NOTIONES

Open-Source Intelligence (OSINT)

Next generation challenges, priorities, and opportunities

Whitepaper

Authors: Andrew Staniforth, Director, SAHER (Europe) OÜ
David Fortune Director, SAHER (Europe) OÜ

DOI: 10.5281/zenodo.7152286

Table of Content

Project introduction

Novel technologies have presented practitioners with new opportunities to improve the intelligence process, but have also created new challenges and threats. Consequently, the timely identification of emerging technologies and analysis of their potential impact, not only on the intelligence community but also on terrorist or criminal organisations, is crucial.

However, time constraints can prevent intelligence practitioners from being updated on the most recent technologies.

In order to address this challenge NOTIONES will establish a network, connecting researchers and industries with the intelligence community. This network will facilitate exchange on new and emerging technologies but also equip solution providers with insights on the corresponding needs and requirements of practitioners. The so gained findings will be disseminated in periodic reports containing technologic roadmaps and recommendations for future research projects and development activities.

The consortium of NOTIONES includes, among its 30 partners, practitioners from military, civil, financial, judiciary, local, national and international security and intelligence services, coming from 9 EU Members States and 6 Associated Countries. These practitioners, together with the other consortium members, grant a complete coverage of the 4 EU main areas: West Europe (Portugal, Spain, UK, France, Italy, Germany, Austria), North Europe (Finland, Denmark, Sweden, Estonia, Latvia), Mittel Europe (Poland, Slovakia, Ukraine), Middle East (Israel, Turkey, Georgia, Bulgaria, Bosnia Herzegovina, North Macedonia) for a total of 21 countries, including 12 SMEs with diverse and complementary competences.

Project Objectives

GATHER the needs of intelligence and security practitioners related to contemporary intelligence processes and technologies;

PROMOTE interaction of technology providers and academy with intelligence and security practitioners;

IDENTIFY novel technologies of relevance for practitioners through research monitoring;

Project introduction

PUBLISH a periodic report, summarising key findings in order to orientate future research and development;

ENSURE the commitment and involvement of new organisations in the pan-European NOTIONES network.

Project Facts:

Duration: 60 Months **Reference:** 101021853

Programme: Horizon 2020 SU-GM01-2020 Coordination and Support Action

Coordinator: FUNDACION TECNALIA RESERACH & INNOVATION (Spain)

Scientific Technical Coordinator: ZANASI ALLESSANDRO SRL (Italy)

This project has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement No 101021853.

Coordinator

Scientific Technical Coordinator

Project Security Officer

Academic | Think-Tanks | Research

Technology Providers

Practitioners

Threat to threat

Notions of intelligence and intelligence gathering are as old as time yet attempts to clearly define where the boundaries of contemporary intelligence are to be found remain increasingly problematic in the digitalised world in which we live [1]. The expansion of the Internet has interwoven continents, cultures, and communities, in addition to integrating with the majority of contemporary technologies. The ubiquity of the Internet has vastly increased the quantity, value, and accessibility of open-source information (OSINF), amplifying the important discipline of open-source intelligence (OSINT) to Security and Defence operations [2]. As the security landscape becomes more complex and domain-agnostic, OSINT provides an invaluable avenue to access and collect information in addition to traditional intelligence gathering and investigative techniques [3].

By definition, OSINT is the intelligence discipline that relates to intelligence produced from publicly available information that is collected, exploited, and disseminated to an appropriate audience for the purpose of addressing a specific intelligence and information requirement [4]. OSINT is now regularly used by private sector organisations as a means to measure customer loyalty, track public opinion and assess product reception. From a national security perspective, OSINT-based solutions can enhance the capabilities of law enforcement agencies and security services, providing access to more actionable intelligence to inform and support existing decision making, tasking and coordination activities. A rise in the prevalence of OSINT and its application by security forces is set against a background of conflict, insecurity, the resurgence of violence in troubled regions across the world and, more recently, the global Coronavirus pandemic and the Russian military invasion of Ukraine.

