and F. Cappa, “Open-source intelligence for risk assessment”, *Business Horizons*, vol. 61, no. 5, pp. 689–697, 2018, ISSN: 0007-6813. DOI: 10.1016/j.bushor.2018.02.001.

[15] J. C. Gomes de Barros, C. M. Revoredo da Silva, L. Candeia Teixeira, *et al.*, “Piracema: A phishing snapshot database for building dataset features”, *Scientific Reports*, vol. 12, no. 1, p. 15 149, 2022. DOI: 10.1038/s41598-022-19442-8.

[16] F. Tabatabaei and D. Wells, “Osint in the context of cyber-security”, in *Open Source Intelligence Investigation: From Strategy to Implementation*, B. Akhgar, P. S. Bayerl, and F. Sampson, Eds. Cham: Springer, 2016, pp. 213–231, ISBN: 978-3-319-47671-1. DOI: 10.1007/978-3-319-47671-1_14.

[17] D. Lande and E. Shnurko-Tabakova, “Osint as a part of cyber defense system”, *Theoretical and Applied Cybersecurity*, vol. 1, no. 1, 2019. DOI: 10.20535/tacs.2664-29132019.1.169091.

[18] R. D. Steele, “The importance of open source intelligence to the military”, *International Journal of Intelligence and CounterIntelligence*, vol. 8, no. 4, pp. 457–470, 1995. DOI: 10.1080/08850609508435298.

[19] Y. Masakowski and J. M. Blatny, “Mitigating and responding to cognitive warfare”, North Atlantic Treaty Organization (NATO), Tech. Rep., 2023.

[20] Strategic Communications, Task Forces and Information Analysis (STRAT.2), “1st report on foreign information manipulation and interference threats”, European External Action Service (EEAS), Tech. Rep., 2023.

[21] R. Fredheim, “Virtual manipulation brief 2023/1: Generative ai and its implications for social media analysis”, NATO Strategic Communications Centre of Excellence (StratCom COE), Tech. Rep., 2023.

[22] J. Whiteaker and S. Valkonen, “Cognitive Warfare: Complexity and Simplicity”, in *Cognitive Warfare: The Future of Cognitive Dominance*, B. Claverie, B. Prébot, N. Buchler, and F. du Cluzel, Eds., NATO Collaboration Support Office, 2022, pp. 11, 1–5, ISBN: 978-92-837-2392-9.

[23] I. Böhm and S. Lolagar, "Open source intelligence: Introduction, legal, and ethical considerations", *International Cybersecurity Law Review*, vol. 2, pp. 317–337, 2021. DOI: 10.1365/s43439-021-00042-7.

[24] Y.-W. Hwang, I.-Y. Lee, H. Kim, H. Lee, D. Kim, and Y. Huo, "Current status and security trend of osint", *Wireless Communications and Mobile Computing*, vol. 2022, Jan. 2022, ISSN: 1530-8669. DOI: 10.1155/2022/1290129.

[25] A. Kanta, I. Coisel, and M. Scanlon, "A survey exploring open source intelligence for smarter password cracking", *Forensic Science International: Digital Investigation*, vol. 35, p. 301 075, 2020, ISSN: 2666-2817. DOI: 10.1016/j.fsidi.2020.301075.

[26] M. Bossetta, "The weaponization of social media: Spear phishing and cyberattacks on democracy", *Journal of International Affairs*, vol. 71, no. 1.5, pp. 97–106, 2018.

[27] S. Bay, N. Biteniece, G. Bertolin, *et al.*, "The current digital arena and its risks to serving military personnel", NATO Strategic Communications Centre of Excellence (StratCom COE), Tech. Rep., 2019.

[28] J. Pastor-Galindo, P. Nespoli, F. Gómez Mármol, and G. Martínez Pérez, "The not yet exploited goldmine of osint: Opportunities, open challenges and future trends", *IEEE Access*, vol. 8, pp. 10 282–10 304, 2020, ISSN: 2169-3536. DOI: 10.1109/ACCESS.2020.2965257.

[29] J. Pastor-Galindo, F. Gómez Mármol, and G. Martínez Pérez, "Nothing to hide? on the security and privacy threats beyond open data", *IEEE Internet Computing*, vol. 25, no. 4, pp. 58–66, 2021. DOI: 10.1109/MIC.2021.3088335.

[30] J. Pastor-Galindo, M. Zago, P. Nespoli, *et al.*, "Spotting political social bots in twitter: A use case of the 2019 spanish general election", *IEEE Transactions on Network and Service Management*, vol. 17, no. 4, pp. 2156–2170, Dec. 2020, ISSN: 1932-4537. DOI: 10.1109/TNSM.2020.3031573.

[31] J. Pastor-Galindo, F. Gómez Mármol, and G. Martínez Pérez, "Profiling users and bots in twitter through social media analysis", *Information Sciences*, vol. 613, pp. 161–183, 2022, ISSN: 0020-0255. DOI: 10.1016/j.ins.2022.09.046.

[32] J. Pastor-Galindo, F. Gómez Mármol, and G. Martínez Pérez, "On the gathering of tor onion addresses", *Future Generation Computer Systems*, vol. 145, pp. 12–26, 2023, ISSN: 0167-739X. DOI: 10.1016/j.future.2023.02.024.

[33] G. W. U. Libraries, *Social feed manager*, version v1.0, 2016. DOI: 10.5281/zenodo.597278.

[34] K.-C. Yang, O. Varol, C. A. Davis, E. Ferrara, A. Flammini, and F. Menczer, "Arming the public with artificial intelligence to counter social bots", *Human Behavior and Emerging Technologies*, vol. 1, no. 1, pp. 48–61, 2019. DOI: 10.1002/hbe2.115.

[35] J. Pastor-Galindo, M. Zago, P. Nespoli, *et al.*, "Twitter social bots: The 2019 spanish general election data", *Data in Brief*, vol. 32, p. 106 047, 2020. DOI: 10.1016/j.dib.2020.106047.

[36] K.-C. Yang, O. Varol, P.-M. Hui, and F. Menczer, “Scalable and generalizable social bot detection through data selection”, in *Proceedings of the AAAI conference on artificial intelligence*, vol. 34, 2020, pp. 1096–1103. DOI: 10.1609/aaai.v34i01.5460.