NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

21ST CENTURY OPEN-SOURCE INTELLIGENCE AND LAW ENFORCEMENT UTILIZATION

by

Andrew J. Horos

March 2023

Co-Advisors: Lauren Wollman (contractor)
Kathryn J. Aten

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE	*Form Approved OMB No. 0704-0188*

1. AGENCY USE ONLY *(Leave blank)*	**2. REPORT DATE** March 2023	**3. REPORT TYPE AND DATES COVERED** Master's thesis

4. TITLE AND SUBTITLE 21ST CENTURY OPEN-SOURCE INTELLIGENCE AND LAW ENFORCEMENT UTILIZATION	**5. FUNDING NUMBERS**
6. AUTHOR(S) Andrew J. Horos	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000	**8. PERFORMING ORGANIZATION REPORT NUMBER**
9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A	**10. SPONSORING / MONITORING AGENCY REPORT NUMBER**

11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.

12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release. Distribution is unlimited.	**12b. DISTRIBUTION CODE** A

13. ABSTRACT (maximum 200 words)

American law enforcement relies heavily on open-source intelligence (OSINT) to effectively protect the citizens and communities that they serve. Because of technological advancements, this form of intelligence has rapidly evolved, making it difficult for law enforcement to efficiently collect, analyze, and disseminate this information. This thesis reviews current law enforcement use of open-source intelligence and conducts a case study on the use of open-source intelligence prior to and during the initial Ukraine invasion by Russian military forces. The research identifies social media open-source intelligence as the most heavily relied-upon form and a lack of collection standards, low public sentiment, and law enforcement culture as obstacles to its full potential use. Unprecedented crowdsourcing and high positive public sentiment toward Ukraine during the invasion were highlighted as key factors to success in defending against invading Russian forces. Forming a national OSINT standards committee, improving public sentiment to encourage public crowdsourcing, and forming a national OSINT database would increase law enforcement open-source intelligence effectiveness.

14. SUBJECT TERMS OSINT, intelligence, open source intelligence, law enforcement, social media, Ukraine, Russia	**15. NUMBER OF PAGES** 111
	16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT Unclassified	**18. SECURITY CLASSIFICATION OF THIS PAGE** Unclassified	**19. SECURITY CLASSIFICATION OF ABSTRACT** Unclassified	**20. LIMITATION OF ABSTRACT** UU

NSN 7540-01-280-5500

Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. 239-18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release. Distribution is unlimited.

21ST CENTURY OPEN-SOURCE INTELLIGENCE AND LAW ENFORCEMENT UTILIZATION

Andrew J. Horos
Lieutenant Harbor Patrol Unit/Air Support Unit,
Washington, DC, Metropolitan Police Department
BBA, Frostburg State University, 2006

Submitted in partial fulfillment of the
requirements for the degree of

**MASTER OF ARTS IN SECURITY STUDIES
(HOMELAND SECURITY AND DEFENSE)**

from the

**NAVAL POSTGRADUATE SCHOOL
March 2023**

Approved by: Lauren Wollman
Co-Advisor

Kathryn J. Aten
Co-Advisor

Erik J. Dahl
Associate Professor, Department of National Security Affairs

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

American law enforcement relies heavily on open-source intelligence (OSINT) to effectively protect the citizens and communities that they serve. Because of technological advancements, this form of intelligence has rapidly evolved, making it difficult for law enforcement to efficiently collect, analyze, and disseminate this information. This thesis reviews current law enforcement use of open-source intelligence and conducts a case study on the use of open-source intelligence prior to and during the initial Ukraine invasion by Russian military forces. The research identifies social media open-source intelligence as the most heavily relied-upon form and a lack of collection standards, low public sentiment, and law enforcement culture as obstacles to its full potential use. Unprecedented crowdsourcing and high positive public sentiment toward Ukraine during the invasion were highlighted as key factors to success in defending against invading Russian forces. Forming a national OSINT standards committee, improving public sentiment to encourage public crowdsourcing, and forming a national OSINT database would increase law enforcement open-source intelligence effectiveness.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

I. 21ST CENTURY OPEN-SOURCE INTELLIGENCE AND LAW ENFORCEMENT UTILIZATION 1

A. PROBLEM STATEMENT 1
B. RESEARCH QUESTION 2
C. LITERATURE REVIEW 2
1. Traditional OSINT and Public Information Technology Advances 2
2. 21st Century OSINT—Benefits and Disadvantages 4
3. Conclusion 8
D. RESEARCH DESIGN 8

II. BACKGROUND: THE EVOLUTION OF OPEN-SOURCE INTELLIGENCE 11

A. AMERICAN OSINT HISTORY 11
B. TWITTER REVOLUTION 12
C. MODERN OSINT COLLECTION METHODS 15

III. CASE STUDY: OSINT USE IN RUSSIAN INVASION 17

A. UKRAINE/RUSSIA 17
B. OSINT PRE-INVASION 19
C. OSINT INVASION 36

IV. LAW ENFORCEMENT OSINT USE 47

A. 21ST CENTURY LAW ENFORCEMENT SOCIAL MEDIA OSINT 48
B. CHALLENGES 51
1. Data 51
2. Public Sentiment 52
3. Law Enforcement Culture 55
4. Lack of National Standards 56

V. FINDINGS AND DISCUSSION 59

A. UKRAINE PUBLIC SUPPORT 59
B. UKRAINE OSINT DATABASE 62
C. LAW ENFORCEMENT COLLECTION STANDARDS 65

VI. RECOMMENDATIONS AND CONCLUSION 69
A. RECOMMENDATIONS 69
1. Solicit Public Crowdsourcing 69
2. National OSINT Database 70
3. National Collection Standards Committee 72
B. LIMITATIONS 74
C. FURTHER RESEARCH TO BE CONDUCTED 75
D. CONTRIBUTION 76
E. SUMMARY 76

LIST OF REFERENCES 79

INITIAL DISTRIBUTION LIST 89

LIST OF FIGURES

Figure 1. Iran Twitter screenshot 13

Figure 2. @4emberlen tweet 19

Figure 3. @gfusfus tweet 20

Figure 4. @herooftheday tweet 21

Figure 5. @JC_Monitoring/@chrisdneumann tweet 22

Figure 6. @marli.litova9003 TikTok 23

Figure 7. @JC_Monitoring convoy tweet 24

Figure 8. @JC_Monitoring satellite tweet 24

Figure 9. Russian media 26

Figure 10. @PLnewstoday tweet 27

Figure 11. @MarQs_ tweet 28

Figure 12. Bellingcat IED reconstruction 29

Figure 13. Natanazart TikTok 30

Figure 14. @YWNReporter tweet 31

Figure 15. @YWNReporter street lights 32

Figure 16. @YWNReporter telephone poles 32

Figure 17. @ReddishCat1 tweet 33

Figure 18. @hakan_pishot tweet 33

Figure 19. Satellite image Golovchino 34

Figure 20. Satellite image Malakeevo 35

Figure 21. ISW map 37

Figure 22. @RALee85 tweet 38

Figure 23. @RALee85 Russian tanks 39

Figure 24. @wargonzoo tweet 41
Figure 25. @tinso_tweet 42
Figure 26. @ZelenskyyUa..... 43
Figure 27. @Polk_Azov tweet 44
Figure 28. @JackDetsch tweet..... 45
Figure 29. Agency use of social media 49
Figure 30. 2020 American confidence in police 53
Figure 31. Eyes on Russia 63
Figure 32. Liveuamap..... 64
Figure 33. Law enforcement per capita spending 67

LIST OF TABLES

Table 1. 2009 YouTube views 14

Table 2. Social media and L.E. challenges 58

Table 3. Top 10 Ukraine hashtags 60

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

BOLO	be on the lookout
BWC	body-worn camera
COMINT	communications intelligence
MDT	mobile data terminal
NATO	North Atlantic Treaty Organization
NCIC	National Crime Information Center
NPCC	National Police Chief's Commission
OSCE	Organization for Security and Co-Operation in Europe
OSINT	open-source intelligence
OSS	Office of Strategic Services
SIGINT	signals intelligence
SOCMINT	social media intelligence
UAV	unmanned aerial vehicle

THIS PAGE INTENTIONALLY LEFT BLANK

EXECUTIVE SUMMARY

Law enforcement agencies have the responsibility of using every tool available to them to protect and serve their communities and citizens. Intelligence to proactively prevent violent crimes is a crucial resource that must be effectively optimized in order to accomplish this task. Open-source intelligence (OSINT) is heavily relied upon by law enforcement agencies around the nation to provide accurate, real-time information that can aid officers in preventing violent crime. Although law enforcement has been using this intelligence for centuries, the rapid development and expansion of the internet and social media platforms have increased the amount of information and reliance on open-source intelligence.

This thesis researches the background of open-source intelligence (OSINT) and the current use of OSINT by law enforcement and conducts a case study of OSINT use prior to and during the initial Ukraine invasion by Russian military forces. The use of open-source intelligence during the Ukraine invasion in February 2022 yielded unprecedented beneficial results in preparation against Russian forces. Although this invasion is an international military conflict, it was selected as a case study because it demonstrates the effective use of evolving modern-day social media open-source intelligence. The mass amounts of data revolving around the conflict were analyzed in detail and proactive defensive maneuvers may be attributed to this intelligence.

The history of the United States government using open-source intelligence in war can be traced back to WWI. Traditional sources included newspapers, magazines, and print media, which were used to counter enemy military tactics during various U.S. conflicts. The creation of the internet changed open-source intelligence by creating platforms to share information around the world instantaneously and without restrictions. The influence of social media was globally highlighted during the Iranian presidential election protests in 2009. Because of Twitter, Iranian citizens were still able to communicate with the world, despite their government's attempts to shut down communication outside of the country.

In December 2021, thousands of Russian troops began moving and staging on Ukraine-bordering Russian land and Russian-occupied Crimea. By January and February of 2022, global news outlets were covering the impending conflict and highlighting President Putin's actions and speeches. The Ukraine-Russia conflict had gathered the world's attention and was "trending" on social media platforms, which resulted in millions of citizens viewing and "sharing" related posts. Pictures, videos, and other information were posted on social media by Russian and Ukrainian citizens and was analyzed by others around the world. Satellite imagery and Google Maps were used to pinpoint staging locations of Russian military assets, disprove Russian mal-information, and counter Russian military tactics.

United States law enforcement has several identified obstacles that have prevented the full utilization of OSINT including the massive amounts of data to be analyzed, low public sentiment around law enforcement technology, a culture of information hoarding, and a lack of national collection standards. The case study showed that, because the public sentiment of Ukraine was so high, much of the world was willing to assist in the dissemination and analysis of social media posts. Support for Ukraine was high, and crowdsourcing was so rampant that many OSINT databases were formed to help gather intelligence in central locations. Public sentiment, crowdsourcing, and these novel OSINT databases were vital in preparing Ukraine for the Russian invasion.

This thesis makes several recommendations through researching current law enforcement OSINT use and the Ukraine case study. The first recommendation is to solicit public crowdsourcing by improving public trust and sentiment toward law enforcement technology. Highlighting and showcasing the successful use of OSINT that demonstrates proactive measures of preventing violent acts such as mass shootings would aid this effort. The second recommendation is the creation of a national OSINT database similar to other national law enforcement databases. This would centralize important intelligence that would assist law enforcement safety measures around the country.

The third recommendation is the creation of an open-source intelligence national collection standards committee. This committee would form collection standards and disseminate "best practices" to guide intelligence analysts in the most efficient and

effective collection methods. The research suggests that if implemented correctly, these recommendations would increase law enforcement's ability to improve public safety and prevent violent crimes. In conclusion, this research means to improve law enforcement's ability to use open-source intelligence to protect the citizens of the communities they serve. By increasing the amount of reliable, real-time open-source intelligence to law enforcement officers, they can more effectively preserve human life and prevent harm to civilians.

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

I want to thank my family and friends who have supported me since the beginning of this journey. My trips out West would not have been possible without the loving support of everyone around me. My Hunter and Olivia, who are my inspiration to always try my best and keep going forward, you will always be my sun and moon. I hope that one day I can inspire you as much as you inspire me on a daily basis.

I am thankful for the NPS staff and all they did for me and my cohort, constantly pushing us to be better, and fostering an environment of learning. Thank you to my advisors, Kathryn Aten and Lauren Wollman, for both encouraging my creative side and pushing me when I felt defeated. A special thank you to Marianne Taflinger. Her continual Slack messages and chapter reviews were worth way more than the coffee I brought her after lunch.

Finally, I want to thank the Washington, DC, Metropolitan Police Department and their support throughout this program. Thank you to Jessica Bress for pushing me to apply to the program, to Inspector Caron, who was always there to talk, and Assistant Chief Carroll for his endorsement and support. Thank you to the brothers and sisters whom I have been fortunate to serve next to, especially during hard times, such as the summer of 2020 and January 6th. You all will always motivate me to improve our field and make a safer environment for fellow officers and the citizens we serve.

THIS PAGE INTENTIONALLY LEFT BLANK

I. 21ST CENTURY OPEN-SOURCE INTELLIGENCE AND LAW ENFORCEMENT UTILIZATION

A. PROBLEM STATEMENT

With the rapid advancement of high-speed, real-time, open-source intelligence (OSINT), traditional law enforcement must adapt and evolve. Current law enforcement OSINT use is generally conducted in the areas of social opinion/sentiment, cyber security, and organized crime.[1] Most of this gathered intelligence is further used in criminal prosecution. While the vast array of social media platforms yields robust and extensive data, law enforcement is underutilizing this resource due to its inability to effectively gather and analyze it.

The different forms of possible collection and analysis provide safe, transparent, and practical opportunities for law enforcement that years ago would require undercover officers or criminal informants. Social media analysis allows law enforcement to identify networks of criminal or terrorist organizations. The geospatial analysis allows monitoring and studying interactions between individuals within these networks. The combination of mass open-source data and efficient collection and analysis of this data creates real-time, evolving information on an individual or group of individuals.[2]

The Russian invasion of Ukraine in late February of 2022 is a model of high-fidelity OSINT utilization on the world stage. In the weeks prior to the invasion, open-sourced intelligence was being utilized by government officials. This information was vast and varied from overhead satellite images of Russian army staging locations to "live streaming" posts of Ukrainian citizens training to fire weapons. The information gathered and analyzed was on numerous different platforms and was data-sourced from citizens posting on social media.

[1] Javier Pastor-Galindo et al., "The Not Yet Exploited Goldmine of OSINT: Opportunities, Open Challenges and Future Trends," *IEEE Access* 8 (2020): 10282–304, https://doi.org/10.1109/ACCESS.2020.2965257.

[2] Pastor-Galindo et al.

The use of open-source intelligence by the Ukrainian government and military strategists highlights two strategic and tactical factors of social media OSINT. Crowdsourcing occurred on an unparalleled level because Ukraine public sentiment was high prior to the Russian invasion, resulting in detailed analysis of the overwhelming amount of information from various platforms. The access to social media intelligence was easier due to the formation of databases that gathered all relevant and related posts into central locations. Increasing public sentiment and trust in law enforcement's use of social media open-source intelligence and forming central databases for OSINT will increase law enforcement's ability to protect the public.

B. RESEARCH QUESTION

What can U.S. law enforcement learn from the Ukrainian use of "high fidelity" open-source intelligence?

C. LITERATURE REVIEW

While law enforcement organizations began to use traditional OSINT decades ago, it is currently the most utilized source of intelligence by federal, state, and local law enforcement agencies. Recent research explores the potential use, advantages, and disadvantages of modern OSINT for state and local law enforcement. This existing research suggests that OSINT can provide benefits to law enforcement. It also suggests, however, that the proliferation of social media, from which analysts create OSINT, has outpaced law enforcement's ability to form related policy, and thus, law enforcement's ability to employ OSINT. Varying interpretations of what defines OSINT and a lack of national collection standards hamper the full employment of this resource.

1. Traditional OSINT and Public Information Technology Advances

The early use of OSINT can be traced back centuries; in fact, the use of OSINT began with the introduction of the printing press. Ungureanu provides an early example of OSINT: in 1865, Otto von Bismark's spy Wilhelm Steiber organized a network of 45,000 individuals that provided foreign and domestic information and details about mission-

specific attacks through print media.[3] In 1870, Steiber used print to demoralize his French enemies by publishing his success and his enemies' failures.[4] As another example, Codruţa Luţai references OSINT when the former Soviet Union's military capabilities were highlighted in *Aviation Weekly*, proving valuable information to their enemies.[5] OSINT use has precedents in the far and near past. Although governments have used OSINT for centuries, the internet, specifically social media, has expanded the amount of data available for law enforcement to analyze, thus expanding the amount of OSINT. Williams and Blum claim that the increase in mobile data cellphones, combined with enhanced internet access, has driven this increase.[6] Noting that law enforcement organizations require "timely, reliable and actionable intelligence" to be successful, Akhgar and Wells claim that social media has greatly advanced the use and value of OSINT.[7] Recognizing this trend, in 2017, the UK's National Police Chief's Commission (NPCC) debated reclassifying social media intelligence (SOCMINT) into a category of intelligence of its own.[8] This discourse demonstrates the recognition of the importance and value of modern-day OSINT.

Academic research on modern OSINT and law enforcement collection of digital data and generation and use of OSINT is outdated and limited in scope. Intelligence is crucial to law enforcement operations and success so, not surprisingly, there has been considerable research by homeland defense scholars on law enforcement and intelligence. This research has explored the post-9/11 intelligence function, training of intelligence analysts, and public-private partnerships relating to intelligence fusion centers. For example, in a 2006 study, Cleary identifies best practices and policies to drive efficient

[3] Gabriel-Traian Ungureanu, "Open Source Intelligence (OSINT). The Way Ahead," *Journal of Defense Resources Management* 12, no. 1 (2021): 179, ProQuest.

[4] Ungureanu, 179.

[5] Raluca Codruţa Luţai, "Open Source Intelligence: Opportunities and Challenges," *Strategic Impact*, no. 1 (2020): 97, ProQuest.

[6] Heather J. Williams and Ilana Blum, *Defining Second Generation Open Source Intelligence (OSINT) for the Defense Enterprise* (Santa Monica, CA: RAND Corporation, 2018), 23, https://www.rand.org/pubs/research_reports/RR1964.html.

[7] Babak Akhgar and Douglas Wells, "Critical Success Factors for OSINT-Driven Situational Awareness," *European Law Enforcement Research Bulletin* Special Conference Edition Nr. 4 (2019): 67, https://bulletin.cepol.europa.eu/index.php/bulletin/article/view/332.

[8] Akhgar and Wells, 68.

sharing of intelligence to protect critical infrastructure and prevent terrorist attacks.[9] In a 2008 thesis, Green explores domestic and foreign law enforcement intelligence analyst programs and recommends training for law enforcement analysts.[10] And, in a 2007 thesis, Simeone researches "virtual public-private partnerships," and discusses how virtual information shared between law enforcement and private organizations can enhance intelligence-led policing.[11] The most recent homeland defense scholarly research was conducted in 2010 by Fresenko, who explores the potential of incorporating social media intelligence into fusion centers and law enforcement.[12] This research has greatly contributed to law enforcement's ability to capitalize vital intelligence. However, as demonstrated by the critical role OSINT played in the Russian invasion of Ukraine, OSINT-generating technology, especially social media, has expanded and continues to evolve. Law enforcement requires updated research.

2. 21st Century OSINT—Benefits and Disadvantages

Scholars draw on technology affordance theory to understand the use and benefits of technologies and define a technological affordance as the perception that a technology can make certain actions easier. As Markus and Silverexplain, a user's capabilities and action-oriented goals determine how to exploit a technological affordance.[13] Law enforcement uses modern OSINT in many ways, and Böhm and Lolagar discuss different

[9] Christopher J. Cleary, "Strategy for Local Law Enforcement Agencies to Improve Collection, Analysis and Dissemination of Terrorist Information" (master's thesis, Naval Postgraduate School, 2006), v, https://hdl.handle.net/10945/2892.

[10] Prioleau Green, "An Analysis of the Requirements and Potential Opportunities for the Future Education of Law Enforcement Intelligence Analysts" (master's thesis, Naval Postgraduate School, 2008), v, https://hdl.handle.net/10945/4235.

[11] Matthew J. Simeone, "The Integration of Virtual Public-Private Partnerships into Local Law Enforcement to Achieve Enhanced Intelligence-Led Policing" (master's thesis, Naval Postgraduate School, 2007), v, https://hdl.handle.net/10945/3207.

[12] Victoria L. Fresenko, "Social Media Integration into State-Operated Fusion Centers and Local Law Enforcement: Potential Uses and Challenges" (master's thesis, Naval Postgraduate School, 2010), v, https://hdl.handle.net/10945/4996.