To prevent all manner of contemporary security threats, avoid strategic surprise and to render visible what hostile actors do not want governments to know, security operations must be intelligence-led. Perhaps we all know important intelligence when we see it but intelligence rarely tells you all you want to know [5]. The most important limitation on intelligence is its incompleteness. Much ingenuity and effort is spent on making intelligence difficult to acquire and hard to analyse, it is often sporadic and patchy and, even after analysis, may still be at best inferential [6]. In the post-9/11 era of asymmetric and grey zone conflict, the acquisition of intelligence to create a richer picture of new and emerging threats remains relentless, serving to fuel the rise of OSINT as an intelligence discipline in the digital age.

Theory and practice

Attempts to develop theories of OSINT are important, because intelligence is both a theoretical concept and a practical activity and thinking in the former can help maximise the effectiveness of the latter. Therefore, OSINT is understood to be both a product, and a business process. The elements of this process can be conceptualised using the intelligence cycle which contains four key steps: collection, processing, exploitation, and production [7]. Further, each step includes sub-sets: collection includes acquisition and retention, processing includes translation and aggregation, exploitation includes authentication and evaluating credibility, and production includes classification and dissemination [8].

Law enforcement agencies have long recognised the value of OSINT, being an efficient way of gathering information that can be used to inform both strategic and tactical responses. Given the scale, accessibility, and high yield of intelligence return for minimum resource, OSINT compliments and increasingly corroborates and confirms other traditional intelligence functions, all of which are relevant operational reasons as to why OSINT has quickly become a rich source of information to disrupt and detect terrorists and organised crime groups (OCGs).

Unlike other intelligence collection disciplines such as Human Intelligence (HUMINT) or Signals Intelligence (SIGNIT), OSINT is not the sole responsibility of any one single government agency but instead is collected by the entire intelligence and law enforcement community. One advantage of OSINT is its accessibility, although the sheer amount of available information can make it difficult to know what is of value.

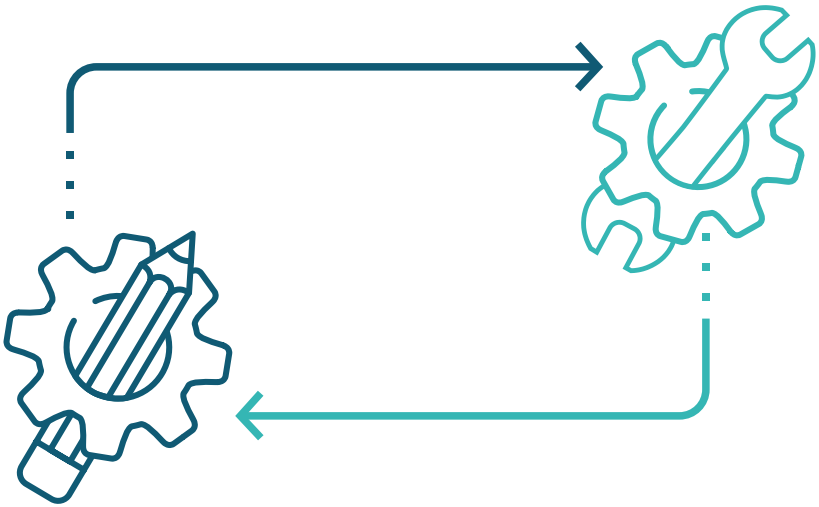
Basic OSINT investigation, within the context of the internet, seeks to identify the online and social footprint of users and to extract relevant data. When used at its most powerful, OSINT is able to augment existing closed source intelligence by providing additional information and direction to where further intelligence may be required [9]. The combined effect of OSINT with traditional intelligence sources reflects the most innovative national security intelligence models in operation today but they are not without their challenges or complications.

