IMSISS
International Master
Security, Intelligence
& Strategic Studies

Erasmus
Mundus

Tracking the Flow of Military Assets and Logistics for OSINT: The Case of the Syrian Civil War

July 2019

2338035

17116325

25113386

Presented in partial fulfilment of the requirements for the Degree of

International Master in Security, Intelligence & Strategic Studies

Word Count: 20,971
Supervisor: Peter Jackson
Date of Submission: July 25, 2019

University of Glasgow

DCU

CHARLES UNIVERSITY

Table of Contents

Table of Figures

Abstract

This research aims to foster a better understanding among decision-makers regarding the potential of Open-Source Intelligence (OSINT) methods and tools to identify, follow, and compromise sensitive military activities based on their logistical footprint, including during overseas combat engagements. To facilitate this understanding, the research first discusses OSINT, the bread and butter of intelligence analysis and collection, from both the perspective of a secrecy spoiler and force multiplier, and in the context of the 21st century information environment. We then explore the issue of military logistics with historical, conceptual and applicative approaches, furthering the concept of Logistical Support Operations (LSOs) and fusing it with OSINT as an emerging nexus. With the OSINT-LSO nexus at the core of our theoretical framework, we affect understanding methodologically through a case study on the Syrian Civil War. Sectioned around three focal points (i.e. Intelligence on Enemy Force Deployment: Russian order of battle in Syria; Forecast: The Trilateral American-British-French Strike on Syria; and Battle Damage Assessment: Israeli Air Force covert raids on Iran in Syria), this case study shows how OSINT platforms or independent analysts have managed to produce the aforementioned intelligence products that rivalled their covert governmental counterparts at times. As OSINT techniques and methods will increasingly proliferate and refine, it is important to draw awareness and produce literature over its nexus with LSOs and potential impact on military operations security (OPSEC) and combat force protection.

1. Introduction

We are living in the golden age of Open-Source Intelligence (OSINT). Massive data proliferation, growing software accessibility and a rapidly enlarging world wide web community have strengthened the potential of open sources. As the information age overhauled all aspects of human interaction, intelligence has also been affected. Rooted in World War II, OSINT has come a long way from translating foreign newspapers. Today, using adequate tools and online channels, OSINT allows us to tune into military conflicts, observe ongoing air strikes, follow tank deployments or survey a country's air defences. While OSINT is often considered the "bread and butter" of intelligence analysis and widely viewed as a force multiplier, few researchers have paid attention to the negative consequences of OSINT. While most scholarly work has focused on conceptualizing OSINT, what it is and what it is not, there is also mentionable pool of literature dealing with the ever-growing capabilities of OSINT. However, very few studies have pointed out that OSINT has also produced a boomerang effect and, moreover, even fewer scholars have produced applicative demonstrations of what OSINT can do (and how).

Intelligence organizations and defence organizations cannot continue to enjoy the spoils of OSINT, without being prepared to counter it. The main sector, in which governments fail to maintain operations security, is in the military logistics department. Due to their large footprint as well as distribution-oriented and multi-party process, military logistics or "logistical support operations" (Kress 2002, 7-12) can be incredibly revealing for military activities abroad. The literature on this topic is also sparse. There is a wide consensus among scholars that, overall, military logistics is largely ignored within the field of strategic studies. The few authors that engage with the topic have approached it either from a historical perspective (i.e. review of the logistical process behind big battles) or a conceptual one (i.e. theory). The small body of practice-oriented literature is mostly produced by military forces with a view to instructing their servicemen in their respective national doctrine, field procedures and tactics (i.e. doctrine papers or field manuals).

The Syrian Civil War is a particularly suitable case study in this regard. It is not only one the most documented wars in history, but also uniquely followed via open-sources and with a near real-time awareness. Many argue that the Syrian conflict is the first social media war (Doucet 2018, 142). Given the myriad of armed forces involved in the conflict and the media attention received, the Syrian Civil War is an optimal test range for OSINT techniques and tools. To both show the efficiency of OSINT in action and profit from the conflict's unique characteristics, the case study is divided in three focal points. Each focal point is based on a different geographical and operational area of the conflict that follows unique military engagements. The case study demonstrates that OSINT methods and tools can be very efficient in following military forces engaged in diverse mission profiles throughout a given conflict (i.e. Syrian Civil War), by deliberately targeting their logistical footprint.

2. Theoretical Background

The following section introduces the concepts of Open-Source Intelligence (OSINT) and military logistics. While vital for facilitating and understanding the case study section, the OSINT-military-logistics-nexus is virtually absent from intelligence and strategic studies. The OSINT sub-section discusses in depth the academic and professional debates surrounding the concept, addressing definitions as well as the role and consequences of OSINT. Moreover, this section showcases selected OSINT online tools by descriptive means and examples, drawing attention to how accessible and efficient they have become.