[13] M. Lynne Markus and Mark S. Silver, "A Foundation for the Study of IT Effects: A New Look at DeSanctis and Poole's Concepts of Structural Features and Spirit," *Journal of the Association for Information Systems* 9, no. 10/11 (2008): 622, ProQuest.

law enforcement actions using OSINT.[14] In 2016, over 500 police agencies participated in a study conducted by the International Association of Chiefs of Police and the Urban Institute. The study showed that 91% of agencies use social media to relay public safety information, 76% of agencies request crime tips on social media, and 70% use social media to gather intelligence for criminal investigations.[15] The Department of Justice and Police Executive Research Forum reports that law enforcement uses social media for suspect tracking, identifying criminal networks, evidence collection, and civil unrest preparation.[16]

Most literature identifies similar benefits for law enforcement regarding OSINT. The access and the ease of sharing intelligence efficiently and immediately with other stakeholders constitutes its key benefit within the law enforcement community. Ungureanu notes this advantage, declaring that technology from the early 2000s has resulted in real-time, efficient communication flow between consumers in the intelligence community without clearance restrictions.[17] Additionally, Qusef and Alkilani assert that the return on investment of OSINT collection outweighs that of classified intelligence-gathering, making it more useful.[18] Access to information is free, making it extremely cost-effective compared to traditional intelligence methods. Thus, OSINT may be particularly useful to agencies that are limited in resources.

Although OSINT provides many potential benefits to law enforcement, the exponential increase in publicly available data compounds the complexity of its analysis and law enforcement's use of OSINT. Best identifies multiple challenges in data collection including identifying and retrieving information, classifying and organizing information,

[14] Isabelle Böhm and Samuel Lolagar, "Open Source Intelligence," *International Cybersecurity Law Review* 2, no. 2 (2021): 319–22, https://doi.org/10.1365/s43439-021-00042-7.

[15] KiDeuk Kim, Ashlin Oglesby-Neal, and Edward Mohr, *2016 Law Enforcement Use of Social Media Survey* (Washington, DC: International Association of Chiefs of Police and the Urban Institute, 2017), 3, https://www.urban.org/research/publication/2016-law-enforcement-use-social-media-survey.

[16] Office of Community Oriented Policing Services and Police Executive Research Forum, *Social Media and Tactical Considerations for Law Enforcement* (Washington, DC: Office of Community Oriented Policing Services, 2013), 17–26, https://cops.usdoj.gov/RIC/Publications/cops-p261-pub.pdf.

[17] Ungureanu, "Open Source Intelligence," 181.

[18] Abdallah Qusef and Hamzeh Alkilani, "The Effect of ISO/IEC 27001 Standard over Open-Source Intelligence," *PeerJ Computer Science*, 2022, 8, https://doi.org/10.7717/peerj-cs.810.

and extracting specific intelligence data.[19] As Codruţa Luţai notes, social media has turned viewers and consumers into "generators" who record and film everyday life; the extreme abundance of data complicates collection and analysis processes.[20]

Negative public sentiment surrounding government collection of personal information is a further obstacle to law enforcement's use of OSINT. Ivan et. al find that the biggest challenge to law enforcement use of social media intelligence is the public matter of confidentiality and consent, specifically the "identification of the boundary between what is public and what is private."[21] Further, Pastor-Galindo et al. note that information available to the public can still be considered sensitive and can have negative reputational effects on individuals.[22] However, this sentiment is not shared by all. According to Leibowitz, many school districts now subscribe to services that monitor students' social media posts for alarming material. Threatening posts are reported to the school, then subsequently to the local police.[23] This example shows that, in some circumstances, the public supports the collection and use of personal information to enhance public safety.

The rapidly evolving technological advances and public resistance to law enforcement's exploitation of social media data and modern OSINT lead to inconsistent collection policies. Tagtekin finds no consistent standards in OSINT collection, leaving intelligence officers without guidelines and boundaries to conduct research; policy development by individual agencies leads to different standards for OSINT collection

[19] Clive Best, "Challenges in Open Source Intelligence," in *2011 European Intelligence and Security Informatics Conference* (2011 European Intelligence and Security Informatics Conference, IEEE, 2011), 58–62, https://doi.org/10.1109/EISIC.2011.41.

[20] Codruţa Luţai, "Open Source Intelligence," 98.

[21] Adrian Liviu Ivan et al., "Social Media Intelligence: Opportunities and Limitations," *CES Working Papers* 7, no. 2A (2015): 507, ProQuest.

[22] Javier Pastor-Galindo et al., "The Not Yet Exploited Goldmine of OSINT: Opportunities, Open Challenges and Future Trends," *IEEE Access* 8 (2020): 10301, https://doi.org/10.1109/ACCESS.2020.2965257.

[23] Aaron Leibowitz, "Could Monitoring Students on Social Media Stop the Next School Shooting?," *New York Times*, September 6, 2018, sec. U.S., https://www.nytimes.com/2018/09/06/us/social-media-monitoring-school-shootings.html.

across agencies at the state and local levels.[24] A lack of consistent policies between agencies and exclusive, individual OSINT policies create inconsistent intelligence collected by the different agencies.

Variance in collection standards is at least partially driven by the lack of an agreed upon the definition of OSINT. For example, sources in the intelligence community adopt the OSINT definition of the Office of the Director of National Intelligence: "intelligence produced from publicly available information that is collected, exploited, and disseminated in a timely manner to an appropriate audience for the purpose of addressing a specific intelligence requirement."[25] "Publicly available" (non-clandestine) information consistently appears in OSINT definitions; however, the reason for collection varies. A "specific intelligence requirement" may include vast possibilities and intelligence officers or agencies can interpret "relevant information" differently. Qusef and Alkilani advise that if access to data requires specialized expertise or methods, it is not "open source."[26] This demonstrates that different logics drive different collection standards.

Additionally, the criteria for what qualifies as intelligence varies by agency. A Center for Strategic and International Studies report interprets "publicly available" as any program available for purchase by the public.[27] For example, the Israeli firm NSO Group sold foreign intelligence services that provided the capability to hack into cell phones.[28] In contrast, Qusef and Alkilani advise that if access to data requires special expertise or methods, it does not qualify as "open source."[29] These contrasting definitions demonstrate the contested nature of what qualifies as OSINT.

---

[24] Orcun Tagtekin, "Open Source Intelligence: A New Era of Information Gathering" (master's thesis, Utica College, 2014), 23, ProQuest.

[25] Williams and Blum, *Defining Second Generation Open Source Intelligence*, 4.

[26] Qusef and Alkilani, "The Effect of ISO/IEC 27001 Standard over Open-Source Intelligence."

[27] Emily Harding, *Move Over JARVIS, Meet OSCAR: Open-Source, Cloud-Based, AI-Enabled Reporting for the Intelligence Community* (Washington, DC: Center for Strategic & International Studies, 2022), 7, https://www.csis.org/analysis/move-over-jarvis-meet-oscar.

[28] Harding, 7.

[29] Qusef and Alkilani, "The Effect of ISO/IEC 27001 Standard over Open-Source Intelligence."

3. Conclusion

The usefulness of OSINT to law enforcement is a key theme in the literature. The literature also identifies multiple barriers that limit law enforcement's ability to collect social media data and generate OSINT. The literature suggests that law enforcement's ability to develop policy is outpaced by social media technologies' constant evolution and growth. In particular, the lack of national collection standards contributes to inconsistent collection policies between agencies. Research demonstrates a lack of public acceptance of OSINT collection and use by law enforcement and suggests this is a major obstacle to wider utilization. It is possible that a uniform definition and collection standard could help overcome this obstacle. The development of standards and policies for unmanned aerial vehicles (UAV) use by law enforcement can be examined to assist this research. UAVs are a 21st century technology that law enforcement has successfully adopted, and the adoption process can provide a possible framework for OSINT policy development. This research will contribute to a greater understanding of how law enforcement can better use OSINT by exploring options, obstacles, and drivers to national collection standards and making policy recommendations.

D. RESEARCH DESIGN

This thesis examines law enforcement's potential use of OSINT to identify the obstacles that agencies encounter when collecting and utilizing this intelligence form. This is accomplished through reviewing the background of law enforcement OSINT, a case analysis of the use of OSINT during the Russian invasion of Ukraine, an examination of current law enforcement agency use of OSINT, findings and conclusions, and a final integration to make recommendations for agency use of OSINT.

This thesis begins by researching the background of OSINT, comparing it to traditional sources of intelligence, and describing how OSINT and its use have evolved. Next, this thesis analyzes the use of OSINT during the Russian invasion of Ukraine focusing on the period prior to the invasion, the initial invasion, and the month preceding the initial invasion. The case study focuses on Russian, Ukraine, and U.S. use of OSINT

to understand how OSNIT was used so effectively during this period of time. Data includes reports, documents and publicly available social media posts.

Next, this thesis explores current law enforcement OSINT use and obstacles to OSINT maximization. To accomplish this, this thesis investigates OSINT collection standards and adoption, public sentiment around law enforcement technology, and law enforcement culture. Finally, it draws conclusions that will assist U.S. law enforcement OSINT use based on current identified obstacles.

THIS PAGE INTENTIONALLY LEFT BLANK

II. BACKGROUND: THE EVOLUTION OF OPEN-SOURCE INTELLIGENCE

Open-source intelligence has evolved throughout history, causing the U.S. government's perspective to evolve accordingly. This chapter discusses the role of OSINT in American history and actions the U.S. government took to effectively use this intelligence form. The chapter also examines early OSINT evolution during the "Twitter Revolution" and the current collection methods used by law enforcement.

A. AMERICAN OSINT HISTORY

The use of OSINT dates back centuries prior to the establishment of any formal intelligence-gathering organization. The current law enforcement use of OSINT can be traced to Major General William J. Donovan. Mr. Donovan attended Columbia Law School in 1905 with Franklin D. Roosevelt (FDR). Shortly after law school, Mr. Donovan fought in WWI, where he received the nation's four highest military awards, including the Medal of Honor.[30] After the war, Donovan became a successful lawyer and lobbied then-U.S. President FDR to validate his intelligence work. On July 11th, 1941, FDR created the position of "Coordinator of Information" for Mr. Donovan.

After the attack on Pearl Harbor, this department was renamed the "Office of Strategic Services" or OSS.[31] This was America's first intelligence agency, and was the precursor to what would become the CIA. The OSS' Research and Analysis Branch proved vital in the allied victory in WWII. This branch authenticated Donovan's vision of a "central all-source analysis capability," mainly demonstrating that vital intelligence could

[30] Tom Neven, "'Wild Bill' Donovan: SOF Pioneer," USSOCOM History and Research Office, last modified May 14, 2018, https://www.socom.mil/wild-bill-donovan-sof-pioneer.

[31] Cameron Colquhoun, "A Brief History of Open Source Intelligence," Bellingcat, last modified July 14, 2016, https://www.bellingcat.com/resources/articles/2016/07/14/a-brief-history-of-open-source-intelligence/.

be discovered through "papers, cables, reports, maps, journals, foreign newspapers, and other materials-laying the foundation of modern intelligence research and analysis."[32]

Crucial information now wasn't only discovered behind enemy lines but could be a combination of various sources. The OSS' Research and Analysis Branch had an entire department dedicated to open-source intelligence, and during the war, they had collections of newspapers, journals, and radio broadcastings. This department combed through the documents for photos or articles that would provide the allies with intelligence about the enemy including German obituaries and images of new battleships and aircraft.[33] The early use of OSINT by the American government in WWII and the Cold War demonstrated that vital intelligence was not required to be covertly collected. Intelligence was gathered from open-source information (newspapers, media reports) and used to counter enemy technology and tactics.

The creation and widespread use of the internet was a groundbreaking landmark for OSINT and "changed the nature of public information.[34]" Böhm and Lolagar highlight that the internet digitized print media and created a manner to share information faster with no restrictions. They state, "This is empowered by a variety of newly created public sources including personal websites, message boards, online encyclopedias, newsletters, blogs, or news groups."[35] The "newly created public spaces" are the social media platforms that are heavily relied upon by law enforcement.

B. TWITTER REVOLUTION

Social media OSINT was first highly publicized in 2009 during the Iranian presidential election protests. A 2009 BBC article titled, "Internet Brings Events in Iran to Life" highlights many of the social media platforms that were used by citizens for the first time on the global stage to protest the presidential election outcome. Twitter, Facebook,

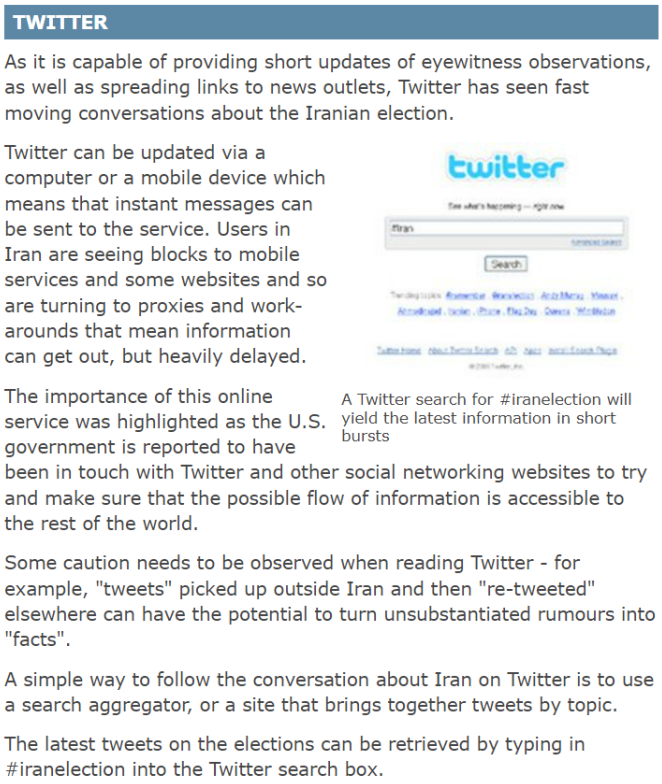
[32] "The Office of Strategic Services: America's First Intelligence Agency," CIA Museum Exhibits, accessed November 15, 2022, https://www.cia.gov/legacy/museum/exhibit/the-office-of-strategic-services-n-americas-first-intelligence-agency/.

[33] Colquhoun, "A Brief History of Open Source Intelligence."

[34] Böhm and Lolagar, "Open Source Intelligence."

[35] Böhm and Lolagar.

websites and blogs, and how to upload photos and videos are described in detail in the article like an instruction manual for first-time users: "Although there are signs that the Iranian government is trying to cut some communications with the outside world, citizen journalism appears to be thriving on the web."[36] Displaying the capabilities and power of social media and its ability to quickly spread information around the world. Figure 1 is a screenshot from the 2009 BBC article which provided a brief tutorial of the Twitter platform.



TWITTER

As it is capable of providing short updates of eyewitness observations, as well as spreading links to news outlets, Twitter has seen fast moving conversations about the Iranian election.

Twitter can be updated via a computer or a mobile device which means that instant messages can be sent to the service. Users in Iran are seeing blocks to mobile services and some websites and so are turning to proxies and work-arounds that mean information can get out, but heavily delayed.

A Twitter search for #iranelection will yield the latest information in short bursts

The importance of this online service was highlighted as the U.S. government is reported to have been in touch with Twitter and other social networking websites to try and make sure that the possible flow of information is accessible to the rest of the world.

Some caution needs to be observed when reading Twitter - for example, "tweets" picked up outside Iran and then "re-tweeted" elsewhere can have the potential to turn unsubstantiated rumours into "facts".

A simple way to follow the conversation about Iran on Twitter is to use a search aggregator, or a site that brings together tweets by topic.

The latest tweets on the elections can be retrieved by typing in #iranelection into the Twitter search box.

Figure 1. Iran Twitter screenshot [37]

According to PEW Research, 98% of Twitter links during the week of June 15–19 2009, were to the Iranian revolution, resulting in many labeling the 2009 Iranian protests

[36] *BBC*. "Internet Brings Events in Iran to Life," June 15, 2009, http://news.bbc.co.uk/2/hi/middle_east/8099579.stm.

[37] Source: *BBC*.

as the "Twitter Revolution."[38] Table 1 shows how the Iranian presidential protests dominated the YouTube Platform in June 2009.

Table 1. 2009 YouTube views[39]

Most Viewed News & Politics Videos on YouTube **June 13 – 19, 2009**
1. A video of protestors that is described as a "riot in the streets in Tehran after election day."
2. Video from Tehran where protestors clash with police
3. Segment of the June 12 edition of the Fox News television program The O'Reilly Factor where host Bill O'Reilly argues with Salon editor Joan Walsh about abortion
4. During a town hall meeting in Wisconsin, Obama writes a note for a 10-year-old girl to excuse her for missing school
5. Teaser for Michael Moore's new movie where he asks the audience to give money to help "Save our CEOs" hurt by the economic downturn

Text messaging and mobile services were cut in the country prior to and after election day; however, internet cafes and the emergence of smartphones created the flow of mass data in various forms out of the country.[40] The 2009 use of OSINT in Iran highlighted the rapid evolution of social media platforms and the mass amounts of information that could be disseminated. Social media provided every Iranian citizen with a communication method to spread real-time messages to the world's audience. Although Twitter was highlighted during this 2009 example, many other forms of social media platforms were highlighted in articles about this event. From 2009 to the beginning of the Ukraine invasion in 2022, social media platforms have expanded, and cell phone

[38] Pew Research Center, "Iran and the 'Twitter Revolution,'" *Journalism Project* (blog), June 25, 2009, https://www.pewresearch.org/journalism/2009/06/25/iran-and-twitter-revolution/.

[39] Source: Pew Research Center.

[40] Octavia Nasr, "Tear Gas and Twitter: Iranians Take Their Protests Online," *CNN*, June 15, 2009, http://www.cnn.com/2009/WORLD/meast/06/14/iran.protests.twitter/index.html.

technology has increased, resulting in more detailed, higher quality information. Law enforcement's social media OSINT relies on these platforms and related technology and will increase as information gathered from social media platforms expands and improves.

C. MODERN OSINT COLLECTION METHODS

Law enforcement has increasingly collected and disseminated SOCMINT since the Twitter Revolution. The high public usership and public reliance on these platforms for information have increased and so has law enforcement's reliance on SOCMINT. It is crucial to understand the various collection methods that are currently used by law enforcement intelligence analysts to evaluate the challenges that are related to these methods.

Social media OSINT collection is accomplished through many methods. The most heavily used are "monitoring, data mining, and research."[41] Since the internet explosion 25 years ago, this "monitoring" is conducted on internet online communities, and social networking sites (Facebook, Twitter, TikTok, etc.). OSINT monitoring also includes traditional sources such as print media, news, television, public speeches, and government reports. Social media and internet-based OSINT have become prominent due to society's reliance on this form of communication and mass consumption of social media.

Due to the vast amount of monitored data, data mining is an imperative step in OSINT collection. This is the process of "predicting outcomes by searching for anomalies, patterns, and correlations in huge data sets."[42] In the private and business world, this information can be exploited to form business strategies, reduce risks, lower expenses, and, ultimately, increase sales and profits.[43] For the law enforcement community, this

[41] Andrew Staniforth, "Police Use of Open Source Intelligence: The Longer Arm of Law," in *Open Source Intelligence Investigation: From Strategy to Implementation*, ed. Babak Akhgar, P. Saskia Bayerl, and Fraser Sampson (Cham, Switzerland: Springer International Publishing, 2016), 21–31, https://doi.org/10.1007/978-3-319-47671-1_3.

[42] Shubhnoor Gill, "12 Top Data Mining Tools in 2022," Hevo, December 21, 2021, https://hevodata.com/learn/data-mining-tools/.

[43] Gill.

information is also exploited to form strategies and reduce risks, but additionally to produce actionable intelligence that will prevent crime and violence in the communities.

The history of OSINT use by the U.S. government displays the value of this intelligence form for a century. Historical events such as WWII and the Pearl Harbor attack resulted in major actions toward expanding OSINT capabilities (i.e., the formation of OSS). The boom of the internet and the "Twitter Revolution" introduced social media capabilities to the world, expanding OSINT collection platforms to another level.

The next chapter will examine and demonstrate how OSINT aided Ukraine to forecast Russian military movements and strategies and better prepare for invasion and attacks.

III. CASE STUDY: OSINT USE IN RUSSIAN INVASION

On February 24, 2022, Russian forces invaded the country of Ukraine. The Ukrainian government successfully prepared for the invasion through open-source intelligence. Open-source commercial imagery afforded Ukraine and western officials the ability to observe Russian troops and vehicles as they mobilized leading up to the February invasion. This assault differed greatly from past conflicts because all civilians and military members carrying smartphones make activities transparent.[44] Mobile devices allow citizens to upload pictures online, geotag them, and live stream activities as they are happening.

This chapter demonstrates how the Ukrainian government used open-sourced social media intelligence to prepare for the February invasion. The chapter presents the timeline of this conflict and examines social media posts to demonstrate how open-source intelligence gained from social media posts informed responses. Because of the complexity and enormity of the Russian-Ukrainian conflict, covering the entire scope of this invasion would be impossible. Therefore, this chapter addresses only the events leading up to February 24th, 2022, the invasion, and the Siege of Mariupol. Thus, this chapter demonstrates how open-source intelligence shaped Ukrainian military preparation, exposed Russian misconduct, and debunked Russian disinformation.

A. UKRAINE/RUSSIA

The history of conflict between Ukraine and Russia dates back centuries; however, the modern conflict began in 2014 when Russia invaded and annexed Ukraine's Crimean Peninsula. The U.S. State Department labeled this invasion as an "illegal seizure," adding that "Russia manufactured a crisis, invaded and occupied Ukraine's territory in Crimea."[45]

[44] Tibi Puiu, "How Open-Source Intelligence (OSINT) Is Exposing the Ukraine War in Real-Time," *ZME Science* (blog), March 15, 2022, https://www.zmescience.com/science/news-science/open-source-intelligence-ukraine/.