OSINT investigation requires careful training and must be carried out by professionals who are shrewd, objective, measured, and can manage the uncertainty of intelligence. Moreover, to progress an OSINT investigation not only requires a high degree of technical expertise but also the commitment to instilling the core competencies of investigative doctrine, requiring excellent decision-making, problem-solving, analytical skills and the ability to keep an open mind while developing complex investigative hypothesis.

Theory and practice

Fusing OSINT with traditional forms of intelligence gathering requires careful consideration, planning and implementation because intelligence can be fragile. It comes from human sources who risk their lives and whom government agencies have a high moral duty to protect, and from technologies whose effectiveness can be countered by skilled opponents [10]. Secret and sensitive intelligence can be painstakingly developed and form part of long-protracted operations involving high-value assets with international dimensions.

OSINT and information from clandestine sources can be progressed separately and effectively combined to be mutually supportive, but without the development of a strategy and structure in place, the synergy of both kinds of data will fail to yield adequate results and outcomes. OSINT does not exist in a vacuum [11]. The overlapping nature of OSINT with other intelligence disciplines—such as intelligence from human sources and from intercepted communications—is not unique and does not diminish OSINT's status as an independent intelligence discipline [12]. This 'all-source fusion' approach, the combination of all forms of intelligence gathering disciplines, has become increasingly important to the professionalisation of OSINT as an intelligence discipline but the provenance, credibility and integrity of OSINT to provide reliable intelligence in support of law enforcement, intelligence agency and military security forces' operations remains its achilleas heal.



Digital disinformation

When handling OSINT as opposed to more traditional closed intelligence sources, the concerns of the intelligence community turn from open sources to the identification of pertinent and accurate information [13]. For these reasons it is increasingly necessary to validate intelligence derived from open sources with that from robust traditional sources of intelligence. But all open sources of information are not created equal; there are some that are able to be assigned a high degree of credibility almost immediately because of the origin of the source, such as news corporations for example [14]. But even major news agencies are prone to making mistakes from time to time, especially in the midst of a large crisis, and true, accurate, independent and politically-impartial media reporting is becoming increasingly rare in the modern 24-hour news cycle, making content susceptible to sophisticated hostile misinformation campaigns.

The intentional spread of false information via fake news represents a significant challenge to the integrity, credibility, and reliability of OSINT. Fake news serves to erode public trust, harms institutions and individuals, and confuses a public trying to make sense of an increasingly complex world. But in times of crisis, such as the global Covid-19 pandemic, misinformation can prove deadly, exploiting the vulnerability and insecurity of citizens. As the Coronavirus spread around the world, so too have conspiracy theories, fake cures, and rumours. In a rapidly changing public health crisis, where accurate information is critical to citizen safety, misinformation serves to undermine government guidance putting lives at greater risk.

The scale of online misinformation during the Coronavirus crisis from rogue actors, trolls and opportunists, infected the web with rumours, myths and lies [15] . A study of 2,ooo people by Ofcom, the UK's regulator for communications services, found that nearly half of all UK adults had been exposed to fake news online about the ongoing Coronavirus crisis [16]. According to the regulator, although 55% of people said they were ignoring false claims made about the virus, with around 15% of those using fact-checking tips to research the authenticity of the claims they saw - one in 14 people admitted to sharing misinformation [17]. Of those surveyed, 40% said they found it difficult to determine what was and was not fake news about the coronavirus [18].

The genuine desire to help others at a time of global insecurity resulted in online users resharing false and inaccurate information, spreading and amplifying fake news that could not be overwhelmed by accurate information from credible sources. To curb the spread of Covid-19, and to ensure citizens followed the correct health and safety guidance, the parallel threat of viral misinformation online requires to be continuously challenged [19].

Digital disinformation

The viral misinformation during the Covid-19 crisis has provided evidence of the speed at which online open-source information gains momentum when it is shared, quoted, or replied to by users with genuine intentions to help others. The scale of the Covid-19 misinformation also shows that even where users were pointing out that the information was false, they could also inadvertently spread inaccuracies by amplifying activity related to false information [20].