In stark contrast with OSINT, the issue of military logistics does not enjoy such a rich literature and scholarly coverage. With the help of historical, doctrinal and a limited number of academic texts, the military logistics subsections addresses the basics and expands on the areas of interest for this dissertation, such as Logistical Support Operations (LSO), logistics network models, and lines of communication. This subsection aims to emphasize the importance of background knowledge and research in the analytical process. Bearing in mind the lessons of OSINT, the subsection ends with a demonstration of how increased subject matter know-how can significantly and easily boost the effectiveness of OSINT acquisition tools.

2.1. Open-Source Intelligence (OSINT)

The question of Open-Source Intelligence (OSINT) is central to this thesis. What OSINT is and is not remains subject of an ongoing debate between pragmatic, reflective and conciliatory perspectives. The common denominator among all parties is that OSINT is derived from publically available information and obtained through overt means. However, further down the road, analysts, decisionmakers, experts and scholars break consensus on some key issues. Does OSINT deserve the designation as a separate collection discipline (INT)? Is OSINT revolutionary for collection and analysis? Or is it just overhyped? And, ultimately, is OSINT even intelligence?

2.1.1. What Is OSINT and Why Is It Important?

Due to their pragmatic nature, governmental institutions, and particularly security, defence, and intelligence agencies, tend to have the most concise definitions of OSINT. For example, the United States Defense Intelligence Agency (DIA) views OSINT as a separate collection discipline and defines it as *“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* (DIA 2013, 46, original emphasis).” Likewise, the United States military views OSINT as the “the intelligence discipline that pertains to 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 and information requirement” (US Department of the Army 2012, 1-2).

Some scholars disagree, arguing that OSINT does not draw on covert means and sources to collect secret information – the inherent essence of intelligence – and therefore should not be considered as a separate discipline or part of the covert art at all. Miller (2018), for example, proposes the term of Open-Source Information (OSINF), also existent in governmental use, as an “unmarketable and tardy compromise” (717). Moreover, Michael Warner names “government intelligence” as the sole bearer of the task to produce intelligence. This restricts the intelligence term from being legitimately used by the many self-proclaimed OSINT non-governmental organizations (NGOs), media websites, and companies that emerged in the past decade. A significant part of OSINT work is nowadays conducted by non-governmental personnel for public or commercial interests. While governmental intelligence often incorporates OSINT acquired from the press and other sources in their assessments, according to Scott & Jackson (2004), “these areas cannot reasonably be defined as intelligence activity” (142).

However, there are mutiple middle ground perspectives. Former intelligence senior head and OSINT advocate Mark Lowenthal (2001) claims that OSINT should be viewed as a “facet of each of them [intelligence disciplines] and not an entirely separate discipline” (61). In a RAND report on second generation OSINT, Williams & Blum (2018) agree with Lowenthal’s (2001) assessment and furthermore argue that INTs should be seen as overlapping (7). A similar notion can be found in Mercado (2004), who points out that “the explosion of OSINT is transforming the world with the emergence of open versions of the cover arts of human intelligence (HUMINT), overhead imagery (IMINT) and signals intelligence (SIGINT).” This inherently renders OSINT easier, more affordable, and tempting for government agencies to exploit, therefore increasing OSINT’s legitimacy in the clandestine world.

While the value of OSINT should not be exaggerated, it should also not be understated. Likewise, OSINT should not be viewed simply as a by-product of the high-tech information-rich 21st century. While the 2000s have refined and boosted its potential, OSINT’s coming-of-age occurred almost a century ago (at least in the Transatlantic community). The U.S. Office of Strategic Services (OSS), the CIA’s predecessor, has been exploiting open-sources since World War II. The OSS established an OSINT-driven institution, called the Foreign Broadcast Information Service (FBIS), tasked with collecting open-source information on Nazi Germany and later on the Soviet Union and Warsaw Pact members. Due to the Freedom of Information Act (FOIA), many FBIS assessments are now declassified and accessible on the CIA website. The writing style, format, and language of the FBIS assessments is almost indistinguishable from covert-source declassified analyses (see for example CIA 1953; CIA 1985; CIA 1970). The FBIS was succeeded by the Director of National Intelligence's Open Source Center in 2005.

Beyond just acknowledging the concept, we know that the U.S. Special Operations Forces' (SOF) community is also increasingly embracing the use of OSINT, since the U.S. Marine Corps pioneered it in the military in 1992. However, in relation with the OSINT debate, Steele (2004) argues in his *Special Operations Forces Open Source Intelligence (OSINT) Handbook* that "only when you combine analytic tradecraft - the proven process of intelligence – with the right sources – do you create OSINT" (4). Gruters & Gruters (2018) argue that, in the case of the Air Force, the U.S. Department of Defense (DOD) should attach OSINT squadrons to their Intelligence, Surveillance and Reconnaissance (ISR) groups (100). In a U.S. Joint Special Operations Command (JSOC) publication, Low (2018) furthermore argues that OSINT has even proven its value in denied unconventional warfare (UW) environments and that its exploitation should be enhanced (4). Draeger (2009) also states that "learning to use OSINT directly contributes to the Army's fight for informational superiority" (39), explaining how "ad-hoc Army units successfully exploited OSINT in Afghanistan, Iraq and throughout the world (40)."