[45] Julia Marnin, "What's Led up to Russia's Invasion of Ukraine? Here's a Brief Look at Their History," *MSN*, accessed October 6, 2022, https://www.msn.com/en-us/news/world/what-s-led-up-to-russia-s-invasion-of-ukraine-here-s-a-brief-look-at-their-history/ar-AAUqeFc.

On February 15, 2015, talks between Russia, Ukraine, Germany, and France resulted in a ceasefire in the Crimea conflict. A day after the ceasefire began, Russia captured the Ukrainian town of Debaltseve. By 2017, the death toll in this conflict had reached 10,000, including many civilian casualties.[46] In 2019, prisoner exchanges between the two countries occurred and by 2020, negotiations between them resulted in a ceasefire and the lowest level of combat since the beginning of the conflict.[47]

In 2021, Russia and President Putin launched a large-scale disinformation campaign claiming that Ukraine caused the Crimea conflict. In April 2021, Russian media reported a Ukrainian drone killed a young boy in the Donbas region.[48] The Organization for Security and Co-Operation in Europe (OSCE) and independent media published reports that found the youth did not die by a drone attack or any Ukrainian actions. Nonetheless, Russian media continued to report the attack and even described it as an "act of terrorism."[49] This shows President Putin and the Russian government taking incremental actions to justify increasing military actions against Ukraine.

During this Russia disinformation campaign, Russia began amassing military forces on Ukrainian borders, including 100,000 troops in the Russian-occupied Crimea.[50] By December of 2021, President Putin had deployed tens of thousands of troops on Ukrainian borders and demanded that Ukraine never be admitted to the North Atlantic Treaty Organization (NATO).[51] By February 2022, U.S. authorities estimated 190,000

[46] Bureau of Conflict and Stabilization Operations, "History of Russia's Aggression against Ukraine," U.S. Department of State, February 11, 2022, https://storymaps.arcgis.com/stories/f477e2c9a9154df3af8508ad1caef919.

[47] Bureau of Conflict and Stabilization Operations.

[48] StopFake, "Fake: A Child Died in Donbas as a Result of a Ukrainian Drone Attack (Update)" April 29, 2021, https://web.archive.org/web/20210429183210/https://www.stopfake.org/en/fake-a-child-died-in-donbas-as-a-result-of-a-ukrainian-drone-attack/.

[49] U. S. Embassy Tbilisi, "Russia Targets Ukraine with Disinformation Campaign," U.S. Embassy in Georgia, last modified January 21, 2022, https://ge.usembassy.gov/russia-targets-ukraine-with-disinformation-campaign/.

[50] Bureau of Conflict and Stabilization Operations, "History of Russia's Aggression against Ukraine."

[51] Madeline Fitzgerald and Elliott Davis, Jr., "Russia Invades Ukraine: A Timeline of the Crisis," *US News & World Report*, February 21, 2023, //www.usnews.com/news/best-countries/slideshows/a-timeline-of-the-russia-ukraine-conflict.

Russian military personnel massed near the Ukrainian border, labeling this as the "most significant military mobilization since World War II.[52]" Russia and Belarus held the largest joint military drills in years, but President Putin claimed no plans of invading Ukraine and dismissed U.S. warnings of a possible invasion.[53] These actions further confirmed a possible upcoming invasion or act of war against Ukraine.

B. OSINT PRE-INVASION

On February 9, 2022, Twitter user @4emberlen posted a video of multiple armored vehicles and tanks traveling through downtown Crimea: "Good morning from Crimea, Sevastopol…Crimea has turned into a military training ground:(," is written in bold print across the video (Figure 2).[54] Twitter user @gfusfus replied to this message, shown in Figure 3.

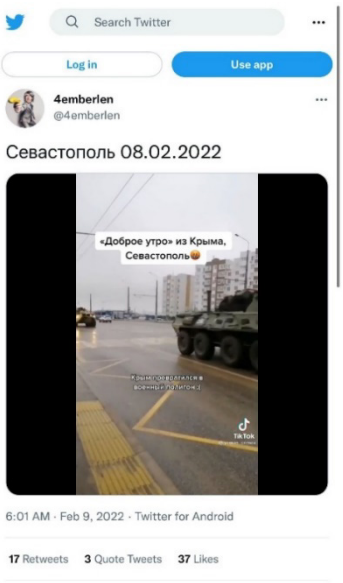


Figure 2. @4emberlen tweet

[52] *Bloomberg*, "A Visual Guide to the Russian Invasion of Ukraine." Accessed October 6, 2022, https://www.bloomberg.com/graphics/2022-ukraine-russia-us-nato-conflict/.

[53] *Bloomberg*.

[54] 4emberlen [@4emberlen], "Севастополь [Sevastopol] 08.02.2022 https://t.co/HWuf8mXjUe," Twitter, February 9, 2022, https://twitter.com/4emberlen/status/1491366702676066309.

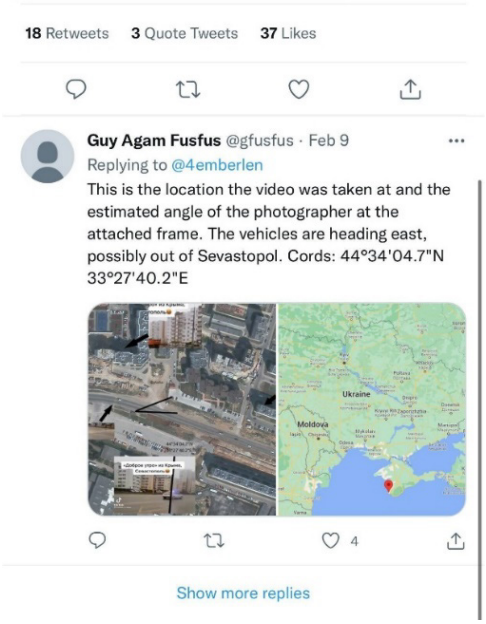


Figure 3. @gfusfus tweet

Twitter user @gfusfus used the original tweet and satellite imagery to determine the exact location where the video was taken. He provided exact coordinates and the military convoys' direction of travel (Figure 3).[55] With real-time, valuable, open-source intelligence like this, Ukrainian and NATO forces could accurately predict where possible invasions would occur so strategic military tactics could reinforce these likely invasion points. This same day, Twitter user @herooftheday10 posted a similar video of a Russian military convoy on the north border of Ukraine, as seen in Figure 4.[56]

[55] Guy Agam Fusfus [@gfusfus], "@4emberlen This Is the Location the Video Was Taken at and the Estimated Angle of the Photographer at the Attached Frame. The Vehicles Are Heading East, Possibly out of Sevastopol. Cords: 44°34'04.7"N 33°27'40.2"E Https://T.Co/5YBcrMIp5W," Twitter, February 9, 2022, https://twitter.com/gfusfus/status/1491433454474764294.

[56] АЗОВ_UA_NATO_USA_ישְׂרָאֵלILUAUSEUGB [@herooftheday10], "Белгородская область. На указателе видна надпись Алексеевка. https://t.co/Z71daf1nQL" [Belgorod region. Alekseevka is visible on the sign], Twitter, February 9, 2022, https://twitter.com/herooftheday10/status/1491328464292827136.

Figure 4. @heroooftheday tweet

The text over the video states, "Belgorod region. The inscription "Alexeyevka" is visible on the gun."[57] Alexeyevka lies in Oblast, Russia, which is approximately 200 miles from Belgorod. This post provided crucial information to defending forces. It provided intelligence on the type of military equipment, weaponry, personnel, etc., and because of the equipment's markings, defending forces could determine the direction from which attacking forces deployed.

Crowdsourcing on an unprecedented global scale took place during this invasion. Whether requested or voluntary, open-source information and posts from different social media sites can be extracted, analyzed, and reposted on other platforms. These posts were available to hundreds of millions of citizens around the globe, resulting in millions of independent analyses of this crucial information. There was no delay in this information and the analyses of these posts to military strategists because it is open source.

[57] АЗОВ_UA_NATO_USA_יִשְׂרָאֵלוILUAUSEUGB [@heroooftheday10].

On February 15th, 2022, TikTok user @dasha.artsova posted a video in Belarus. The video shows a convoy of trucks carrying tanks and military armored vehicles. Twitter user @JC_Monitoring reposted the TikTok video with the text "Russian convoy of military hardware spotted in Rechytsa, Belarus – headed southeast."[58] Figure 5 shows that Twitter user @chrisdneumann commented "Nice. Right next to the new bridge over the Pripyat river."[59]

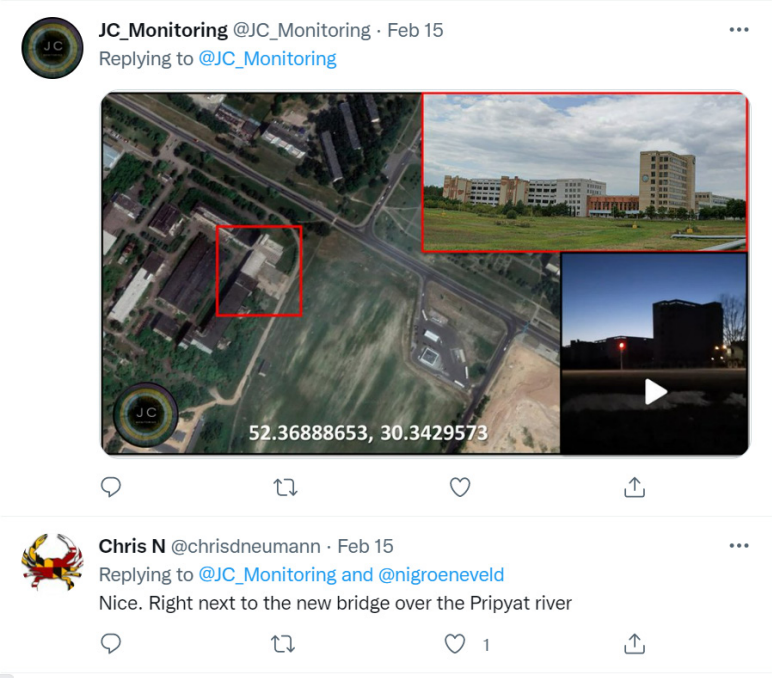


Figure 5. @JC_Monitoring/@chrisdneumann tweet

This example demonstrates the far-reaching effects of OSINT, because locals who know the area were reading these tweets and could identify specific landmarks within these videos and pictures.

[58] JC_Monitoring [@JC_Monitoring], "Russian Convoy of Military Hardware Spotted in Rechytsa, Belarus - Heading Southeast Coordinates - 52.36888653, 30.3429573 Https://T.Co/WDmgBtryvT," Twitter, February 16, 2022, https://twitter.com/JC_Monitoring/status/1493738346564268032.

[59] Chris N [@chrisdneumann], "@JC_Monitoring @nigroeneveld Nice. Right next to the New Bridge over the Pripyat River," Twitter, February 16, 2022, https://twitter.com/chrisdneumann/status/1493773632367054856.

On February 16th, 2022, TikTok user @mari.litova9003 posted a video of a Russian train carrying military equipment and personnel with very generic hashtags such as "#war, #russia, etc." (Figure 6).[60]

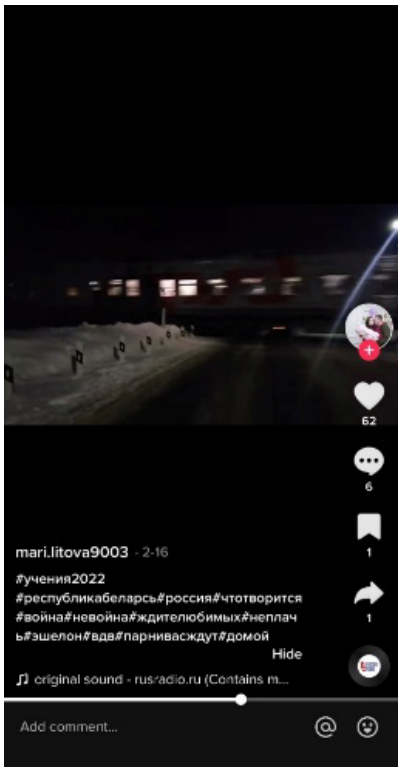


Figure 6. @marli.litova9003 TikTok

Twitter user @JC_Monitoring reposted this video on Twitter with the text "Trainload of Russian hardware under the cover of darkness, spotted in Kosmynino, Kostroma Oblast." The individual also provided a follow-up tweet demonstrating how he

[60] JC_Monitoring [@JC_Monitoring], "Trainload of Russian Military Hardware under the Cover of Darkness, Spotted in Kosmynino, Kostroma Oblast. Coordinates - 57.58571217, 40.75765208 Https://T.Co/H5CUhSwgGH," Twitter, February 16, 2022, https://twitter.com/JC_Monitoring/status/1494073105249181702.

determined the exact coordinates and direction of travel by using satellite imagery and Google Maps (Figures 7 and 8).[61]

Figure 7. @JC_Monitoring convoy tweet

Figure 8. @JC_Monitoring satellite tweet

[61] C_Monitoring [@JC_Monitoring], "Trainload of Russian Military Hardware under the Cover of Darkness, Spotted in Kosmynino, Kostroma Oblast. Coordinates - 57.58571217, 40.75765208 Https://T.Co/H5CUhSwgGH," Twitter, February 16, 2022, https://twitter.com/JC_Monitoring/status/1494073105249181702.

This second tweet shows the ground control panels and power converters from both an overhead satellite image and a street view from Google Maps. @JC_Monitoring posts a side-by-side picture of a screenshot of the original video showing the same control panel and power converter.[62] The tweet also highlights the Russian movement "under the cover of darkness." This OSINT post spoils any tactical element of surprise that the Russian military had planned. This is another example of tracking military assets by geotagging, through crowdsourcing.

This OSINT provided by Russian and Belarusian citizens showed that Russia was preparing to invade Ukraine. On February 21, 2022, President Putin made an hour-long speech in Brazil to the world.[63] President Putin announced his plans to recognize the Donetsk and Luhansk territories as sovereign states.[64] He accused Ukraine of genocide in these regions and alleged that the Ukrainian government was torturing women and children in these areas. During this address, President Putin also reiterated that Ukrainian membership in NATO would directly threaten Russian national security.[65] President Putin commented, "I would like to be clear and straightforward: in the current circumstances, when our proposals for an equal dialogue on fundamental issues have actually remained unanswered by the United States and NATO when the level of threats to our country has increased significantly, Russia has every right to respond in order to ensure its security…That is exactly what we will do."[66] He claimed to see no end in sight to the "killings of civilians, the blockade, the abuse of people, including children, women, and

[62] JC_Monitoring [@JC_Monitoring], "Trainload of Russian Military Hardware under the Cover of Darkness, Spotted in Kosmynino, Kostroma Oblast. Coordinates - 57.58571217, 40.75765208 Https://T.Co/H5CUhSwgGH," Twitter, February 16, 2022, https://twitter.com/JC_Monitoring/status/1494073105249181702.

[63] Robyn Dixon, "In Long Speech, Putin Recognizes Two Ukrainian Regions as Independent, a Potential Pretext for War," *Washington Post*, February 21, 2022, ProQuest.

[64] Dixon.

[65] Dixon.

[66] Dixon.

the elderly."[67] Thus, confirming the veracity of the OSINT that was provided during the movement of Russian assets.

This speech spread around the world and people took it as a warning of an impending invasion of Ukraine under false pretenses, specifically the Ukrainian government's atrocities towards its citizens.

On February 22, 2022, Russian media reported a vehicle-born IED was detonated at 0500 AM on a highway between Donetsk and Horlivka. The Russian Ministry of Defence posted the following photos and videos on Twitter and Telegram (Figure 9).[68]

Figure 9. Russian media

The text at the bottom of the picture states "On February 22, Ukrainian saboteurs detonated a min-explosive device on the Donetsk Gorlovka highway. As a result of the terrorist act, three civilians were killed."

[67] *Rio Times*, "President Putin's February 21 Speech to the Nation - Full Text," February 24, 2022, https://www.riotimesonline.com/brazil-news/modern-day-censorship/president-putins-full-text-of-february-21-2022-speech-to-the-nation/.

[68] "Народная Милиция ДНР" [People's Militia of the DPR], Telegram, accessed October 7, 2022, https://t.me/s/nm_dnr?before=6298.

The photo shows the vehicle that Russian officials claim was hit by a Ukrainian IED. The three deceased civilians were still inside the vehicles while Russian authorities are observed working on the vehicle at the crime scene (Figure 10).[69]

Figure 10. @PLnewstoday tweet

The Twitter video is of a Russian news reporter at the scene of the explosion reporting on the alleged killings of these three civilians (Figure 11).[70]

[69] Patrick Lancaster [@PLnewstoday], "3 Civilians Killed in a Roadside IED near Donetsk Just after Russia Recognized the #DPR and #LPR. My Video Report and Investigation Soon. Https://T.Co/Ywavy3aevL," Twitter, February 22, 2022, https://twitter.com/PLnewstoday/status/1496070006685196294.

[70] marqs [@MarQs__], "#DPR Claims There Was a 'Terrorist Attack' at the #Donetsk - Gorlovka Highway with Three People Killed Https://T.Co/MyD6vnCVip," Twitter, February 22, 2022, https://twitter.com/MarQs__/status/1496042122302181377.

Figure 11. @MarQs_ tweet

Bellingcat studied the pictures of the vehicles, deceased civilians, and the video and investigated these claims based on what Russian media and officials had posted. Bellingcat is an online, multinational, fact-checking organization that uses OSINT to research and investigate a variety of subjects to provide accountability and transparency.[71] The website recreated an overhead view of the scene using Google Maps and Maxar Satellite (Figure 12).

[71] "About," bellingcat, accessed February 27, 2023, https://www.bellingcat.com/about/.

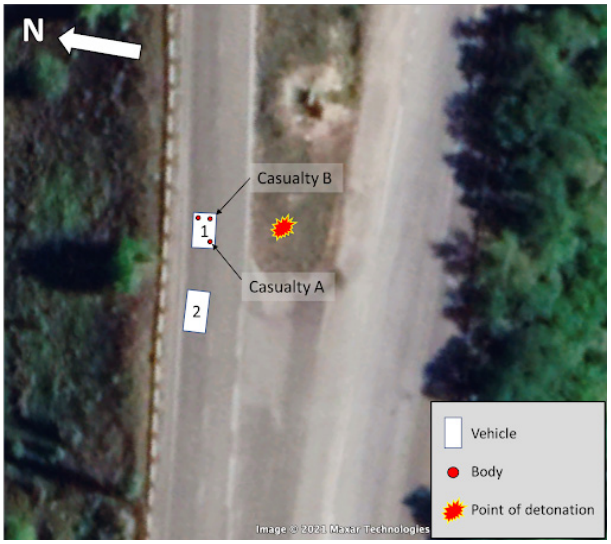


Figure 12. Bellingcat IED reconstruction

Online observers have pointed out many inconsistencies with the Russian account of the events. Many pointed out the lack of plates on the vehicles. Additionally, the location of the vehicles after the blast suggests that they were not moving when damaged.[72] In the same way, Chris Cobb-Smith, the director of Chiron Resources and an explosive weapons expert, concluded in an examination of these pictures: "The incident has been manufactured to give the impression it was a result of the detonation of an IED or off-road bomb."[73] Likewise, bellingcat solicited the assistance of a forensic scientist to examine the photos of the deceased civilians. The pictures of the bodies in the vehicles showed injuries inconsistent with the Russian media claims. The bodies were determined to be cadavers with marks and wounds consistent with autopsies.[74] Dr. Owens stated, "One would thus conclude that this is another case of exploiting human cadavers in order to fraudulently engineer a 'crime scene,' with obvious implications for the swaying of public opinion and thus justification for the military action that is currently underway."[75] Thus, three sources

[72] Nick Waters, "'Exploiting Cadavers 'and 'Faked IEDs': Experts Debunk Staged Pre-War 'Provocation' in the Donbas," *bellingcat*, February 28, 2022, https://www.bellingcat.com/news/2022/02/28/exploiting-cadavers-and-faked-ieds-experts-debunk-staged-pre-war-provocation-in-the-donbas/.

[73] Waters.

[74] Puiu, "How Open-Source Intelligence (OSINT) Is Exposing."

[75] Waters, "'Exploiting Cadavers 'and 'Faked IEDs.'"

verified the staging of these bodies to spread disinformation in support of Russia over Ukraine.

On Wednesday February 23, 2022, at approximately 0500 AM, TikTok user @natanazart posted a video on an unknown Russian road (Figure 13) showing a large convoy of Russian tanks and armored personnel carriers. The caption on the video stated, "Defenders of the Border," revealing that these military vehicles were staged close to the Ukrainian border.[76]

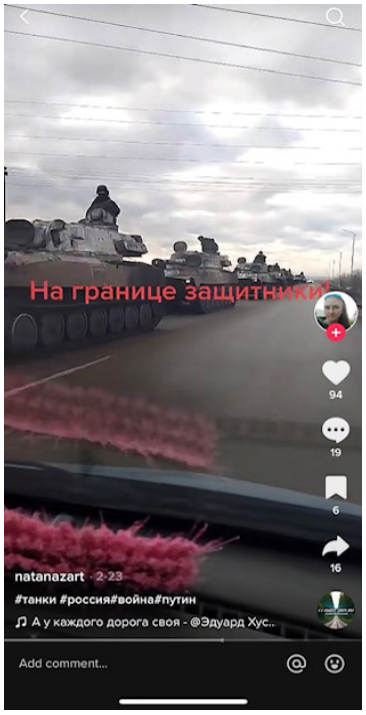


Figure 13. Natanazart TikTok

[76] Natanazart [@natanazart], "#украина#война#танки#белгород" [#Ukraine#war#tanks#Belgorod], TikTok, February 23, 2022, https://www.tiktok.com/@natanazart/video/7066269915409435905.