The proliferation of online open source information during the Covid-19 crisis highlighted the challenge for OSINT credibility. Corroboration remains a key part of the process to investigating the provenance of OSINT, being hindered by the 'echo' effect, whereby a source appears highly credible because of multiple information sources proffering the same information which actually derives from a single source of uncorroborated information. The authenticity of the single source is thereby artificially inflated by the high volume of clicks, comments and shares it receives online [21].

During March 2022, as the Russian invasion of Ukraine entered its third week, the battle for hearts and minds — via social media posts, viral videos, and outright propaganda — entered a new phase. According to five Western national security and disinformation officials, with Kremlin-backed news outlets being banned across the European Union and platforms like Facebook and Twitter reducing their reach worldwide, Moscow shifted its game plan to focus increasingly on its domestic audience, as well as the Russian-speaking diaspora in neighbouring countries and those farther afield [22]. Moscow's narratives about its invasion continued to evolve after its goal of toppling Kyiv within a week failed and its campaign turned to entrenched warfare, with civilians increasingly targeted as part of the wider aggression.

The underground information campaigns have pitted Russian digital actors against their Ukrainian propagandists, with other groups — some motivated by political agenda, others by money — also throwing their own hats in the ring [23]. Yet as Google, Facebook, Twitter and TikTok actively removed, or demoted, content associated with Moscow, new strategies have begun to bubble to the surface. On TikTok, for instance, multiple Russian-language influencers parroted the same script in defence of Ukraine's invasion. On Instagram, a network of pro-Kremlin accounts, posing as local news outlets in Poland, spread false claims that Ukrainian refugees were attacking Poles after fleeing the war zone. Across Telegram — a social media network that is now a battleground between pro-Ukrainian and pro-Russian camps — channels with tens of thousands of subscribers have posted grainy war footage of alleged atrocities or of military vehicles heading toward Kyiv, though much of this content was either taken out of context or reused from previous conflicts. Yet it has

been highly coordinated, according to fact-checking groups tracking this activity, and significantly amplifies the challenges and complexity of corroborating OSINT.

Corroborating OSINT, as with verifying all other forms of intelligence gathered by traditional methods, is a key component for turning OSINF into OSINT. The difference between basic and best OSINT fundamentally lies within the analytical process. Verification stages of OSINT analysis can turn OSINT into validated OSINT, which has a much higher degree of credibility, and although capturing OSINT is highly efficient at the front-end of the process, the back-end corroboration and analysis requires increasingly robust, rigorous, and intensive resource to validate and verify its credibility.

The verification processing phases of OSINT faces many new challenges, not just from malicious misinformation campaigns, but also processing big data in less-structured formats [24]. The abundance of data complicates the verification of OSINT, but open-source intelligence analysts today have access to a myriad of different analytical tools and technologies to support their efforts. Although commercial off-the-shelf tools can serve the interests of the intelligence agency and law enforcement community, they are rarely a perfect match, and many tools have extremely limited utility for intelligence analysis because they are not designed for its purposes [25]. While OSINT has been revolutionised over the past two decades it remains underutilised in Defence because of the difficulties in understanding dynamic OSINT sources and methods, particularly social media platforms [26]. Moreover, senior decision-makers, especially those in command and control of dynamic operations, require increasing levels of confidence that their OSINT operatives are able to extract and validate fact from fiction if the important OSINT discipline is to be valued alongside other traditional forms of intelligence collection.