Two hours after this post, twitter user @YWNReporter geolocated the video to the Belorod region of Russia "just 8 miles from the Ukrainian border" (Figure 14).[77]

Figure 14. @YWNReporter tweet

Moshe Schwartz (@YWNReporter) located the convoy's exact coordinates using Google Maps and Google Street View. He uses landmarks in the video including multiple large and small telephone poles, utility towers, and a lone "house in the distance" in the video (Figures 15 and 16).

[77] Moshe Schwartz [@YWNReporter], "I've Geolocated This Video Uploaded 2 Hours Ago to the Belgorod Region of Russia Just 8 Miles from the Ukrainian Border. 50.437254,36.380161 - Use Google Street View, However, Note That You Won't See Street Lights on the Right Side of the Street. See Thread for Details. Https://T.Co/CYjyvBkKwI," Twitter, February 23, 2022, https://twitter.com/YWNReporter/status/1496452064578347009.

Figure 15. @YWNReporter street lights

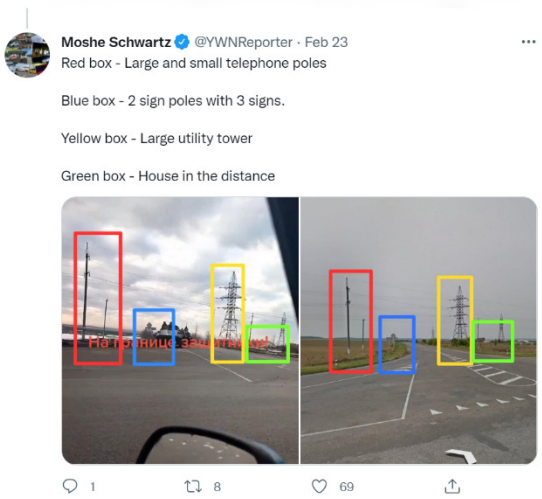


Figure 16. @YWNReporter telephone poles

Twitter user @ReddishCat1 replied on the thread and listed the military vehicles in the convoy (Figure 17): [78]

[78] ReddishCat [@ReddishCat1], "MT-LBu (multi-purpose armored carrier)x3. And 2S1 Gvozdika 122 mm (self-propelled howitzer)x7 fully amphibious," Twitter, February 23, 2022, https://twitter.com/YWNReporter/status/1496452064578347009.

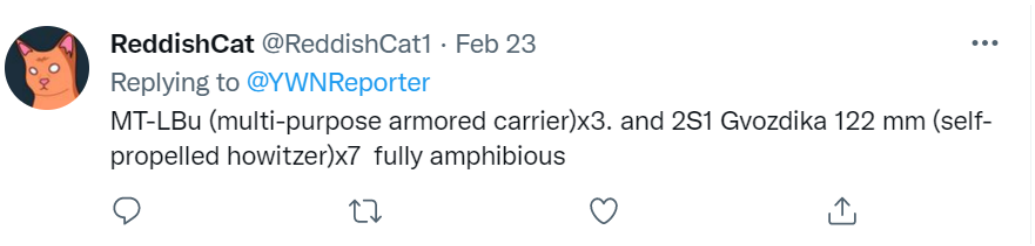


Figure 17. @ReddishCat1 tweet

Twitter user @hakan_pishot replied on the thread with a pinned map of the exact location (Figure 18).[79]

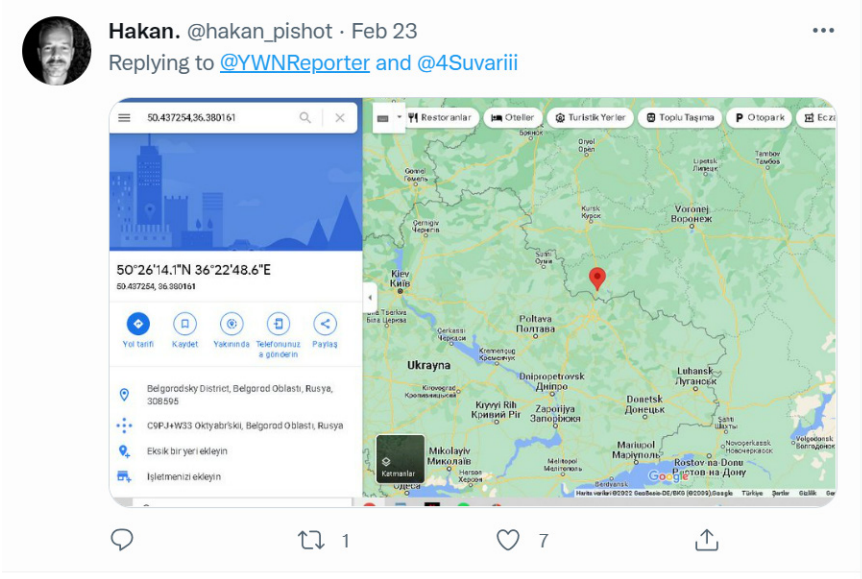


Figure 18. @hakan_pishot tweet

This same day, Maxar technology satellite photos revealed multiple Russian military staging locations just north of the Ukrainian border. Posters used readily available Maxar satellite technology to monitor Russian military staging locations prior to the

[79] Hakan [@hakan_pishot], "I've Geolocated This Video Uploaded 2 Hours Ago to the Belgorod Region of Russia Just 8 Miles from the Ukrainian Border. Https://T.Co/CYjyvBkKwI," Twitter, February 23, 2022, https://twitter.com/YWNReporter/status/1496452064578347009.

invasion. On February 23, 2022, satellite images showed staging locations in Yaruga, Golovchino, Krasnaya, Kupino, and Malakeevo.[80]

Multiple vehicles were staged in Golovchino, Russia, approximately 10 miles north of the Ukrainian border (Figure 19).

Figure 19. Satellite image Golovchino

A similar satellite photo captures a Russian staging area in Malakeevo, Russia. This location lies approximately 20 miles north of the Ukrainian border. Both photos showed fresh tire marks in the snow, demonstrating that the staging was relatively recent (Figure 20).

[80] Marianne Guenot, "Satellite Photos Show Russia's Final Troop Deployments around Ukraine before Putin Launched an Invasion," *Business Insider*, February 24, 2022, https://www.businessinsider.com/satellite-images-show-final-russia-troop-deployments-before-ukraine-invasion-2022-2.

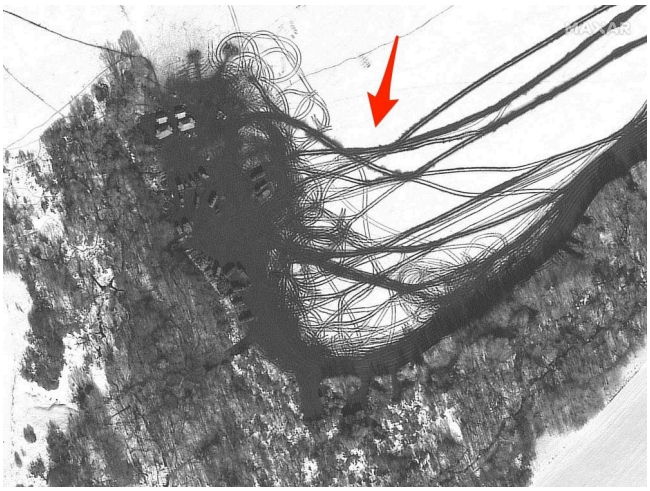


Figure 20. Satellite image Malakeevo

Satellite imagery and geo-tagged social media posted on the days leading up to the invasion provided valuable information for defending forces. President Putin's speech and the staged IED attack created extremely high tension in a dynamic situation, and any information on Russian military movements was crucial. Defending forces now knew the proximity of multiple convoys to the border, the types of military vehicles, and an estimated time of arrival if Russia decided to invade. Knowing these staging areas exposed Russian strategic, and military plans and tactics.[81]

Less than 24 hours after these photos were taken, President Putin announced a military assault against Ukraine. President Putin stated, "The goal is to defend people who have been victims of abuse and genocide from the Kyiv regime. And we will strive to demilitarize and de-Nazify Ukraine…we will also hand over everyone who committed bloody crimes against civilians, including Russian citizens, to court."[82] Additionally, any countries that intervened would suffer "consequences they have never seen." [83] The signs

[81] Guenot.

[82] John Haltiwanger, "Russian President Vladimir Putin Announces Military Assault against Ukraine in Surprise Speech," *Business Insider,* February 23, 2022, https://www.businessinsider.com/putin-announces-military-assault-against-ukraine-in-surprise-speech-2022-2.

[83] Haltiwanger,.

and signals from the plethora of videos, livestreams, and photos proved to be an accurate indication of the coming invasion.

The Ukrainian government and military were able to prepare for the ensuing invasion thanks to the combined efforts of OSINT and the millions of Ukrainian and Russian citizens who were posting information and analyzing others' posts. Russian citizens were posting videos and pictures of staged military assets and Ukrainian officials were able to use this information to effectively plan defense against invasion points.

C. OSINT INVASION

On February 24, 2022, Russia launched a full scale invasion of Ukraine. Russian President Vladimir Putin stated this invasion was to "demilitarize and de-Nazify Ukraine," and an attempt to free the Ukrainian people from government "genocide and bullying." [84] On this same day, Ukranian President Volodymyr Zelenskyy tweeted "Russian occupation forces are trying to seize the #Chornobyl_NPP….This is a declaration of war against the whole of Europe."[85]

The invasions began at 0400 AM local time and occurred on the northern border with Belarus and Russian-occupied Crimea. Ukrainian forces successfully defended against most invasion points on the initial invasion. Russian forces from Crimea successfully secured Kherson city and Russian forces from Belarus secured the Chernobyl Exclusion Zone. Russian forces attacked the Hostomel military air base in an attempt to ground all Ukrainian assets by attacking all military airports. This attempt failed—reports claimed Ukrainian forces shot down seven Russian aircraft and seven Russian helicopters.[86]

[84] Paul Kirby, "Why Has Russia Invaded Ukraine and What Does Putin Want?," *BBC*, May 9, 2022, https://www.bbc.com/news/world-europe-56720589.

[85] Володимир Зеленський [@ZelenskyyUa], "Russian occupation forces are trying to seize the #Chornobyl_NPP. Our defenders are giving their lives so that the tragedy of 1986 will not be repeated. Reported This to @SwedishPM. This Is a declaration of war against the whole of Europe.," Twitter, February 24, 2022, https://twitter.com/ZelenskyyUa/status/1496862540957114370.

[86] Institute for the Study of War, "Ukraine Conflict Updates," August 15, 2022, https://www.understandingwar.org/backgrounder/ukraine-conflict-updates.

Figure 21 is a map published by the Institute for the Study of War that shows Ukraine's areas of conflict and Russian maneuver and attacks on the first day of the invasion.

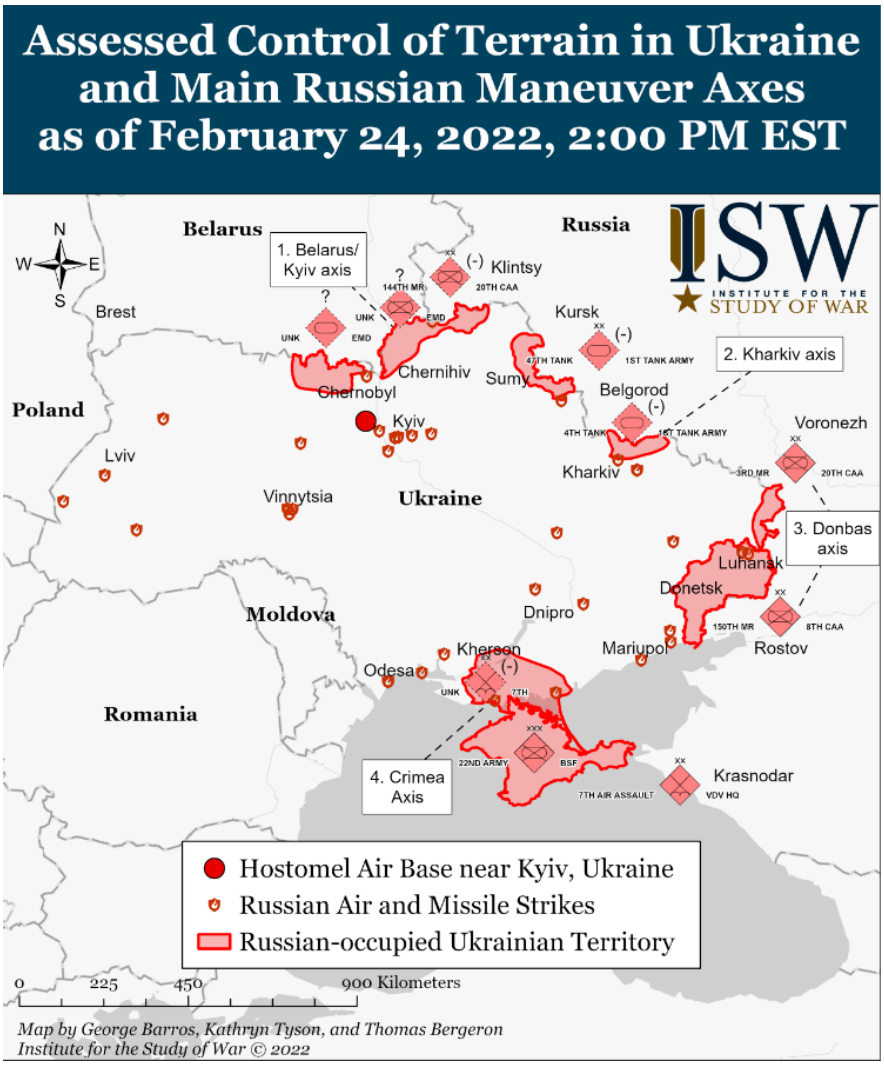


Figure 21. ISW map[87]

In the same report, U.S. military officials estimated that initial strikes during the invasions included 100 missiles, including medium-range, cruise, and sea-launched

[87] Source: Institute for the Study of War, "Ukraine Conflict Update 7," February 24, 2022, https://www.understandingwar.org/backgrounder/ukraine-conflict-update-7.

missiles, and that 75 Russian bomber aircrafts participated in the attack. The greatest success that Russia had in the initial invasion was on the Southern front from Russian-based Crimea's invading forces. This area was previously invaded by Russian forces and therefore had fewer civilians to provide the information geotagged in the northern regions. Russian citizens posted all OSINT gained from social media prior to the invasion. Once Russian forces entered Ukrainian territory, Ukrainian citizens and the Ukrainian military began posting information similar to the Russian citizens' but with more detailed information. Twitter user @RALee85 posted a YouTube live stream from Ukrainian locals early on during the first day of the invasion, shown in Figure 22.[88]

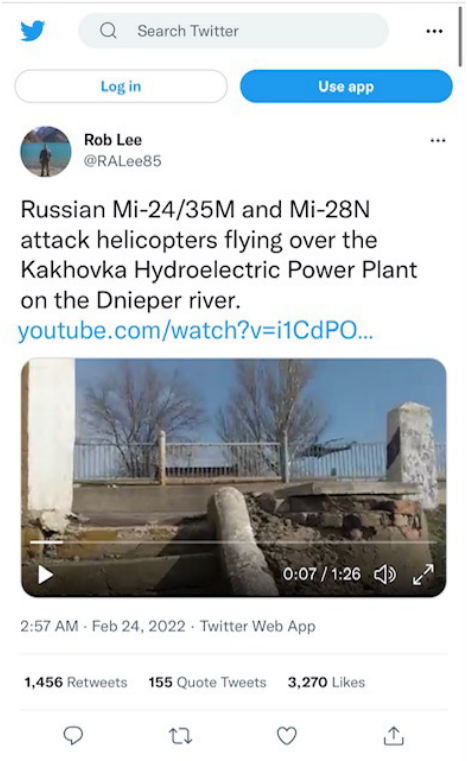


Figure 22. @RALee85 tweet

[88] Rob Lee [@RALee85], "Russian Mi-24/35M and Mi-28N Attack Helicopters Flying over the Kakhovka Hydroelectric Power Plant on the Dnieper River. Https://Youtube.Com/Watch?V=i1CdPO7brQQ&t=63s Https://T.Co/B2sXC9xhGP," Twitter, February 24, 2022, https://twitter.com/RALee85/status/1496801532066635779.

The Ukrainian dialogue roughly translates to "It's happening in front of my eyes, can't tell if these are Ukrainian or Russian military planes. Soldiers are pointing guns at them. Ok these are Russian army not Ukrainian. I am in the center of everything, probably need to stop shooting." The video shows the types of Russian military helicopters, the direction of travel, and most importantly the actions of the Russian helicopters. Twitter user @RALee85 identified the types of Russian helicopters and posted an additional video of ground forces (Figure 23). In this second video, he identified the Russian armored vehicles.[89]

Figure 23. @RALee85 Russian tanks

Shortly after these two posts, @RALee85 posted a video of Russian soldiers raising a Russian flag over the Kahovka hydroelectric power plant. Live streaming Russian military tactics during an invasion of an individual location like this power plant provided invaluable OSINT to the Ukrainian forces. It showed the defending forces what resources Russia would allocate for a facility of this size. Thus, it aided Ukraine in preparing similar infrastructure for future attacks or invasions.

[89] Rob Lee [@RALee85], "Russian Mi-24/35M and Mi-28N Attack Helicopters Flying over the Kakhovka Hydroelectric Power Plant on the Dnieper River. Https://Youtube.Com/Watch?V=i1CdPO7brQQ&t=63s Https://T.Co/B2sXC9xhGP," Twitter, February 24, 2022, https://twitter.com/RALee85/status/1496801532066635779.

Mariupol Atrocities during Seizure

The city of Mariupol lies in southeastern Ukraine, approximately 6 miles from the Sea of Azov. It is a port city and a popular vacation spot with a population of approximately 440,000 citizens. The Azon Sea port employed many of the city residents, exporting iron, grain, steel, and machinery.[90] Russian forces began the invasion of Mariupol on February 24, 2022, the first day Ukraine was invaded. The battle officially ended on May 20, 2022, when the remaining Ukrainian forces surrendered to Russian military. This period featured an overwhelming amount of livestreaming, pictures, and videos uploaded by citizens and military personnel.

On April 16, 2022, Twitter user @wargonzoo posts a video of a Russian military unit on a Mariupol beach with a Russian caption that translates to "Fighters of the legendary Donbass battalion together with other units, the DPR and the Russian Armed Forces finally drove out the neo-Nazis out of the city" (see Figure 24).[91]

[90] Greta Hamann, "Mariupol: Before and after Pictures Show Extent of Devastation," *Deutsche Welle*, April 24, 2022, https://www.dw.com/en/mariupol-before-and-after-pictures-show-extent-of-devastation/a-61570963.

[91] Семён Пегов [@wargonzoo], "ВИДЕО«Сомалийцы» на центральном пляже Мариуполя Бойцы легендарного донбасского батальона «Сомали» совместно с другими подразделениями НМ ДНР и ВС РФ окончательно выбили неонацистов из города и с северного направления вышли к морю. Прямо на центральный пляж Мариуполя. https://t.co/I1qiQHu3H8" [IDEO"Somalis" on the central beach of Mariupol the fighters of the legendary Donbass battalion "Somali", together with other units of the NM of the DPR and the RF Armed Forces, finally drove the neo-Nazis out of the city and went to the sea from the northern direction. Right on the central beach of Mariupol], Twitter, April 16, 2022, https://twitter.com/wargonzoo/status/1515269158560309250.

Figure 24. @wargonzoo tweet

Figure 25 shows Twitter user @tinso_ww post, a two-minute video of various gun battles of Russian Chechen forces in the downtown area.[92]

[92] Aldin ВА [@tinso_ww], "Chechen Forces in Mariupol. Https://T.Co/QvbEF98reC," Twitter, March 26, 2022, https://twitter.com/tinso_ww/status/1507806075608829955.

Figure 25. @tinso_tweet

During the seizure of Mariupol, data collected from OSINT helped debunk Russian government and media lies and disinformation. In early March, President Putin stated that Mariupol would be one of several Ukrainian cities with a "humanitarian corridor" for the safe passage of innocent civilians to Russia and Belarus.[93] Russian officials deny claims of war crimes and targeting civilian locations. On March 11, 2022 President Zelensky made a public announcement that the humanitarian corridor set up from Mariupol had been blocked off. He further stated that when he sent in a convoy of trucks with food, water, and medicine, they were attacked by Russian tanks. He stated, "the occupiers launched a tank attack exactly where this corridor was supposed to be."[94]

Ukrainian official, Sergiy Orlov, reported a week into the invasion, "They (Russian forces) have used aviation, artillery, multiple rocket launchers, grenades and other types of weapons we don't even know about. This isn't simply treacherous. It's a war crime and

[93] Agence France Presse, "Russia-Ukraine War: Russian Tanks Attacked Humanitarian Corridor in Mariupol," NDTV, March 11, 2022, https://www.ndtv.com/world-news/russia-ukraine-war-russian-tanks-attacked-humanitarian-corridor-in-mariupol-ukraine-president-volodymyr-zelensky-2816343.

[94] Agence France Presse.

pure genocide." [95] He further listed civilian targets such as residential homes, maternity hospitals, and civilian workplaces.

On March 9, 2022, Ukrainian President Zelenskyy (@ZelenskyyUa) posted a minute-long video of a maternity hospital that was destroyed by Russian forces.[96] Figure 26 shows a screenshot of the tweet.

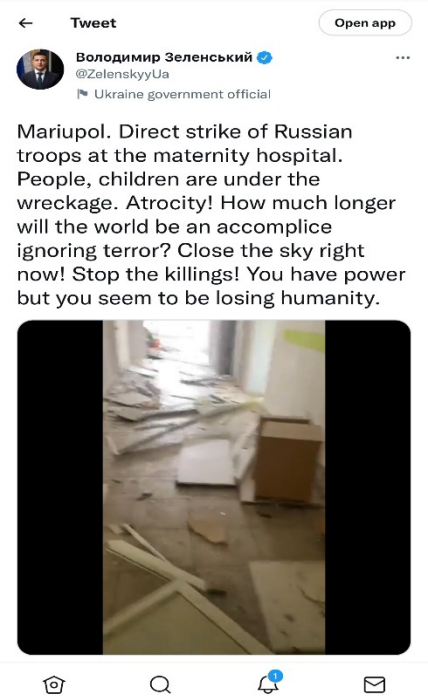


Figure 26. @ZelenskyyUa

On April 4, 2022, Twitter user @Polk_Azoz posted an overhead view of multiple residential housing complexes in Mariupol, seen in Figure 27. The quote translates to "Mariupol today. 40 days ago, the city was beautiful. The invaders took away our spring.

[95] Luke Harding, "'Pure Genocide': Civilian Targets in Mariupol 'Annihilated' by Russian Attacks," *The Guardian*, March 9, 2022, sec. World news, https://www.theguardian.com/world/2022/mar/09/pure-genocide-civilian-targets-in-mariupol-annihilated-by-russian-attacks.

[96] Володимир Зеленський [@ZelenskyyUa], "Mariupol. Direct Strike of Russian Troops at the Maternity Hospital. People, Children Are under the Wreckage. Atrocity! How Much Longer Will the World Be an Accomplice Ignoring Terror? Close the Sky Right Now! Stop the Killings! You Have Power but You Seem to Be Losing Humanity. Https://T.Co/FoaNdbKH5k," Twitter, March 9, 2022, https://twitter.com/ZelenskyyUa/status/1501579520633102349.

They burned, mutilated, plundered."[97] On April 8, 2022, Russian authorities reported 5,000 civilians had died in Mariupol since the beginning of the invasion. Ukrainian officials were "cautious" of this 5,000 number and stated that many of the bodies of the casualties were still trapped in the rubble. They predicted this number could rise to "dozens of thousands."[98]

Figure 27. @Polk_Azov tweet

[97] AZOV Regiment [@Polk_Azov], "Маріуполь сьогодні. 40 днів тому місто було прекрасним. Окупанти забрали нашу весну. Вони спалили, понівечили, сплюндрували... І за це може бути тільки смерть. Смерть і жодного прощення. https://t.co/RKhQjvCuMx" [Mariupol today. 40 days ago, the city was beautiful. The invaders took away our spring. They burned, mutilated, plundered... And for that can only be death. Death and no forgiveness], Twitter, April 4, 2022, https://twitter.com/Polk_Azov/status/1510913245103591426.

[98] Tim Borlay, "Pro-Russian Authorities in Mariupol Put Civilian Dead at 5,000," Turned News, April 8, 2022, https://turnednews.com/pro-russian-authorities-in-mariupol-put-civilian-dead-at-5000-war-in-ukraine/.

On April 21, 2022, Twitter user @JackDetsch posted a Maxar satellite image of a possible grave site just outside of the city of Mariupol.[99] Figure 28 shows the screenshot.

Figure 28. @JackDetsch tweet

[99] Jack Detsch [@JackDetsch], "NEW: Satellite Imagery Reveals a Mass Grave Site about 12 Miles West of Ukraine's Besieged City of Mariupol. Russian Soldiers Have Been Reportedly Taking the Bodies of People Killed in Mariupol to This Site in Manhush, Ukraine That Contains More than 200 Graves. @Maxar Https://T.Co/SgHlwSXZsj," Twitter, April 21, 2022, https://twitter.com/JackDetsch/status/1517159822868758528

The same area captured by Maxar satellites showed no graves in March 2022. The Mariupol City Council stated that similar Maxar satellite images showed mass graves in the city of Bucha that were approximately 20 times this size.[100] The mayor of Mariupol reported that as many as 22,000 Mariupol residents died during the seizure. The mayor's advisor, Petro Andriuschenko, claimed that the process of confirming the casualties had been difficult because Russian forces had been burying the deceased civilians.[101] For the first time in history, the world witnessed the staging, amassing, and training of military assets on both sides of the conflict because of modern technology. Social media live streaming, geotagging, and satellite imagery brought the Russian-Ukraine war onto every smartphone and computer in the world. Twitter, Instagram, Facebook, and other social media outlets have made it possible for ordinary citizens to become global reporters and documentarists.

Open-source information from Eastern European citizens in the conflict zones and borders of these territories provided invaluable insights to Ukrainian military forces. Crowdsourcing was effectively utilized to analyze and spread this OSINT at an unprecedented rate. Prior to the invasion, social media posts were utilized to locate Russian movements, staging locations, and military equipment. During the initial invasion, social media posts were utilized to expose Russian military tactics and prepare for future attacks. Social media posts during the seizure of Mariupol were utilized to expose war crimes and atrocities committed by Russian forces. During this entire period, social media was used to debunk Russian misinformation and disprove Russian propaganda. Open-source information was utilized by Ukrainian forces to prepare for an impending invasion. It can be reasoned that this information has saved lives and is the reason powerful Russian military forces have not been as successful in the Ukrainian-Russian conflict.

[100] Yuliya Talmazan, "Satellite Imagery Points to Mass Grave Site near Besieged Mariupol," *NBC News*, April 22, 2022, https://www.nbcnews.com/news/world/mariupol-mass-graves-identified-satellite-images-rcna25530.

[101] *Interfax-Ukraine*, "At Least 22,000 Civilians Killed in Mariupol - Mayor's Adviser," May 25, 2022, https://en.interfax.com.ua/news/general/834794.html.

IV. LAW ENFORCEMENT OSINT USE

The Ukraine case study demonstrates the effectiveness of OSINT and the benefits that the information can provide to the forces using this information. Domestic law enforcement is different from an international military conflict, but the same OSINT platforms are used to gather this intelligence. This chapter discusses the current use of OSINT by law enforcement and key obstacles that have been identified as minimizing OSINT effectiveness. This chapter and Chapter III are the basis for this thesis's recommendations to improve the use of OSINT in American law enforcement.

Law enforcement agencies depend on OSINT in law enforcement more than any other category of collected intelligence.[102] Law enforcement uses this intelligence for various reasons including notifying the public of safety concerns, community outreach, soliciting crime tips, recruitment, and monitoring public sentiment.[103] Open-source intelligence is a form of intelligence that is produced from "publicly available information that is collected, exploited, and disseminated in a timely manner to an appropriate audience for the purpose of addressing a specific intelligence and information requirement."[104] While many other intelligence disciplines such as signals intelligence (SIGINT) and communications intelligence (COMINT) rely on government resources (wiretaps, military vessels, etc.), OSINT can be obtained by any officer or citizen. Law enforcement relies heavily on this data because it is unclassified, non-sensitive, and available to everyone.

Because the information is publicly available, it is relatively cost-efficient for law enforcement to collect, which is especially valuable to agencies with limited budgets. Additionally, high-quality geospatial information can now be collected on free specialized websites, essentially replacing SIGINT for many purposes. Because this information is

[102] Gašper Hribar, Iztok Podbregar, and Teodora Ivanuša, "OSINT: A 'Grey Zone'?," *International Journal of Intelligence and CounterIntelligence* 27, no. 3 (2014): 529–49, https://doi.org/10.1080/08850607.2014.900295.

[103] Kim, Oglesby-Neal, and Mohr, *2016 Law Enforcement Use of Social Media Survey*.

[104] Staniforth, "Police Use of Open Source Intelligence."

gathered from the internet, it eliminates the risk of endangering an undercover officer or using a paid informant to gather intelligence.[105]

A. 21ST CENTURY LAW ENFORCEMENT SOCIAL MEDIA OSINT

In the early 21st century, American law enforcement encountered multiple issues with "traditional" policing and community relations. Many high-profile police interactions with civilians resulted in public concern; former President Barack Obama's Task Force on 21st-Century Policing identified best practices and recommendations to promote policing practices and effective crime reduction techniques while building public trust.[106] The third recommendation or "pillar" was labeled "Technology and Social Media.[107]" This pillar includes all relevant law enforcement technology (radio spectrum, "less lethal," body worn cameras, etc.). This section of the report discusses the constantly evolving technology that is regularly used to improve policing practices. The task force states, "Law enforcement agencies and leaders need to be able to identify, assess, and evaluate new technology for adoption and do so in ways that improve their effectiveness, efficiency, and evolution."[108]

This technology has been evaluated and adopted to "improve effectiveness, efficiency, and evolution." This pillar includes "social media," which has been utilized in effective manners since the 2015 report.[109]

In 2016, the International Association of Chiefs of Police and the Urban Institute surveyed 539 law enforcement agencies. Figure 29 shows responses to the question of how agencies use social media. The survey showed 91% of agencies use social media to notify the public of safety concerns and 89% use it for community outreach. This same report showed only 70% of agencies used social media to gather intelligence for investigations

[105] Codruţa Luţai, "Open Source Intelligence."

[106] President's Task Force on 21st Century Policing, *Final Report of the President's Task Force on 21st Century Policing* (Washington, DC: Office of Community Oriented Policing Services, 2015), https://www.ojp.gov/ncjrs/virtual-library/abstracts/final-report-presidents-task-force-21st-century-policing.

[107] President's Task Force on 21st Century Policing.

[108] President's Task Force on 21st Century Policing, 2–3.

[109] President's Task Force on 21st Century Policing, 2-3.

(seventh of eleven options on the list). This is the most recent survey of this nature—with the expansion of social media, the numbers are now presumably higher.[110]

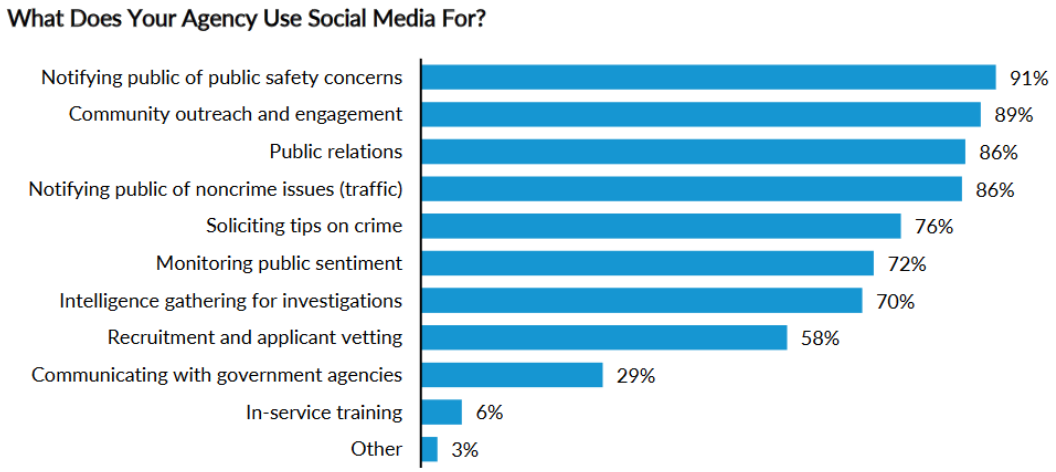


Figure 29. Agency use of social media

It can be argued that only 70% of agencies using social media to gather intelligence for investigations is not effective, efficient, or evolutionary. Social media intelligence is robust with vital information and can aid in reducing the "unknown" by monitoring communities more closely than would be possible otherwise. According to Ivan et al., SOCMINT can "determine some behavioral patterns that can apply for certain groups or certain individuals….in times of crisis, SOCMINT is a source of real-time information and an important element in their (groups) management."[111] This theory demonstrates the magnitude of social media OSINT. If the law enforcement intelligence community can use SOCMINT to monitor communities or networks of individuals, they may be able to predict behavioral patterns, thus creating proactive opportunities to prevent crime through the collection and analysis of information from social media platforms belonging to these individuals.

[110] Kim, Oglesby-Neal, and Mohr, *2016 Law Enforcement Use of Social Media Survey*.

[111] Ivan et al., "Social Media Intelligence."

SOCIMINT can also be used to monitor the processes of "radicalization and violent behavior," which can better predict future trends.[112] This identified benefit can directly assist in the prevention of two top-priority threats identified by Homeland Security: active combatants and domestic violent extremists, both increasing in frequency.[113] A *New York Times* article examined more than 100 public school systems and universities that contracted private companies that use SOCMINT to prevent active combatant incidents. These companies "geofence" for social media posts or tweets that contain keywords or a combination of words that warrant further investigation. These companies advertise 24/7 student monitoring of public social media posts.[114]

The second threat which has increased in difficulty to predict and defend against is a domestic violent extremist attack. Because these extremist organizations practice an unorthodox "leaderless resistance" principle, traditional intelligence collection methods are impractical. DVEs do not follow a "top-down" leadership hierarchy, so law enforcement methods of monitoring and addressing these threats often fall short. This shortfall was demonstrated prior to the January 6 Capitol attack. There were warning signs and indicators that an attack was likely to occur, but there was a failure to disseminate or act upon this information. In late December of 2021, NYPD intelligence sent over "raw intel" of various social media platforms predicting there would "likely be violence when lawmakers certified the presidential election on January 6th."[115] Former acting deputy DHS secretary Kenneth Cuccinelli II told the *New York Times* that Capitol Police were given access to a social media channel information tool; this tool disseminated information from popular social media platforms and Cuccinelli II further stated "it was clear the Capitol was the focus of that [attack]."[116]

---

[112] Ivan et al.

[113] Department of Homeland Security, "Counter Terrorism and Homeland Security Threats" accessed February 27, 2023, https://www.dhs.gov/counter-terrorism-and-homeland-security-threats.

[114] Leibowitz, "Could Monitoring Students on Social Media Stop the Next School Shooting?"

[115] Mitchell D. Silber, *Domestic Violent Extremism and the Intelligence Challenge* (Washington, DC: Atlantic Council, 2021), 5, https://www.atlanticcouncil.org/in-depth-research-reports/domestic-violent-extremism-and-the-intelligence-challenge/.

[116] Silber, 5.

Crucial information prior to the January 6th Capital attack was obtained through social media and was sent through the appropriate channels to have prepared for this insurrection. The Capitol Police ignored this real-time, detailed intelligence available on these platforms and through these tools, and as a result, failed to act. If acted upon, this OSINT may have prevented or at least hampered this attack, saving lives and valuable resources.

B. CHALLENGES

The maximization of OSINT has encountered several main obstacles that have prevented full utilization by law enforcement. Massive amounts of data to be analyzed, public sentiment surrounding government intrusion, law enforcement cultural resistance to change, and the lack of national collection standards are some of the many challenges relating to OSINT.

1. Data

The tremendous volume of OSINT data is continuously growing and evolving. This volume grows at an exponential rate with the development of the dark web and the increasing number of social media platforms and technological advancements.[117] Ivan et al. discusses this issue at length relating to the use of SOCMINT. He describes information as a "needle in a haystack," because social network sites translate approximately 4 billion data points and 250 million new photos every day.[118] He further states that, because of this flow of endless data, intelligence officers may "formulate erroneous positions."[119] Codruţa Luţai highlights the added challenge with this data of the "fake news" phenomenon and concludes that intelligence analysts must now make additional efforts to reverify information that would have been used prior to the dis/mis/malinformation wave of online information.[120] This extra step can delay the spread of this intelligence, which can hinder

[117] Ungureanu, "Open Source Intelligence."

[118] Ivan et al., "Social Media Intelligence."

[119] Ivan et al.

[120] Codruţa Luţai, "Open Source Intelligence."

its effectiveness. Analysts must validate or disprove misinformation and disinformation spread by individuals; automated bots also formulate contradictory information on social media platforms.[121]

This flow of information can be compared to drinking water from a firehose. In order to scope or filter this incoming data, identifying relevant subjects or subject matter is crucial. Best advises that the first challenge is "to identify and retrieve the most relevant data from within the sea of data on the internet and elsewhere."[122] Staniforth advises starting any investigation with a "hypothesis as a starting point."[123] This hypothesis is based on reasoning and an assumption of its truth as a starting point to further investigate its validity. Staniforth adds that the information-rich OSINT provides a more detailed data set to investigate this hypothesis by accessing this "lawfully accessed" information, intelligence analysts are able to network with friends, and associates to build on these facts.[124]

2. Public Sentiment

Public regard towards law enforcement has dropped significantly since multiple deadly encounters with citizens. Figure 30 is from a 2020 poll measuring "confidence" in law enforcement officers. In 2004, the poll showed over 60%; in 2020, for the first time since the poll began, confidence dropped below 50%.[125]

[121] Harry Kemsley, "In OSINT We Trust?," *The Hill*, September 1, 2021, https://thehill.com/opinion/national-security/569738-in-osint-we-trust/.

[122] Best, "Challenges in Open Source Intelligence," 58.

[123] Staniforth, "Police Use of Open Source Intelligence," 27.

[124] Staniforth, "Police Use of Open Source Intelligence."

[125] "Public Perceptions of the Police," Council on Criminal Justice, October 7, 2020, https://councilоncj.org/public-perceptions-of-the-police/.

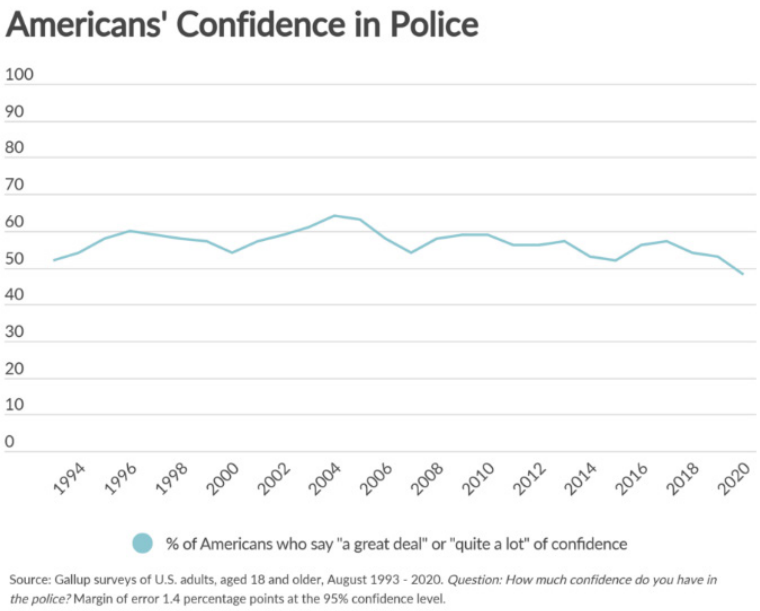


Figure 30. 2020 American confidence in police

A 2016 CATO Institute report showed similar results but added that, although there is less confidence in law enforcement, there is not a high percentage of "unfavorable" views of the police. Instead, there are more "neutral" feelings toward police officers.[126] This CATO poll does reveal strong public feelings against the use of technology relating to privacy concerns. Although the use of open-source intelligence by law enforcement was not a subject of the poll, citizens were polled on police use of unmanned aerial vehicles (also known as "drones"). Fifty-four percent (54%) of citizens worried drones would present a risk to privacy. Sixty percent (60%) of all millennials polled worried about these privacy concerns.[127]

The use of any technology in law enforcement is usually challenged and bounded by court rulings. Social media OSINT collection has had few court proceedings, specifically if the information posted on the various social media websites is protected by

[126] Emily Ekins, "Policing in America: Understanding Public Attitudes toward the Police. Results from a National Survey," Cato Institute, December 7, 2016, https://www.cato.org/survey-reports/policing-america-understanding-public-attitudes-toward-police-results-national.

[127] Ekins.

the fourth amendment of the Constitution. One related court case is U.S. v. Joshua Meregildo in 2012, filed in the District Court for the Southern District of New York. The suspect had his Facebook account privacy set to "private" and the government obtained incriminating information through a cooperating Facebook "friend."[128]

The court ruled against the defendant and stated, "legitimate expectation of privacy ended when he disseminated to his 'friends' because those 'friends' were free to use the information however they wanted—including sharing it with the government." This case ruled in favor of the government using evidence that is not publicly available to all. The lack of court rulings to challenge the legality of law enforcement practices related to the fourth amendment may be resulting in a lack of public trust in these methods.