Next generation

Contemporary OSINT is a result of the convergence of current technologies which continues to develop at pace. The OSINT discipline will not stand still, and other new and emerging technologies will continue to augment and amplify OSINT possibilities. The next generation of OSINT tools and techniques will largely depend upon the development of the internet and there is great value for all in national security intelligence-related disciplines to recognise where the web is going, both for the user and for analytic opportunities. What technology experts deem the "Semantic Web", the next generation of OSINT, widely regarded as the third wave of OSINT, will have to possess the capabilities for direct and indirect machine processing of data, machine learning, and automated reasoning [27]. Thus, the third generation of OSINT will likely be built on machine learning and automated reasoning, having to deal with pervasive encryption denying access to OSINF, and may focus on collection and dissemination of big data. Moreover, the growing appetite to live-stream online content, which presents very real operational challenges for security forces, and when combined with Virtual Reality (VR), Augmented Reality (AR) and Artificial Intelligence (AI), the next generation of OSINT will witness a substantial transformation in capacity and capability [28].

The next generation of OSINT will also be better equipped to tackle the curse of compromise via misinformation and fake news. Advancements in developments to cross-check, corroborate and analyse data provenance will be revolutionised to the extent that experts indicate that the credibility and integrity of validated OSINT could reach evidential standard requirements. Traditionally, intelligence and evidence are fundamentally different, and while evidence could always provide some degree of intelligence the reverse was not the case. If OSINT is to be relied on, evidentially it will need to meet the same forensic standards and clear the same legal hurdles as any other forms of evidence. Therefore, all in authority need to be aware of these standards and hurdles from the outset – and to ensure so far as practicable – that they are in a position to address them. At its heart, the principal difference between intelligence and evidence remains purposive [29]. The purpose of intelligence is wide-ranging, almost undefined, and can cover an array of activities. Evidence, on the other hand, has one function: to assist a court or finder of fact to determine a matter that has come before it. But such are the technical possibilities and ambitions of OSINT, that being set against a regulated framework, the potential evidential uses for the next generation of OSINT are vast.

Given the scale and scope of new and emerging opportunities offered by the next generation of OSINT tools and techniques, all in authority must dedicate themselves to increasing OSINT expertise and developing new approaches to harness the innovations of OSINT that have the potential to transform Defence intelligence structures. To simply

ignore or dismiss the positive benefits of OSINT would be both misplaced and unwise. Harnessing the full power of OSINT would be a game-changer for national security policymakers, professionals, and practitioners. But all in authority must acknowledge the inconvenient truth that even integrating the next generation of OSINT into traditional disciplines, intelligence will still rarely tell you all you need to know.

Despite OSINT advancements, difficult decisions must still be made on the basis of intelligence which is fragmentary and difficult to interpret. In summary, some intelligence will still be gold, some will still be dross, and all of it requires rigorous validation, analysis and assessment. When intelligence is gold it shines and illuminates, saves lives, protects nations, and informs policy [30]. When identified as dross it needs to be rejected: that will take some confidence. OSINT of the future will still require intelligence professionals of integrity not only to collect it but also to prioritise, sift, judge, and use it. Much has been accomplished in the professionalisation of OSINT over recent years but there remains much more to do to convince all senior leaders in national security that the current and future generations of OSINT offers the panacea predicted by technology experts.

Future challenges and Opportunities

The world is being reinvented by open sources and security forces have been part of a major shift towards harnessing the capacity of online information in the public domain to enrich their intelligence gathering activities. Such developments need to continue at pace and assessing the full impact of OSINT on the broader intelligence practices focusing upon the ability to better deliver safety and security to the public must be further explored. When the intelligence community is seeking new and innovative ways in which to cut costs, amplify output and digitalise operating practices through investment in the latest technology, the opportunities offered by OSINT must be considered as part of Defence transformation programmes.

Harnessing the power of OSINT presents a unique opportunity to keep one step ahead of adversaries, but the seamless integration with traditional intelligence practices also presents numerous challenges. The interrogation of increasingly large data sets raises acute concerns for capacity, together with the ability to share and analyse large volumes of data. The introduction of OSINT capabilities will require the rigorous review of existing intelligence models and associated processes to ensure practitioners have the latest tools and training provision to maximise the full potential of OSINT.