Trottier claims that monitoring OSINT results in "social costs," and reports "the main risk is that people confine themselves in their communication due to the feeling of being watched."[129] Rigoglioso concurs, and points out that the revelations uncovered by Edward Snowden sparked a national debate about civil liberties and government technology used to collect and store vast amounts of citizens' personal information.[130] More specifically, information that is "collected, kept, and shared with little to no oversight, or awareness by the general public," and these technologies change the relationship between the citizen and the state.[131]

Public trust in law enforcement has decreased, and thus, according to public polls and some scholars, support for OSINT collection has decreased. American culture and fear of a "big brother" utopia is a crucial challenge in law enforcement OSINT collection. There is an understanding that posting information about oneself on various social media

[128] Office of Community Oriented Policing Services and Police Executive Research Forum, *Social Media and Tactical Considerations for Law Enforcement*.

[129] Daniel Trottier, "Open Source Intelligence, Social Media and Law Enforcement: Visions, Constraints and Critiques," *European Journal of Cultural Studies* 18, no. 4–5 (2015): 530–47, https://doi.org/10.1177/1367549415577396.

[130] Marguerite Rigoglioso, "Civil Liberties and Law in the Era of Surveillance," *Stanford Lawyer*, no. 91 (Fall 2014), https://law.stanford.edu/stanford-lawyer/articles/civil-liberties-and-law-in-the-era-of-surveillance/.

[131] Rigoglioso.

platforms is available to all. Some of the public does not believe that the "all" should include law enforcement agencies.

Citizens are likely to support police technology only with the belief that these technologies are necessary and will not invade their privacy. Public sentiment towards law enforcement matters—people who trust in the police are less likely to be suspicious about them abusing technology.[132] A 2021 Veritone survey of American citizens showed that the public is more likely to support technology whose uses and capabilities are transparent.[133] This same survey showed that 61% of respondents agree with using technology to identify criminal suspects and 84% of respondents believe that police should spend their time on violent crimes.[134]

The public is concerned with violent criminal acts and supports the technology that identifies criminal suspects. Because the public supports use of transparent technology by law enforcement, it is necessary for law enforcement to demonstrate OSINT use in preventing violent crimes. The use of this technology must be transparent to create public support and aid in the prevention of these criminal acts.

3. Law Enforcement Culture

There are two main challenges to OSINT maximization due to the current culture of law enforcement. Law enforcement agencies are reluctant to prioritize OSINT due to its "open" nature. Law enforcement does not embrace a culture of information sharing with other agencies and departments. These law enforcement intelligence-related traditions are counteractive to the effective collection and dissemination of OSINT.

Rowley claims that agencies use outdated technology and spend most efforts on curating internal intelligence data, stating, "This is driven by the culturally outdated assumption that the greatest insights will always be found in the mountains of data that big

[132] Ekins, "Policing in America."

[133] Veritone, "How Law Enforcement Builds Transparency and Trust with Technology," September 20, 2022, https://www.veritone.com/blog/law-enforcement-builds-transparency-and-trust-with-technology/.

[134] Veritone.

organizations have spent decades accumulating."[135] Hwang et al. concur with Rowley and add that "organizational perception and prejudice" of open-source intelligence is a major disadvantage to this information, claiming that agencies underestimate the value of the data because of its public availability.[136] OSINT holds less weight to law enforcement intelligence analysts because any citizen can access the same information. As previously discussed, open-source intelligence may be shared relatively quickly due to the lack of security clearance requirements. This advantage is quickly diminished if analysts and agencies hold this vital information. Herrington asserts that "knowledge management" includes "bringing the right information to the right people at the right time."[137]

The U.S. Congress Committee for Intelligence Reform highlighted the importance of information sharing, noting that there are cultural incentives not to share information between agencies: "These include a natural impulse to hoard information to protect turf, and a deeply ingrained passion for secrecy," stated the committee.[138] It went on reiterate that reform must start with altering agency culture to promote information sharing which will produce timely and constructive intelligence.[139]

4. Lack of National Standards

The internet boom beginning in the early 2000s has resulted in various social media platforms from which law enforcement agencies to collect open-source intelligence. There are no national collection standards because of the rapid rate at which these platforms have evolved and the lack of court cases where the information collected by law enforcement

[135] Mark Rowley, "Open Source Intelligence - the Cinderella of the Investigative Family?," *The Police Foundation* (blog), October 28, 2021, https://www.police-foundation.org.uk/2021/10/open-source-intelligence-the-cinderella-of-the-investigative-family/.

[136] Yong-Woon Hwang et al., "Current Status and Security Trend of OSINT," ed. Yan Huo, *Wireless Communications & Mobile Computing* 2022 (2022): 1–14, https://doi.org/10.1155/2022/1290129.

[137] Vee Herrington, "Intelligence Reform Brings New Opportunities for Info Pros," *Information Outlook* 12, no. 3 (March 2008): 10–16, ProQuest.

[138] David Boren et al., "Guiding Principles for Intelligence Reform," *Congressional Record* 150, no. 114 (September 21, 2004): S9429, https://www.congress.gov/congressional-record/volume-150/issue-114/daily-digest.

[139] Boren et al.

has been challenged. Therefore, information gathered by one agency is bound by regulations (or lack thereof) that do not restrict other agencies in the same way.

Within the New York City Police Department, for example, analysts are able to create fake accounts or "aliases" and interact with individuals to gain information; the only requirement for this is record keeping and notification to a supervisor.[140] The Detroit Police Department, on the other hand, can create aliases to interact with individuals on social media only after approval from the Deputy Chief of their Detective Bureau.[141] All such aliases are managed and controlled by the Local Agency Security Officer.[142] The Michigan State Police Department scrolls and scans social media posts using facial ID recognition programs and compares them to law enforcement databases. A July 2021 Detroit PD monthly report showed that 35% of facial recognition cases were used with a combination of social media posts.[143] Because there is no national collection standard for open-source intelligence, there are varying tools, methods, regulations, and policies from one jurisdiction to another. These inconsistencies result in a less favorable culture of information sharing. Agencies are hesitant to share information because of the varying standards. The receiving agency might also be less likely to use intelligence because it is unknown how the information was collected.

A lack of national standards also results in various training inconsistencies. As shown in the Table 2, the IACP and Urban Institute poll shows training as the third highest ranking challenge to utilizing social media.[144] With no national "best practices" or "benchmark standards," agencies are unable to confidently train analysts on the most effective manner to collect this intelligence.

---

[140] Office of Community Oriented Policing Services and Police Executive Research Forum, *Social Media and Tactical Considerations for Law Enforcement*.

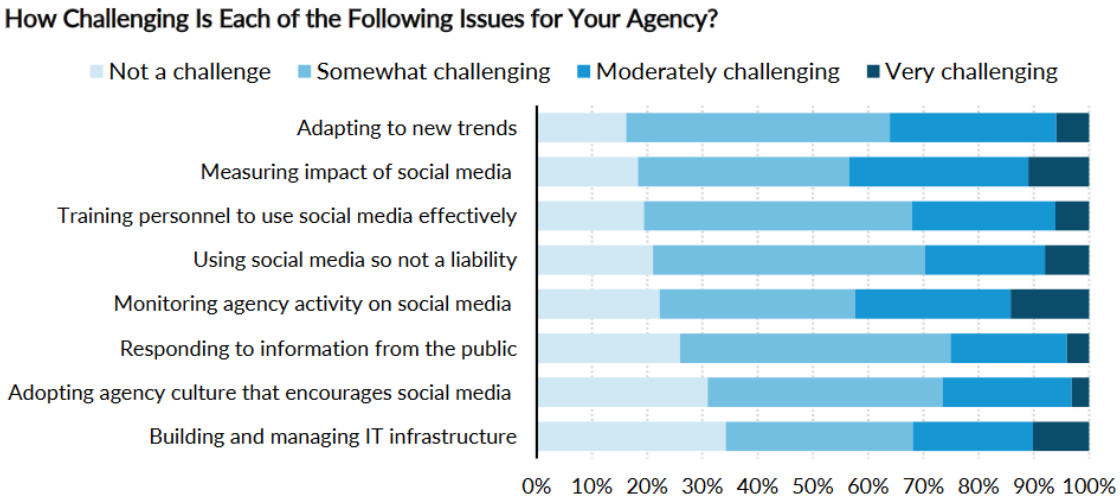
[141] Malachi Barrett, "How Police Monitor Social Media to Find Crime and Track Suspects," *mlive*, August 11, 2021, https://www.mlive.com/politics/2021/08/how-police-monitor-social-media-to-find-crime-and-track-suspects.html.

[142] Barrett.

[143] Barrett.

[144] Office of Community Oriented Policing Services and Police Executive Research Forum, *Social Media and Tactical Considerations for Law Enforcement*.

Table 2. Social media and L.E. challenges



A 2013 Department of Justice report highlighted the importance of social media and recommended that agencies build their related policies with regard to several points.[145] The report states that "agencies must consider a number of issues including: which types of online content should be viewed, who will conduct the observation and analysis, and how information will be communicated to operational commanders and field officers."[146] Very broad recommendations from various federal committees and agencies similar to the 2013 report have created numerous standards whose variations depend on the political climate, geographical location, and citizens in that department's jurisdiction.

Law enforcement agencies face heavy public scrutiny for using publicly available information to prevent and prosecute criminal acts. Various federal reports stress the importance of policies and regulations that regulate law enforcement's use of social media to investigate crimes, and on the whole recommend national standards and training regarding the collection of open-source intelligence. Law enforcement must overcome the culture of "secret" intelligence and conform to a culture of information sharing.

[145] Office of Community Oriented Policing Services and Police Executive Research Forum, *Social Media and Tactical Considerations for Law Enforcement*.

[146] *Social Media and Tactical Considerations for Law Enforcement*, 11.

V. FINDINGS AND DISCUSSION

Law enforcement's effective use of open-source intelligence is rapidly changing as technological capabilities evolve. In addition to the evolving technology, information sharing among various social media platforms has made this intelligence available in real-time with constantly updated information. The efficacy and potential of open-source intelligence use were demonstrated prior to the Ukraine invasion by Russian forces. Ukraine forces were able to properly prepare in part because of open-source intelligence. Social media posts, pictures, videos, and satellite imagery were shared on the world stage.

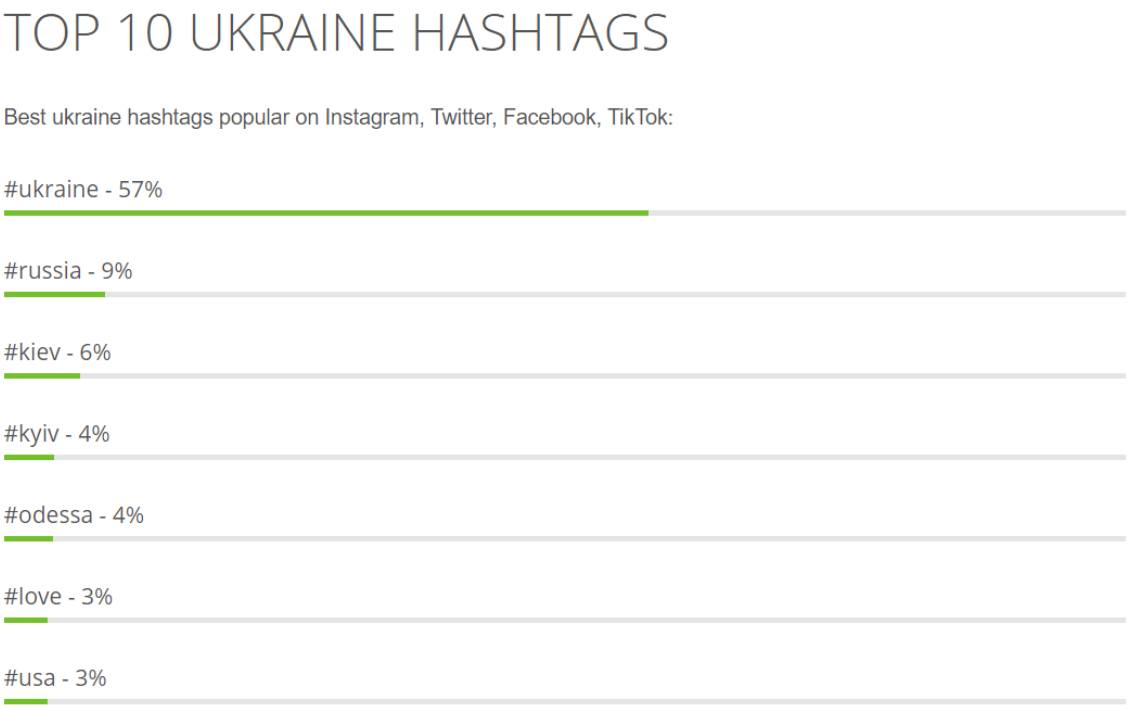
This case study of OSINT use during the Ukraine invasion and research of current American law enforcement has led to several conclusions. The first conclusion is public sentiment towards the nation of Ukraine and American law enforcement are vastly different. This Ukrainian support led to unmatched global crowdsourcing creating a "Russia vs. the world" social media war. The second conclusion is many of the OSINT databases created and utilized during the Ukraine invasion were vital to the successful use of the intelligence. These databases gathered and organized all related OSINT to one central location. The third conclusion is OSINT technology is rapidly evolving and requires constant training and reevaluation of its current use. Several times since the February 2022 invasion, technology has improved, thus capabilities have improved that successfully aided Ukraine to defend against Russian attacks. Inconsistencies in law enforcement agency sizes, funding, resources, and training have resulted in the inability to provide OSINT training.

A. UKRAINE PUBLIC SUPPORT

President Putin and the Russian government were displaying signs of an imminent attack prior to the February invasion. Global media coverage proved inconsistencies with Russian coverage of Ukraine relations and debunked Russian dis- and misinformation. This led to the overwhelming support of Ukraine and its citizens.

A 2022 poll showed that 82% of Americans considered Russia an "enemy," compared to 65% prior to the invasion.[147] This same poll shows 76% of Americans consider Ukraine an "ally" compared to 49% prior to the invasion.[148] Table 3 shows the most popular Ukraine-related "hashtags from several popular social media platforms."[149]

Table 3. Top 10 Ukraine hashtags[150]



Due to the mass sharing of pro-Ukraine and anti-Russian information on social media, the world saw crowdsourcing on an incomparable level. The valuable military strategic information contained in these posts was shared across the globe in real-time.

[147] Carla Babb, "Poll: Majority of Americans Support Continued Aid for Ukraine," *VOA*, December 1, 2022, https://www.voanews.com/a/poll-majority-of-americans-support-continued-aid-for-ukraine/6858460.html.

[148] Babb.

[149] best-hashtags.com, "Hashtags for #ukraine to Grow Your Instagram, TikTok," Hashtags for #ukraine, accessed January 16, 2023, https://best-hashtags.com/hashtag/ukraine/.

[150] Source: best-hashtags.com.

Ukraine supporters shared their information pulled from these posts through open-source technology. This information was then confirmed by thousands of others around the world (including military strategists) and ultimately relied upon as credible intelligence.

The public's sentiment towards the use of OSINT in American law enforcement is different from the world's sentiment towards OSINT use in aiding Ukraine. The nation's political polarization and relatively recent, reoccurring, fatal encounters between law enforcement and citizens have led to a lack of trust in law enforcement. A 2020 Pew survey showed that, while most Americans had at least "some confidence" in police, only 26% had a "great deal of confidence in the police."[151] Additionally, these numbers lowered significantly for young adults compared to middle-aged or older Americans.[152]

Crowdsourcing was paramount in the Ukraine case study and its success relied heavily on the public's support of Ukraine. Law enforcement must improve their trust within the communities to create an environment of similar crowdsourcing support to proactively prevent crime. The "young adults" age bracket is the most crucial demographic because of their understanding and reliance upon social media. Law enforcement must promote success stories of OSINT utilization that prevented criminal acts that the public deems as morally inexcusable. Examples of OSINT's success in preventing mass shootings or crimes against children and animals are ways to encourage crowdsourcing to aid law enforcement.

Crowdsourcing played a role in the apprehension of the Tsarnaev brothers in 2013 after the 2014 Boston Marathon bombing that left three citizens dead and hundreds injured. Within hours of the attack, the FBI requested the help of the public to identify the suspects, specifically sharing any "photos, videos, or anything specific."[153] This was prior to many modern social media platforms, but Reddit and 4Chan saw increased traffic, and Reddit

[151] Shannon Greenwood, "Trust in America: Do Americans Trust the Police?," Pew Research Center, January 5, 2022, https://www.pewresearch.org/2022/01/05/trust-in-america-do-americans-trust-the-police/.

[152] Greenwood.

[153] Chenda Ngak, "Crowdsourcing or Witch Hunt? Reddit and 4chan Users Attempt to Solve Boston Bombing Case," *CBS News*, April 19, 2013, https://www.cbsnews.com/news/crowdsourcing-or-witch-hunt-reddit-and-4chan-users-attempt-to-solve-boston-bombing-case/.

created a sub-channel called "findbostonbombers" to elicit assistance. In 2014, Philadelphia PD used crowdsourcing to apprehend suspects in a violent attack against a same-sex couple while dining in the downtown area. Twitter User @FanSince09 used his thousands of followers to assist Detective Joseph Murray by sending him posts, photos, and tips. Murray stated after the investigation, "This is how Twitter is supposed to work for cops. I will take a couple thousand Twitter detectives over any one real detective any day."[154] This demonstrates the value of communities working with law enforcement when the public overwhelmingly agree that the suspects must be apprehended and prevented from causing further harm to others.

These are two examples of criminal acts that have been deemed by the American majority as morally inexcusable. Because they are high profile, especially the Boston Bombing, they have been exposed to the public by major media outlets. There are countless similar cases on local levels that must be publicized to show the value of crowdsourcing to the American public.

B. UKRAINE OSINT DATABASE

Many platforms were created during the Ukraine invasion that aided users in organizing and visualizing the mass amounts of data. These platforms were useful in centralizing all relevant information and separating intelligence into categories by date, location, or event type. Dattalion is a website organized and operated by volunteers. The website boasts that the database contains 5,500 videos and 26,100 photos and states, "We want to counter the russian government's misinformation about what we are living through in this war."[155] These various databases make the information user-friendly for the end user. Figure 31's "Eyes on Russia Map" organizes all the data, color codes the intel based on event type and places them on a map.[156]

[154] Tim Jimenez, "Social Media Users Help ID Suspects in Alleged Assault of Same-Sex Couple in Center City," *CBS News Philadelphia*, September 17, 2014, https://www.cbsnews.com/philadelphia/news/social-media-users-help-id-suspects-in-assault-of-same-sex-couple-in-center-city/.

[155] "Dattalion: Ukraine's Data Battalion," Dattalion, accessed January 16, 2023, https://dattalion.com/.

[156] "Eyes on Russia Map," C4ADS Innovation for Peace, accessed January 16, 2023, https://eyesonrussia.org/.

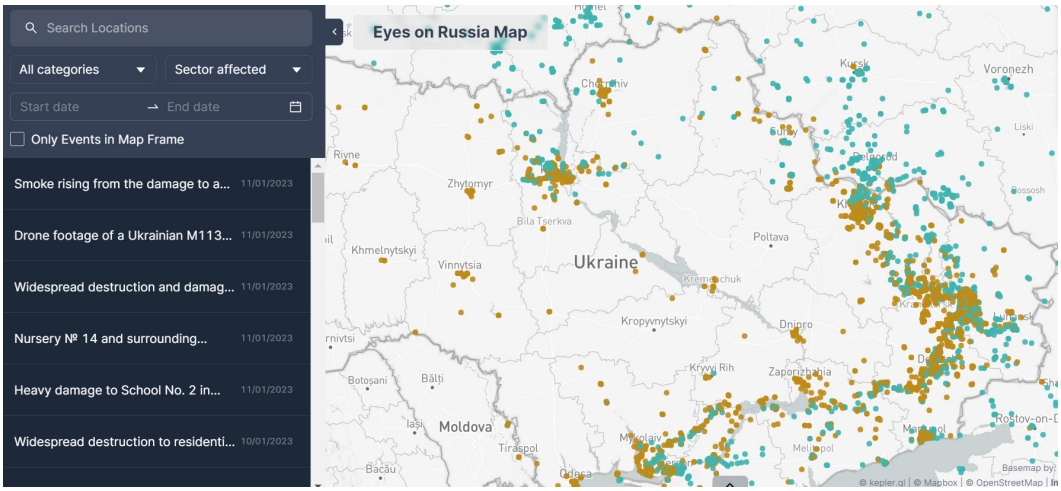


Figure 31. Eyes on Russia

The picture (Figure 32) on the left shows a user's view of "liveuamap." This platform uses "bomb pins," to show users the locations of explosive attacks. It also shades the areas dark red that are currently engaged in increased conflict.[157]

[157] "Ukraine Interactive Map - Ukraine Latest News," Ukraine Interactive map, accessed January 16, 2023, https://liveuamap.com/.