While OSINT presents many opportunities, any developments to gather open sources of information in an increasingly digitalised world, will have to be guided by the state's relationship with its citizenry and the law. Citizens remain cautious and suspicious of access to, and use of, their online data. Any damage to public trust is counter-productive to contemporary security practices and just because the state may have developed the technology and techniques to harness OSINT does not necessarily mean that it should. The legal, moral and ethical challenges to OSINT must be fully explored alongside civil liberties and human rights yet balanced with protecting the public from all manner of security hazards. All in authority must also avoid at all costs the increased use of OSINT as a knee-jerk reaction to placate the public and the press following crisis events.

Experience over recent years shows that in the aftermath of crisis events political stakes are high: politicians and legislators fear being seen as lenient or indifferent and often grant the executive broader authorities without thorough debate. New special provisions intended to be temporary turn out to be permanent. Although government may frame their new provisions in terms of a choice between security and liberty, sometimes the loss of liberty is not necessarily balanced by the gain in safety, and the measures introduced become counter-productive.

Future challenges and Opportunities

The application of OSINT should be carefully considered in a post-COVID-19 world and not misused, as it may lead to a long-term damage of relations with citizens and communities due to the over-extended and inappropriate use of OSINT capabilities. OSINT must not be introduced by stealth either, but through informed dialogue, passing though the due democratic process of government. Following the Russian invasion of Ukraine, it is anticipated that European citizens are more likely to support robust measures used by their government's national security agencies that are necessary, appropriate, and proportionate. That being said, many citizens, and senior politicians for that matter, remain to be convinced that harnessing the full future power of OSINT, amplified by the next generation of AI, is an essential part of protecting their nations health, security and economic well-being.

Andrew Staniforth is Director of SAHER (Europe) OÜ & NOTIONES Project Senior Researcher

David Fortune is Director of SAHER (Europe) OÜ & NOTIONES Project Senior Researcher

References

[1] Richards, J *The Art and Science of Intelligence Analysis* (2010) Oxford

[2] Akhgar, B Bayerl, S P, & Sampson F *Open-Source Intelligence Investigation – From Strategy to Implementation* (2016) Springer: London

[3] Staniforth, *A Transforming Intelligence in the Digital Age – Next Generation Open-Source Intelligence* (13 July 2020) Defence iQ: London [Online] Available at: *https://www.defenceiq.com/cyber-defence-and-security/whitepapers/transforming-intelligence-in-the-digital-age-next-generation-osint* (Accessed 2/4/2022)

[4] Federal Bureau of Investigation, Intelligence Branch, Intelligence Collection Disciplines, *https://www.fbi.gov/about/leadership-and-structure/intelligence-branch*

[5] Manningham-Buller, Dame E *The international terrorist threat and the dilemmas in countering it - Speech by the Director General of the Security Service at the Ridderzaal, Binnenhof, The Hague, Netherlands* (1/10/05) [Online] Available at: *https://www.mi5.gov.uk/news/the-international-terrorist-threat-and-the-dilemmas-in-countering-it#sthash.JUti82Pt.dpuf* (Accessed 1/4/22)

[6] Rt Hon The Lord Butler of Brockwell, *Review of Intelligence on Weapons of Mass Destruction, Report of a Committee of Privy Counsellors* (14/7/04) London: The Stationery Office [Online] Available at: *http://news.bbc.co.uk/nol/shared/bsp/hi/pdfs/14_07_04_butler.pdf* (Accessed 10/3/22)

[7] Blum, I & H J, Williams *Defining Second Generation Open-Source Intelligence (OSINT) for the Defence Enterprise* (2018) RAND Corporation [Online] Available at: *https://www.rand.org/pubs/research_reports/RR1964.html* (Accessed 23/2/22)

[8] Blum, I & H J, Williams *Defining Second Generation Open-Source Intelligence (OSINT) for the Defence Enterprise* (2018) RAND Corporation [Online] Available at: *https://www.rand.org/pubs/research_reports/RR1964.html* (Accessed 10/3/22)

[9] Ernst & Young [Online] Available at: *https://www.ey.com/en_gl/forensic-integrity-services/how-to-identify-fact-from-fiction-during-the-covid-19-pandemic-and-beyond* (Accessed 28/3/22)

[10] Akhgar, B Bayerl, S P, & Sampson F *Open-Source Intelligence Investigation – From Strategy to Implementation* (2016) Springer: London

References

[11] Manningham-Buller, Dame E *The international terrorist threat and the dilemmas in countering it - Speech by the Director General of the Security Service at the Ridderzaal, Binnenhof, The Hague, Netherlands* (1/10/05) [Online] Available at: https://www.mi5.gov.uk/news/the-international-terrorist-threat-and-the-dilemmas-in-countering-it#sthash.JUti82Pt.dpuf (Accessed 2/4/22)

[12] Blum, I & H J, Williams *Defining Second Generation Open-Source Intelligence (OSINT) for the Defence Enterprise (2018) RAND Corporation* [Online] Available at: https://www.rand.org/pubs/research_reports/RR1964.html (Accessed 12/3/22)

[13] Akhgar, B Bayerl, S P, & Sampson F *Open-Source Intelligence Investigation – From Strategy to Implementation* (2016) Springer: London

[14] Akhgar, B Bayerl, S P, & Sampson F *Open-Source Intelligence Investigation – From Strategy to Implementation* (2016) Springer: London

[15] Ernst & Young [Online] Available at: https://www.ey.com/en_gl/forensic-integrity-services/how-to-identify-fact-from-fiction-during-the-covid-19-pandemic-and-beyond (Accessed 15/2/22)

[16] Ofcom *Half of UK adults exposed to false claims about coronavirus* (9/4/20) [Online] Available at: https://www.ofcom.org.uk/about-ofcom/latest/features-and-news/half-of-uk-adults-exposed-to-false-claims-about-coronavirus (Accessed 11/3/22)

[17] Sky News Coronavirus: *Almost half of adults exposed to fake COVID-19 news* (9/4/20) [Online] Available at: https://news.sky.com/story/coronavirus-almost-half-of-adults-exposed-to-fake-covid-19-news-11970811 (Accessed 9/3/22)

[18] Ofcom *Half of UK adults exposed to false claims about coronavirus* (9/4/20) [Online] Available at: https://www.ofcom.org.uk/about-ofcom/latest/features-and-news/half-of-uk-adults-exposed-to-false-claims-about-coronavirus (Accessed 3/3/22)

[19] Ernst & Young [Online] Available at: https://www.ey.com/en_gl/forensic-integrity-services/how-to-identify-fact-from-fiction-during-the-covid-19-pandemic-and-beyond (Accessed 28/3/22)

[20] Web Foundation *Three steps you can take to help fight viral Covid-19 misinformation* (2/4/20) [Online] Available at: https://webfoundation.org/2020/04/three-steps-you-can-take-to-help-fight-viral-covid-19-misinformation/ (Accessed 5/3/22)

References

[21] Akhgar, B Bayerl, S P, & Sampson F *Open-Source Intelligence Investigation – From Strategy to Implementation* (2016) Springer: London

[22] Scott, M As war in Ukraine evolves, so do disinformation tactics (10/3/22) Politico [Online] Available at: *https://www.politico.eu/article/ukraine-russia-disinformation-propaganda/* (Accessed 3/4/22)

[23] Scott, M As war in Ukraine evolves, so do disinformation tactics (10/3/22) Politico [Online] Available at: *https://www.politico.eu/article/ukraine-russia-disinformation-propaganda/* (Accessed 3/4/22)

[24] Blum, I & H J, Williams Defining Second Generation Open-Source Intelligence (OSINT) for the Defence Enterprise (2018) RAND Corporation [Online] Available at: *https://www.rand.org/pubs/research_reports/RR1964.html* (Accessed 30/1/22)