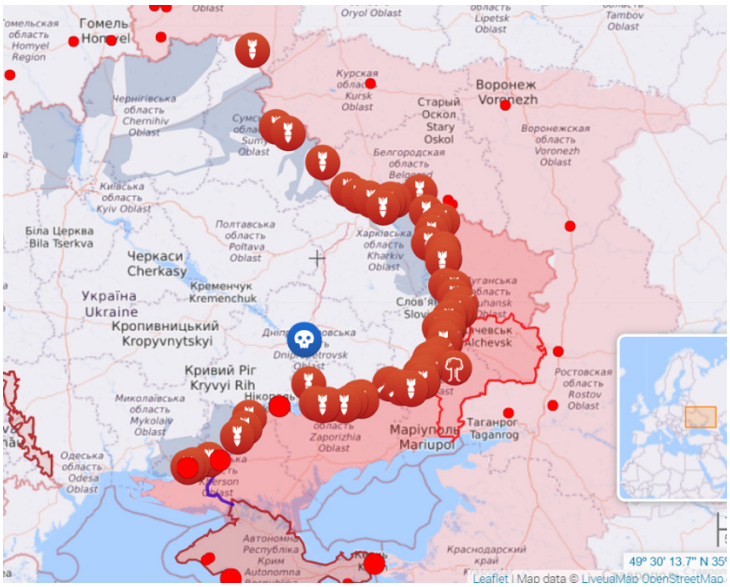


Figure 32. Liveuamap[158]

Both platforms and many other similar technologies formed prior to and during the invasion. This demonstrates the necessity of a database that contains intelligence to make information sharing more accessible for the end user. When intelligence is in one central location, it expedites access to information and increases usability for the customer.

American law enforcement has no designed OSINT database or platforms. The National Crime Information Center (NCIC) is a national database containing criminal information designed for the "rapid exchange of information between criminal justice agencies."[159] NCIC is utilized by federal, state, and local law enforcement agencies for daily investigations. Law enforcement sensitive information is entered into the NCIC database, so it is available to all officers who have access around the country. NCIC includes information such as active warrants, sexual offenders, stolen firearms, suicidal subjects, and other important information. It does not include OSINT if it does not fit into designated categories.

[158] "Ukraine Interactive Map."

[159] "National Crime Information Center (NCIC) - The Investigative Tool - A Guide to the Use and Benefits of NCIC," NCJRS Virtual Library, 1984, https://www.ojp.gov/ncjrs/virtual-library/abstracts/national-crime-information-center-ncic-investigative-tool-guide-use.

Current dissemination methods of OSINT vary by agency and state or jurisdiction. "Be on the lookouts" (BOLOs) are flyers emailed or passed around to agencies containing a subject's personal information and other information relevant to law enforcement. BOLOs are either regional or national and include crucial information gathered from OSINT. These individuals make threats against law enforcement or the public on various social media platforms or post videos with specific weapon types. Depending on the nature of the BOLO, the information is not entered into any national database that is available to the officers who may encounter these individuals. There is no central location for this information and there are countless times that subjects carry out violent or deadly attacks on the public and law enforcement because of this information gap. In tourist destinations such as Washington, D.C., New York City, and Los Angeles, officers must have this information to protect the community from subjects intent on committing acts of violence.

C. LAW ENFORCEMENT COLLECTION STANDARDS

The lack of collection standards is identified as a hindering factor to OSINT maximization. The OSINT collected in the Ukraine case study was completed by citizens of the world who are not bound by any federal state or local laws, and it is not possible to know their training or level of experience. Based on these facts, it is implausible to draw a correlation between OSINT collection standards in the Ukraine invasion and OSINT collection standards in American law enforcement.

This research finds the lack of OSINT collection standards is the result of many factors. American law enforcement agency sizes, funding, and training vary tremendously. There are over one million police officers in the United States.[160] These officers make up approximately 18,000 municipal, state, and county departments nationwide. Eighty-seven percent (87%) of these agencies are comprised of 25 or fewer police officers.[161] The largest police department in the country is the New York City Police Department with just under

[160] USAFacts, "Police Departments in the US: Explained," April 28, 2021, https://usafacts.org/articles/police-departments-explained/.

[161] Darlena Cunha, "The Average Size of a Police Department," Classroom, October 4, 2017, https://classroom.synonym.com/the-average-size-of-a-police-department-13583335.html.

40,000 sworn members. Washington, DC, and New York State have the highest number of officers per capita (6.5 and 4.3 per 1,000 residents).[162]

In 2021, the Council on Criminal Justice formed the Task Force on Policing, comprising individuals from various backgrounds including police officers, politicians, civil rights activists, and police oversight advocates. They highlighted a shocking discrepancy in the number of hours of initial police recruit training among U.S. law enforcement agencies. The average law enforcement academy training in the United States is approximately 6 months. However, the state of Hawaii requires over 1,000 hours of initial training, while the state of Georgia requires only 404 hours.[163]

The United States spent $215 billion on law enforcement in 2022.[164] Republican states spent an average of $544 per capita on law enforcement while Democrat states spent an average of $757 per capita.[165] Washington, DC, spent $1,337 per capita and Kentucky spent $390 per capita.[166] Florida spent 7.3% of their budget on law enforcement and corrections while Iowa spent 3.4% of its budget on the same resource.[167] These discrepancies in state spending demonstrate the inconsistent prioritization of law enforcement. This results in the various training standards as previously discussed.

Lack of uniformity in agency size and populations contributes to discrepancies in law enforcement agencies' funding on a county level. The USAFacts 2017 graph (shown in Figure 33) shows "Law enforcement per capita in counties with more than 200,000 residents:[168]

---

[162] USAFacts, "Police Departments in the US."

[163] Task Force on Policing, "Task Force Calls for Overhaul of U.S. Police Training, National Standards to Reduce Use of Force," March 22, 2021, https://policing.councilоncj.org/2021/03/22/task-force-calls-for-overhaul-of-u-s-police-training-national-standards-to-reduce-use-of-force/.

[164] Ingrid Cruz, "Policing and Corrections Spending by State," MoneyGeek, October 19, 2020, https://www.moneygeek.com/living/state-policing-corrections-spending/.

[165] Cruz.

[166] Cruz.

[167] Cruz.

[168] USAFacts, "How Much Do America's Biggest Counties Spend on Police?," October 1, 2020, https://usafacts.org/articles/police-funding-local-governments/.

Figure 33. Law enforcement per capita spending[169]

These discrepancies lead to different agencies with access to various technology because of budgetary constraints. This was very apparent during the implementation of body-worn cameras in American law enforcement. The Bureau of Justice Statistics published a report in November 2018 that showed 80% of "large law enforcement agencies" had equipped their officers with body-worn cameras compared to the 47% national average.[170] This same study showed that agencies without body-worn cameras identified cost as the main reason for not equipping their officers with this technology.

A 2013 PERF study found that a police agency of 100 spends approximately $86,000 in year one to start a body-worn camera (BWC) program.[171] This covers the cost of the camera as well as the storage/cloud monthly data fees. This demonstrates the high-priced equipment and upkeep that is required for the successful implementation of technology relevant and required by law enforcement. The majority of law enforcement agencies and the public have placed a high priority on body-worn cameras to improve

[169] Source: USAFacts.

[170] National Institute of Justice, "Research on Body-Worn Cameras and Law Enforcement," January 7, 2022, https://nij.ojp.gov/topics/articles/research-body-worn-cameras-and-law-enforcement.

[171] Cliff Judy, "The Cost of Police Body Cameras," *Atlanta Journal-Constitution*, April 12, 2015, zhttps://www.ajc.com/news/national/the-cost-police-body-cameras/gS80Bxexi9R6zC6TXxfhjI/.

transparency in law enforcement interactions with citizens. OSINT is not as highly prioritized as BWCs and thus requires more consistency amongst agency priorities.

Technology is expensive and requires regular investments for updates and new equipment. With the rapid evolution of OSINT technology and platforms, there is a requirement for a similar prioritization of OSINT and funding. Funding for this technology must include the personnel and training dedicated to this form of intelligence. Regular upkeep and training for technological advancements and any emerging sources is a necessity.

VI. RECOMMENDATIONS AND CONCLUSION

The law enforcement intelligence community agrees on the significance of open-source intelligence in preventing and prosecuting crime. OSINT accounts for the majority of intelligence utilized by law enforcement and prevents violent crimes and provides valuable evidence in prosecuting criminals. Law enforcement relies on social media OSINT due to the increase in platforms, the evolution in social media technology, and the high percentage of Americans who use these platforms.

This thesis argues for maximum use of OSINT in American law enforcement. The research included the history and evolution of OSINT, challenges and obstacles, social media OSINT, and the current use of OSINT in law enforcement. A case study was conducted on the use of OSINT in the ongoing Ukraine-Russian conflict. Social media OSINT prior to the February 2022 invasion and during the initial weeks after the invasion were studied. Individual posts were used to highlight the crowdsourcing that occurred by citizens around the world that aided the Ukrainian government and citizens in the invasion by Russian forces.

A. RECOMMENDATIONS

Several recommendations can be formed through the OSINT Ukraine case study and the research on current American law enforcement use of OSINT. The first recommendation is to inform and educate the public of the OSINT benefits for public safety and the prevention of violent crimes to encourage crowdsourcing. The second recommendation is for a national OSINT database to increase consistent dissemination of real-time OSINT. The third recommendation is for a national-level committee to form OSINT collection best practices to disseminate to law enforcement intelligence analysts and fusion centers.

1. Solicit Public Crowdsourcing

As discussed in the case study, crowdsourcing was vital to the successful use of OSINT prior to and during the Ukraine invasion. Information was rapidly spread around

the world and citizens acted as intelligence analysts to assist Ukraine. This was then used by Ukrainian officials as intelligence to plan against Russian invasions and future attacks. American law enforcement has had similar public assistance in cases of mass shootings, crimes against children, or other criminal or socially unacceptable behavior.

Building and increasing trust with the public plays a foremost role in this task. The support for law enforcement changes often depending on the political climate and current events. Demonstrating the benefits of crowdsourcing OSINT during a period of high law enforcement support will yield the best results. Demonstrating how crowdsourcing and utilizing OSINT could have prevented events such as the Boston Bombing, Pulse nightclub shooting, or Sandy Hook shooting would influence the public and yield the greatest effect.

Many mass shootings have been thwarted by anonymous tips to law enforcement regarding troubling social media posts. Like a "hotline" or "tipline," law enforcement can establish digital platforms for information that would gather OSINT to proactively prevent crime. Communication with the public through these platforms is key to success. Reiterating that crowdsourcing would be used for heinous acts against society and not minor property or drug offenses would be important.

This "buy-in" would overcome two major obstacles identified in the research. This would improve public sentiment related to law enforcement's use of OSINT and aid in its tedious analysis process. An increase in crowdsourcing could result in an increase of vigilantism. Suspects are confidential in most law enforcement investigations and suspect information is not released to the public until there is probable cause for an arrest. Prior confidential suspect and/or suspect information may become available to the public before an arrest is made. This may result in endangering the suspect or revealing victim information to the public. These effects are outside the scope of this thesis and would require additional research.

2. National OSINT Database

The second recommendation is the creation of a national OSINT database. This OSINT database would be similar to the NCIC database and would result in a rapid

exchange of open-source intelligence between local and state police agencies. Although the OSINT database is publicly available information, the information in the database would remain law-enforcement–sensitive. Because the information would have been collected and analyzed for law enforcement, the public would not have access to this database.

The OSINT database would require one central body for regulation, though contributions would be made by all agencies. OSINT gathered and analyzed from different agencies could be used to build the national database. Agencies would require dedicated sworn or civilian personnel for OSINT collection and analysis. These members would require initial training as well as regular training because OSINT platforms and technology are always evolving. These units would work with state and federal fusion centers to accomplish this task.

Intelligence officers would be covered from legal ramifications if they were sending this information to the OSINT database for dissemination. Because of this, intelligence officers would collect, analyze, and disseminate information to distribute for proactive and investigative purposes. A national database would cause fewer issues during judicial hearings where the information was used towards probable cause for an arrest. The OSINT database similar to multiple national databases used daily by thousands of law enforcement officers would create more trust in the community. The OSINT database for information sharing would lower public scrutiny of law enforcement OSINT utilization because all intelligence would be disseminated from a central database based on national standards.

Law enforcement has the ability to run one individual in multiple databases at the same time. Ideally, the national OSINT database could be integrated into in this process. If an individual is run for warrants, missing person, etc., the OSINT database would also be searched to display information to the requesting officer. This recommendation would require federal funding to complete. Contracting a technology company to create and manage the software of this database would be an added cost. Currently, some law enforcement agencies issue their officers cell phones while others do not. The OSINT database could be used as an app on a smartphone or on a mobile data terminal (MDT/ cruiser computer). Larger police departments have the funding to support this program,

though smaller agencies do not. Federal funding would be required to encourage smaller to medium-sized agencies to buy into the program and equip their officers with the technology.

Citizen buy-in is not as essential as the first recommendation for this national database. The first recommendation depends entirely on citizen involvement and participation. This database could be launched and implemented with no public support if every agency possessed equal funding and highly prioritized intelligence. Because this is not feasible, federal funding is required to start, maintain, and incentivize the program to smaller agencies. Gaining support from the federal government would require gaining support from the other stakeholders. Constituents vote and representatives run on varying political platforms, creating the need for support from the other stakeholders.

Several foreseeable obstacles could arise that would obstruct the implementation of an OSINT national database. Law enforcement culture is a major obstacle to any change. This database would require complete buy-in from all agencies and fusion centers to accomplish the intended goal. Agency leaders and management would need to promote and invest in this program. They would need to work with the public to gain their support and assistance for an effective program.

The program could be interpreted by the public as a "big brother" government intrusion tool. Rights' advocate organizations would likely protest an additional national database of information, even if gathered from open sources. The allocation of federal sources is a topic of debate and there would be critics from all political sides that would attempt to prevent the success of this program. Data and supporting court cases on the legality of OSINT use and dissemination must be transparent to the public to decrease uncertainty.

3. National Collection Standards Committee

The varying agency sizes and lack of training standards result in different initial intelligence collection training. The third recommendation is the formation of a national committee to establish "best practices" for collection standards. These collection standards

would be disseminated to analysts and fusion centers around the nation to encourage consistent collection standards.

While the first two recommendations rely heavily upon citizen buy-in and support, this recommendation involves communication and buy-in with the law enforcement community. The value of OSINT collection standards must be emphasized to police departments of all sizes. Valuable networking venues such as the International Association of Chiefs of Police conferences and intelligence/detective conferences should all be briefed on the intended standards and their benefits to law enforcement. Law enforcement publications and social media sites would also be platforms for communication. Many retired police officers and subject matter experts have an influence on police agencies because of past experience and knowledge.

This effort would require minimum funding compared to the second recommendation. The costs would include forming a working group to study current best practices around the nation. There are countless intelligence professionals who would make invaluable contributions to this effort. The committee would require representatives from agencies of various sizes, and local, state, and federal agencies. The committee would also benefit from scholars and academics who study open-source intelligence and legal representatives who could forecast potential legal ramifications.

These best practices would be evaluated as often as necessary to determine if technological advancements, evolving social media platforms, or federal case law have resulted in necessary amendments. The national committee would also include individual state or local restrictions on OSINT collection. Educating intelligence analysts will enhance their understanding of their collection restrictions and boundaries. Analysts will have a guide of the most efficient and effective collection methods and clear insight into their local scope of collection standards.

Feedback and evaluation from analysts must be studied to improve the recommendations to implement this program. This cannot be a standard government working group that sends out recommendations and does not follow up and ignores after-action reports. The research shows the complexity of open-source social media platforms

and their constantly evolving nature makes them a unique form of intelligence. Because of this, consistent evaluations of standards are a necessity. The committee must add civilians who have the knowledge and training of new OSINT technology as it develops.

There are overlapping obstacles with the second recommendation to the success of this committee. Law enforcement culture and resistance to change is the most readily perceived hindrance. The stronghold of intelligence, lack of transparency of intelligence collection methods, and the reluctance to receive and implement federal training or recommendations all contribute to this problem. These issues and their improvement are out of the scope of this thesis and would require additional research.

B. LIMITATIONS

The case study was chosen because of the ease of access to a plethora of information related to a current event at the time of research. There are other examples of OSINT being utilized during international events, however, none are as widespread and well-documented as this conflict. There is a clear difference between an international, strategic military invasion and everyday American law enforcement planning, tactical, and logistical operations. The military is not bound by the same laws and regulations as law enforcement and American values and culture differ from Ukraine's.

The Ukraine-Russia conflict is still occurring and evolving, and technology has drastically changed and adapted since the case study was conducted. The case study was conducted in the weeks prior to the invasion and the weeks following to limit the amount of data to be studied. The conflict is still emerging and there has been a year of war since the case study timeframe and the time of this writing. Social media OSINT has been used by both sides in different manners that were not discussed in this thesis.

This thesis connected Ukrainian military decisions and OSINT that were collected, analyzed, and disseminated by the public. It is not possible to know what influenced these military decisions because there is classified information that was not available during the case study. Only years after the conflict has been resolved will this information be available for review and research.

The research on American law enforcement OSINT utilization was conducted during a time period when trust and law enforcement credibility is at a historic low. Because of the high-profile events that led up to the 2020 protests and civil unrest, there is a rift in the relationships between agencies and communities. Skepticism and suspicion of law enforcement are high during a period with constantly evolving social media open-source intelligence platforms. It is challenging to weigh the potential impacts or law enforcement and public partnerships during this tumultuous environment.

C. FURTHER RESEARCH TO BE CONDUCTED

There are domestic incidents where OSINT and crowdsourcing were utilized that yielded successful results. Two of these incidents were briefly referenced in this thesis and should be examined and studied. The first highly publicized U.S. mass shooting was at Columbine High School in 1999. There have been hundreds of similar events since then, and during this time, social media and other open-source intelligence have evolved. OSINT has been released after many of these events by local or federal law enforcement that can be researched.

OSINT's role in the attack on the U.S. Capitol on January 6, 2021, can be researched in detail and in many ways. The FBI's request to the public for assistance has led to hundreds of prosecutions and can be researched; how the rioters used OSINT to organize the attack can also be researched. The failure of intelligence has been researched and reported by many, including several committees and intelligence professionals. Research can be conducted on the success that OSINT provided to local law enforcement in preparing for that day.

Public sentiment towards law enforcement is a recurring theme in this thesis and is visited in every chapter. Methods to increase public trust and decrease polarization are important for OSINT utilization. Research can be conducted on a correlation between law enforcement technology and a decrease in violent criminal acts. Studies and research similar to this can assist in communicating the necessity of OSINT utilization by law enforcement.

The capabilities of OSINT technology have not been fully exposed due to its complexity and technical nature. Engineers and IT experts should be included by law enforcement and homeland security professionals when conducting future research on these evolving and complicated platforms. OSINT technology such as geospatial and satellite imagery can be researched as it is frequently being utilized by the American public on social media.

D. CONTRIBUTION

The Ukraine-Russia conflict is relatively recent and ongoing, so there is currently little research available on OSINT's impact on the conflict. The case study highlighted theories and practices that will improve American law enforcement OSINT utilization. Although an international military conflict, there are practical applications that can be applied to American law enforcement. The crowdsourcing and analysis of the OSINT that was researched during the Ukraine conflict were performed by citizens of all different backgrounds and cultures, similar to the communities in the United States.

This thesis studied an emerging 21st century international conflict and the accompanying military decisions based on current social media OSINT technology. These recommendations were extrapolated from this international conflict and can be applied to American law enforcement. The recommendations in this thesis are not easily implemented and require public, local, state, and federal buy-in and funding. If implemented, these recommendations would have a major impact on American law enforcement and public safety.

E. SUMMARY

American law enforcement relies heavily on open-source intelligence to make logistical and tactical decisions that directly affect public safety. The antiquated state, local, and federal governments have not evolved as quickly as OSINT technology has developed. The archaic approach to technology combined with stubborn law enforcement culture, and inconsistent national law enforcement agency funding and training have led to inconsistent collection and dissemination methods.

Public crowdsourcing of OSINT prior to the Ukraine invasion by Russian forces aided the Ukrainian government to prepare for the attack. After the invasion, OSINT was utilized by Ukrainian soldiers and citizens to counter Russian attacks and military conflicts. Key factors that led to this success were global crowdsourcing due to the overwhelming support of Ukraine, databases to centralize all relevant OSINT and the quick response to evolving OSINT technology.

American law enforcement should adopt similar practices to improve public safety and prevent acts of violence against citizens. Engaging the American public in crowdsourcing social media OSINT will significantly decrease the overwhelming amount of raw data for analysts. Centralizing OSINT in an easily accessible law enforcement database will result in a consistent dissemination method. A national committee to continuously research new OSINT technology will create consistent collection methods. Increasing trust and confidence with the public is paramount to the success of these practices.

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF REFERENCES

4emberlen [@4emberlen]. "Севастополь [Sevastopol] 08.02.2022 https://t.co/HWuf8mXjUe." Tweet. *Twitter*, February 9, 2022. https://twitter.com/4emberlen/status/1491366702676066309.

Agence France Presse. "Russia-Ukraine War: Russian Tanks Attacked Humanitarian Corridor in Mariupol." NDTV, March 11, 2022. https://www.ndtv.com/world-news/russia-ukraine-war-russian-tanks-attacked-humanitarian-corridor-in-mariupol-ukraine-president-volodymyr-zelensky-2816343.

Akhgar, Babak, and Douglas Wells. "Critical Success Factors for OSINT-Driven Situational Awareness." *European Law Enforcement Research Bulletin* Special Conference Edition Nr. 4 (2019): 67–74. https://bulletin.cepol.europa.eu/index.php/bulletin/article/view/332.