[25] Colquhoun, C A Brief History of Open-Source Intelligence (14/7/16) Bellingcat [Online] Available at: *https://www.bellingcat.com/resources/articles/2016/07/14/a-brief-history-of-open-source-intelligence/?source=post_page----------*

[26] Blum, I & H J, Williams Defining Second Generation Open-Source Intelligence (OSINT) for the Defence Enterprise (2018) RAND Corporation [Online] Available at: *https://www.rand.org/pubs/research_reports/RR1964.html* (Accessed 5/2/22)

[27] Blum, I & H J, Williams Defining Second Generation Open-Source Intelligence (OSINT) for the Defence Enterprise (2018) RAND Corporation [Online] Available at: *https://www.rand.org/pubs/research_reports/RR1964.html* (Accessed 18/2/22)

[28] Colquhoun, C A Brief History of Open-Source Intelligence (14/7/16) Bellingcat [Online] Available at: *https://www.bellingcat.com/resources/articles/2016/07/14/a-brief-history-of-open-source-intelligence/?source=post_page----------*

[29] Akhgar, B Bayerl, S P, & Sampson F *Open-Source Intelligence Investigation – From Strategy to Implementation* (2016) Springer: London

[30] Manningham-Buller, Dame E The international terrorist threat and the dilemmas in countering it (Speech by the Director General of the Security Service at the Ridderzaal, Binnenhof, The Hague, Netherlands) (1/10/05) [Online] Available at: *https://www.mi5.gov.uk/news/the-international-terrorist-threat-and-the-dilemmas-in-countering-it*

Disclaimer

This document contains material which is copyright of certain NOTIONES consortium parties. All NOTIONES consortium parties have agreed to the full publication of this document.

Neither the NOTIONES consortium as a whole, nor any certain party of the NOTIONES consortium warrants that the information contained in this document is capable of use, or that use of the information is free from risk, and accepts no liability for loss or damage suffered by any person using the information.

The contents of this document are the sole responsibility of the NOTIONES consortium and can in no way be taken to reflect the views of the European Commission. The European Commission is not responsible for any use that may be made of the information it contains.

The commercial use of any information contained in this document requires a license from the proprietor of that information. For information and permission requests, contact the NOTIONES project coordinator Erkuden Rios Velasco (TECNA) at *Erkuden.Rios@tecnalia.com*.

The content of this document may be freely distributed, reproduced or copied as content in the public domain, for non-commercial purposes, at the following conditions:

a) it is requested that in any subsequent use of this work the NOTIONES project is given appropriate acknowledgement with the following suggested citation:

"White paper "Open-Source Intelligence (OSINT) – Next generation challenges, priorities, and opportunities" (2022), Authors: Andrew Staniforth and David Fortune, Directors, SAHER (Europe) OÜ, produced under the NOTIONES project, which has received funding from the European Union's Horizon2020 Programme for research and innovation under grant agreement No. 101021853. Available at: *Home - Notiones*

b) this document may contain material, information, text, and/or images created and/or prepared by individuals or institutions external to the NOTIONES consortium, that may be protected by copyright. These sources are mentioned in the "References" section, in captions and in footnotes. Users must seek permission from the copyright owner(s) to use this material.

NOTIONES

Coordinator

tecnalia

Scientific Technical Coordinator

Zanasi & Partners
Security Research and Advisory

Project Security Officer

Academic | Think-Tanks | Research

LAUREA

ISS

DRI
Defence Research Institute

ICSA

Bar-Ilan University

APRE

Technology Providers

VTT

expert.ai

SAHER EUROPE

MARKETSCAPE

Tecoms

SYNYO

Practitioners

Financial Intelligence Unit

ISEM INSTITUTE
INTERNATIONAL SECURITY AND EMERGENCY MANAGEMENT INSTITUTE

Polisen

Keeping People Safe

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101021853.