Babb, Carla. "Poll: Majority of Americans Support Continued Aid for Ukraine." VOA, December 1, 2022. https://www.voanews.com/a/poll-majority-of-americans-support-continued-aid-for-ukraine/6858460.html.

BBC. "Internet Brings Events in Iran to Life." BBC, June 15, 2009. http://news.bbc.co.uk/2/hi/middle_east/8099579.stm.

bellingcat. "About." Accessed February 27, 2023. https://www.bellingcat.com/about/.

Best, Clive. "Challenges in Open Source Intelligence." In *2011 European Intelligence and Security Informatics Conference*, 58–62. IEEE, 2011. https://doi.org/10.1109/EISIC.2011.41.

Best Hashtags. "Hashtags for #ukraine to Grow Your Instagram, TikTok." Hashtags for #ukraine. Accessed January 16, 2023. https://best-hashtags.com/hashtag/ukraine/.

Bloomberg. "A Visual Guide to the Russian Invasion of Ukraine." Bloomberg. Accessed October 6, 2022. https://www.bloomberg.com/graphics/2022-ukraine-russia-us-nato-conflict/.

Böhm, Isabelle, and Samuel Lolagar. "Open Source Intelligence." *International Cybersecurity Law Review* 2, no. 2 (2021): 317–37. https://doi.org/10.1365/s43439-021-00042-7.

Boren, David, Bill Bradley, Frank Carlucci, William Cohen, Robert Gates, John Hamre, Gary Hart et al. "Guiding Principles for Intelligence Reform." *Congressional Record* 150, no. 114 (September 21, 2004): S9428–29. https://www.congress.gov/congressional-record/volume-150/issue-114/daily-digest.

Borlay, Tim. “Pro-Russian Authorities in Mariupol Put Civilian Dead at 5,000.” Turned News, April 8, 2022. https://turnednews.com/pro-russian-authorities-in-mariupol-put-civilian-dead-at-5000-war-in-ukraine/.

Bureau of Conflict and Stabilization Operations. “History of Russia’s Aggression against Ukraine.” U.S. Department of State, February 11, 2022. https://storymaps.arcgis.com/stories/f477e2c9a9154df3af8508ad1caef919.

CCJ Task Force on Policing. “Task Force Calls for Overhaul of U.S. Police Training, National Standards to Reduce Use of Force.” Task Force on Policing, March 22, 2021. https://policing.councilоncj.org/2021/03/22/task-force-calls-for-overhaul-of-u-s-police-training-national-standards-to-reduce-use-of-force/.

Central Intelligence Agency. “The Office of Strategic Services: America’s First Intelligence Agency.” CIA Museum Exhibits. Accessed November 15, 2022. https://www.cia.gov/legacy/museum/exhibit/the-office-of-strategic-services-n-americas-first-intelligence-agency/.

Centre for Information Resilience. “Eyes on Russia Map.” C4ADS Innovation for Peace. Accessed January 16, 2023. https://eyesonrussia.org/.

Chris N [@chrisdneumann]. “@JC_Monitoring @nigroeneveld Nice. Right next to the New Bridge over the Pripyat River.” Tweet. *Twitter*, February 16, 2022. https://twitter.com/chrisdneumann/status/1493773632367054856.

Cleary, Christopher J. “Strategy for Local Law Enforcement Agencies to Improve Collection, Analysis and Dissemination of Terrorist Information.” Master’s thesis, Naval Postgraduate School, 2006. https://hdl.handle.net/10945/2892.

Codruţa Luţai, Raluca. “Open Source Intelligence: Opportunities and Challenges.” *Strategic Impact*, no. 1 (2020): 95–109. ProQuest.

Colquhoun, Cameron. “A Brief History of Open Source Intelligence.” Bellingcat, July 14, 2016. https://www.bellingcat.com/resources/articles/2016/07/14/a-brief-history-of-open-source-intelligence/.

Council on Criminal Justice. “Public Perceptions of the Police.” Council on Criminal Justice, October 7, 2020. https://councilоncj.org/public-perceptions-of-the-police/.

“Counter Terrorism and Homeland Security Threats | Homeland Security.” Accessed February 27, 2023. https://www.dhs.gov/counter-terrorism-and-homeland-security-threats.

Cruz, Ingrid. “Policing and Corrections Spending by State.” MoneyGeek, October 19, 2020. https://www.moneygeek.com/living/state-policing-corrections-spending/.

Cunha, Darlena. "The Average Size of a Police Department." Classroom, October 4, 2017. https://classroom.synonym.com/the-average-size-of-a-police-department-13583335.html.

Dattalion. "Dattalion: Ukraine's Data Battalion." Dattalion. Accessed January 16, 2023. https://dattalion.com/.

Dixon, Robyn. "In Long Speech, Putin Recognizes Two Ukrainian Regions as Independent, a Potential Pretext for War." *Washington Post*, February 21, 2022. ProQuest.

Ekins, Emily. "Policing in America: Understanding Public Attitudes toward the Police. Results from a National Survey." Cato Institute, December 7, 2016. https://www.cato.org/survey-reports/policing-america-understanding-public-attitudes-toward-police-results-national.

"Fake: A Child Died in Donbas as a Result of a Ukrainian Drone Attack (Update) | StopFake," April 29, 2021. https://web.archive.org/web/20210429183210/https://www.stopfake.org/en/fake-a-child-died-in-donbas-as-a-result-of-a-ukrainian-drone-attack/.

Fresenko, Victoria L. "Social Media Integration into State-Operated Fusion Centers and Local Law Enforcement: Potential Uses and Challenges." Master's thesis, Naval Postgraduate School, 2010. https://hdl.handle.net/10945/4996.

Gill, Shubhnoor. "12 Top Data Mining Tools in 2022." Hevo, December 21, 2021. https://hevodata.com/learn/data-mining-tools/.

Green, Prioleau. "An Analysis of the Requirements and Potential Opportunities for the Future Education of Law Enforcement Intelligence Analysts." Master's thesis, Naval Postgraduate School, 2008. https://hdl.handle.net/10945/4235.

Greenwood, Shannon. "Trust in America: Do Americans Trust the Police?" Pew Research Center, January 5, 2022. https://www.pewresearch.org/2022/01/05/trust-in-america-do-americans-trust-the-police/.

Guenot, Marianne. "Satellite Photos Show Russia's Final Troop Deployments around Ukraine before Putin Launched an Invasion." Business Insider, February 24, 2022. https://www.businessinsider.com/satellite-images-show-final-russia-troop-deployments-before-ukraine-invasion-2022-2.

Guy Agam Fusfus [@gfusfus]. "@4emberlen This Is the Location the Video Was Taken at and the Estimated Angle of the Photographer at the Attached Frame. The Vehicles Are Heading East, Possibly out of Sevastopol. Cords: 44°34'04.7"N 33°27'40.2"E Https://T.Co/5YBcrMIp5W." Tweet. *Twitter*, February 9, 2022. https://twitter.com/gfusfus/status/1491433454474764294.

Haltiwanger, John. "Russian President Vladimir Putin Announces Military Assault against Ukraine in Surprise Speech." Business Insider, February 23, 2022. https://www.businessinsider.com/putin-announces-military-assault-against-ukraine-in-surprise-speech-2022-2.

Hamann, Greta. "Mariupol: Before and after Pictures Show Extent of Devastation." Deutsche Welle, April 24, 2022. https://www.dw.com/en/mariupol-before-and-after-pictures-show-extent-of-devastation/a-61570963.

Harding, Emily. *Move Over JARVIS, Meet OSCAR: Open-Source, Cloud-Based, AI-Enabled Reporting for the Intelligence Community*. Washington, DC: Center for Strategic & International Studies, 2022. https://www.csis.org/analysis/move-over-jarvis-meet-oscar.

Harding, Luke. "'Pure Genocide': Civilian Targets in Mariupol 'Annihilated' by Russian Attacks." *The Guardian*, March 9, 2022, sec. World news. https://www.theguardian.com/world/2022/mar/09/pure-genocide-civilian-targets-in-mariupol-annihilated-by-russian-attacks.

Herrington, Vee. "Intelligence Reform Brings New Opportunities for Info Pros." *Information Outlook* 12, no. 3 (March 2008): 10–16. ProQuest.

Hribar, Gašper, Iztok Podbregar, and Teodora Ivanuša. "OSINT: A 'Grey Zone'?" *International Journal of Intelligence and CounterIntelligence* 27, no. 3 (2014): 529–49. https://doi.org/10.1080/08850607.2014.900295.

Hwang, Yong-Woon, Lee Im-Yeong, Hwankuk Kim, Hyejung Lee, and Donghyun Kim. "Current Status and Security Trend of OSINT." Edited by Yan Huo. *Wireless Communications & Mobile Computing* 2022 (2022): 1–14. https://doi.org/10.1155/2022/1290129.

Institute for the Study of War. "Ukraine Conflict Update 7." Institute for the Study of War, February 24, 2022. https://www.understandingwar.org/backgrounder/ukraine-conflict-update-7.

———. "Ukraine Conflict Updates." Institute for the Study of War, August 15, 2022. https://www.understandingwar.org/backgrounder/ukraine-conflict-updates.

Interfax-Ukraine. "At Least 22,000 Civilians Killed in Mariupol – Mayor's Adviser." Interfax-Ukraine, May 25, 2022. https://en.interfax.com.ua/news/general/834794.html.

Ivan, Adrian Liviu, Claudia Anamaria Iov, Raluca Codruta Lutai, and Marius Nicolae Grad. "Social Media Intelligence: Opportunities and Limitations." *CES Working Papers* 7, no. 2A (2015): 505–10. ProQuest.

JC_Monitoring [@JC_Monitoring]. "Russian Convoy of Military Hardware Spotted in Rechytsa, Belarus – Heading Southeast Coordinates – 52.36888653, 30.3429573 Https://T.Co/WDmgBtryvT." Tweet. *Twitter*, February 16, 2022. https://twitter.com/JC_Monitoring/status/1493738346564268032.

———. "Trainload of Russian Military Hardware under the Cover of Darkness, Spotted in Kosmynino, Kostroma Oblast. Coordinates – 57.58571217, 40.75765208 Https://T.Co/H5CUhSwgGH." Tweet. *Twitter*, February 16, 2022. https://twitter.com/JC_Monitoring/status/1494073105249181702.

Jimenez, Tim. "Social Media Users Help ID Suspects In Alleged Assault Of Same-Sex Couple In Center City." CBS News Philadelphia, September 17, 2014. https://www.cbsnews.com/philadelphia/news/social-media-users-help-id-suspects-in-assault-of-same-sex-couple-in-center-city/.

Judy, Cliff. "The Cost of Police Body Cameras." *Atlanta Journal-Constitution*, April 12, 2015. https://www.ajc.com/news/national/the-cost-police-body-cameras/gS80Bxexi9R6zC6TXxfhjI/.

Kemsley, Harry. "In OSINT We Trust?" *The Hill* (blog), September 1, 2021. https://thehill.com/opinion/national-security/569738-in-osint-we-trust/.

Kim, KiDeuk, Ashlin Oglesby-Neal, and Edward Mohr. *2016 Law Enforcement Use of Social Media Survey*. Washington, DC: International Association of Chiefs of Police and the Urban Institute, 2017. https://www.urban.org/research/publication/2016-law-enforcement-use-social-media-survey.

Kirby, Paul. "Why Has Russia Invaded Ukraine and What Does Putin Want?" BBC News, May 9, 2022. https://www.bbc.com/news/world-europe-56720589.

Leibowitz, Aaron. "Could Monitoring Students on Social Media Stop the Next School Shooting?" *New York Times*, September 6, 2018, sec. U.S. https://www.nytimes.com/2018/09/06/us/social-media-monitoring-school-shootings.html.

Live Maps. "Ukraine Interactive Map – Ukraine Latest News." Ukraine Interactive map. Accessed January 16, 2023. https://liveuamap.com/.

Madeline Fitzgerald, and Elliott Davis, Jr. "Russia Invades Ukraine: A Timeline of the Crisis." U.S. *News & World Report*, February 21, 2023. //www.usnews.com/news/best-countries/slideshows/a-timeline-of-the-russia-ukraine-conflict.

Markus, M. Lynne, and Mark S. Silver. "A Foundation for the Study of IT Effects: A New Look at DeSanctis and Poole's Concepts of Structural Features and Spirit." *Journal of the Association for Information Systems* 9, no. 10/11 (2008): 609–32. ProQuest.

Marnin, Julia. "What's Led up to Russia's Invasion of Ukraine? Here's a Brief Look at Their History." MSN. Accessed October 6, 2022. https://www.msn.com/en-us/news/world/what-s-led-up-to-russia-s-invasion-of-ukraine-here-s-a-brief-look-at-their-history/ar-AAUqeFc.

Moshe Schwartz [@YWNReporter]. "I've Geolocated This Video Uploaded 2 Hours Ago to the Belgorod Region of Russia Just 8 Miles from the Ukrainian Border. 50.437254,36.380161 – Use Google Street View, However, Note That You Won't See Street Lights on the Right Side of the Street. See Thread for Details. https://T.Co/CYjyvBkKwI." Tweet. *Twitter*, February 23, 2022. https://twitter.com/YWNReporter/status/1496452064578347009.

Nasr, Octavia. "Tear Gas and Twitter: Iranians Take Their Protests Online." CNN, June 15, 2009. http://www.cnn.com/2009/WORLD/meast/06/14/iran.protests.twitter/index.html.

Natanazart [@natanazart]. "#украина#война#танки#белгород" [Ukraine#war#tanks#Belgorod]. *TikTok*, February 23, 2022. https://www.tiktok.com/@natanazart/video/7066269915409435905.

National Institute of Justice. "Research on Body-Worn Cameras and Law Enforcement." National Institute of Justice, January 7, 2022. https://nij.ojp.gov/topics/articles/research-body-worn-cameras-and-law-enforcement.

Ngak, Chenda. "Crowdsourcing or Witch Hunt? Reddit and 4chan Users Attempt to Solve Boston Bombing Case." CBS News, April 19, 2013. https://www.cbsnews.com/news/crowdsourcing-or-witch-hunt-reddit-and-4chan-users-attempt-to-solve-boston-bombing-case/.

Office of Community Oriented Policing Services, and Police Executive Research Forum. *Social Media and Tactical Considerations for Law Enforcement*. Washington, DC: Office of Community Oriented Policing Services, 2013. https://cops.usdoj.gov/RIC/Publications/cops-p261-pub.pdf.

Office of Justice Programs. "National Crime Information Center (NCIC) – The Investigative Tool – A Guide to the Use and Benefits of NCIC." NCJRS Virtual Library, 1984. https://www.ojp.gov/ncjrs/virtual-library/abstracts/national-crime-information-center-ncic-investigative-tool-guide-use.

Pastor-Galindo, Javier, Pantaleone Nespoli, Félix Gómez Mármol, and Gregorio Martínez Pérez. "The Not Yet Exploited Goldmine of OSINT: Opportunities, Open Challenges and Future Trends." *IEEE Access* 8 (2020): 10282–304. https://doi.org/10.1109/ACCESS.2020.2965257.

———. "The Not Yet Exploited Goldmine of OSINT: Opportunities, Open Challenges and Future Trends." *IEEE Access* 8 (2020): 10282–304. https://doi.org/10.1109/ACCESS.2020.2965257.

Pew Research Center. "Iran and the 'Twitter Revolution.'" *Journalism Project* (blog), June 25, 2009. https://www.pewresearch.org/journalism/2009/06/25/iran-and-twitter-revolution/.

President's Task Force on 21st Century Policing. *Final Report of the President's Task Force on 21st Century Policing*. Washington, DC: Office of Community Oriented Policing Services, 2015. https://www.ojp.gov/ncjrs/virtual-library/abstracts/final-report-presidents-task-force-21st-century-policing.

Puiu, Tibi. "How Open-Source Intelligence (OSINT) Is Exposing the Ukraine War in Real-Time." *ZME Science* (blog), March 15, 2022. https://www.zmescience.com/science/news-science/open-source-intelligence-ukraine/.

Qusef, Abdallah, and Hamzeh Alkilani. "The Effect of ISO/IEC 27001 Standard over Open-Source Intelligence." *PeerJ Computer Science*, 2022, 1–26. https://doi.org/10.7717/peerj-cs.810.

Rigoglioso, Marguerite. "Civil Liberties and Law in the Era of Surveillance." *Stanford Lawyer*, no. 91 (Fall 2014). https://law.stanford.edu/stanford-lawyer/articles/civil-liberties-and-law-in-the-era-of-surveillance/.

Rob Lee [@RALee85]. "Russian Mi-24/35M and Mi-28N Attack Helicopters Flying over the Kakhovka Hydroelectric Power Plant on the Dnieper River. https://Youtube.Com/Watch?V=i1CdPO7brQQ&t=63s https://T.Co/B2sXC9xhGP." Tweet. *Twitter*, February 24, 2022. https://twitter.com/RALee85/status/1496801532066635779.

Rowley, Mark. "Open Source Intelligence – The Cinderella of the Investigative Family?" *The Police Foundation* (blog), October 28, 2021. https://www.police-foundation.org.uk/2021/10/open-source-intelligence-the-cinderella-of-the-investigative-family/.

RT Staff Reporters. "President Putin's February 21 Speech to the Nation – Full Text." *Rio Times*, February 24, 2022. https://www.riotimesonline.com/brazil-news/modern-day-censorship/president-putins-full-text-of-february-21-2022-speech-to-the-nation/.

Silber, Mitchell D. *Domestic Violent Extremism and the Intelligence Challenge*. Washington, DC: Atlantic Council, 2021. https://www.atlanticcouncil.org/in-depth-research-reports/domestic-violent-extremism-and-the-intelligence-challenge/.

Simeone, Matthew J. "The Integration of Virtual Public-Private Partnerships into Local Law Enforcement to Achieve Enhanced Intelligence-Led Policing." Master's thesis, Naval Postgraduate School, 2007. https://hdl.handle.net/10945/3207.

Staniforth, Andrew. "Police Use of Open Source Intelligence: The Longer Arm of Law." In *Open Source Intelligence Investigation: From Strategy to Implementation*, edited by Babak Akhgar, P. Saskia Bayerl, and Fraser Sampson, 21–31. Cham, Switzerland: Springer International Publishing, 2016. https://doi.org/10.1007/978-3-319-47671-1_3.

Tagtekin, Orcun. "Open Source Intelligence: A New Era of Information Gathering." Master's thesis, Utica College, 2014. (ProQuest). ProQuest.

Talmazan, Yuliya. "Satellite Imagery Points to Mass Grave Site near Besieged Mariupol." NBC News, April 22, 2022. https://www.nbcnews.com/news/world/mariupol-mass-graves-identified-satellite-images-rcna25530.

Tom Neven. "'Wild Bill' Donovan: SOF Pioneer." USSOCOM History and Research Office, May 14, 2018. https://www.socom.mil/wild-bill-donovan-sof-pioneer.

Trottier, Daniel. "Open Source Intelligence, Social Media and Law Enforcement: Visions, Constraints and Critiques." *European Journal of Cultural Studies* 18, no. 4–5 (2015): 530–47. https://doi.org/10.1177/1367549415577396.

U. S. Embassy Tbilisi. "Russia Targets Ukraine with Disinformation Campaign." U.S. Embassy in Georgia, January 21, 2022. https://ge.usembassy.gov/russia-targets-ukraine-with-disinformation-campaign/.

Ungureanu, Gabriel-Traian. "Open Source Intelligence (OSINT). The Way Ahead." *Journal of Defense Resources Management* 12, no. 1 (2021): 177–200. ProQuest.

USAFacts. "How Much Do America's Biggest Counties Spend on Police?" USAFacts, October 1, 2020. https://usafacts.org/articles/police-funding-local-governments/.

———. "Police Departments in the US: Explained." USAFacts, April 28, 2021. https://usafacts.org/articles/police-departments-explained/.

Veritone. "How Law Enforcement Builds Transparency and Trust with Technology." A Comprehensive Guide to Using AI in Law Enforcement, September 20, 2022. https://www.veritone.com/blog/law-enforcement-builds-transparency-and-trust-with-technology/.

Waters, Nick. "'Exploiting Cadavers 'and 'Faked IEDs': Experts Debunk Staged Pre-War 'Provocation' in the Donbas." Bellingcat, February 28, 2022. https://www.bellingcat.com/news/2022/02/28/exploiting-cadavers-and-faked-ieds-experts-debunk-staged-pre-war-provocation-in-the-donbas/.

Williams, Heather J., and Ilana Blum. *Defining Second Generation Open Source Intelligence (OSINT) for the Defense Enterprise*. Santa Monica, CA: RAND Corporation, 2018. https://www.rand.org/pubs/research_reports/RR1964.html.

АЗОВ_UA_NATO_USA_יִשְׂרָאֵלiluauseugb [@herooftheday10]. “Белгородская область. На указателе видна надпись Алексеевка. https://t.co/Z71daf1nQL.” [Belgorod region. Alekseevka is visible on the sign]. Tweet. *Twitter*, February 9, 2022. https://twitter.com/herooftheday10/status/1491328464292827136.

THIS PAGE INTENTIONALLY LEFT BLANK

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California