By most estimates, 80 percent of U.S. intelligence is derived from open sources. In Hulnick's (2002) words, OSINT is the "bread and butter" of intelligence analysis (566). There are several undeniable advantages that speak for the use of OSINT.

First of all, OSINT is timely and fast, particularly in the golden age of information and communication technology. As of March 2019, over 4.3 billion people or 56 percent of the world population have Internet access (Internet World Stats 2019) and a slightly higher number (4.7 billion) are mobile phone users (Statista 2019). Search engines and social media networks have reached an unprecedented level of popularity. Software applications and platforms, which were previously considered advanced level, are becoming widely accessible. Should a crisis occur in an area of interest, conventional broadcasting stations and social media are fast to report on it, producing valuable information that can be exploited for early warning, contingency planning, and situational awareness. There is no better example of how information relating to watershed events developing in remote locations were rapidly disseminated through OSINT channels than the Arab Spring protests or the Syrian Civil War. As Rovner (2013) points out "social media provides anyone with an iPhone and a Twitter account the ability to report in real time, and the spread of mobile devices means that reports can be sent from otherwise closed societies" (268).

OSINT is inexpensive and easily produced (Draeger 2009, 41). By definition, OSINT is open, free, and widely available. When looking at OSINT, the collector can potentially take intelligence "off the shelf," rather than collecting it with costly and time-consuming assets (e.g. human operatives, unmanned aerial vehicle surveillance, airborne signals interception etc.). While cheaper is not always better, OSINT's primary role is to augment, not replace traditional collection.

OSINT aids resource management efforts by taking over adequate tasks and freeing other INTs for more specialized or demanding collection duties (Steele 1995, 458). Furthermore, there are way more human resources outside the intelligence community, such as experts, scholars, journalists, bloggers, "intelligence minutemen" (see Politi 2010) than clandestine service members. For example, OSINT can provide historical context (Gibson 2004, 20) and fill basic collection gaps for analytical requirements. If properly enlisted, this support can be a true force multiplier for the collector.

As a transparent and overt collection silo, OSINT can be shared with coalition partners and allies. Intelligence sharing facilitates trust and provides a mutual advantage for the parties involved without revealing clandestine sources (Steele 1995, 458).

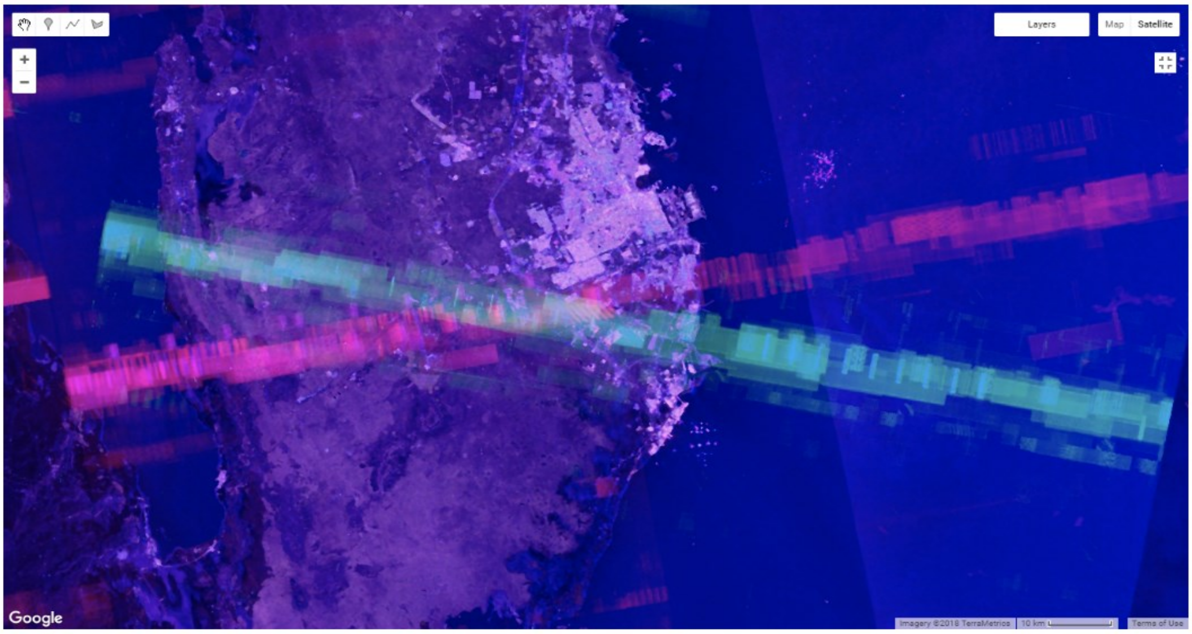
2.1.2. How To Exploit OSINT?

As many authors have argued (e.g. Lowenthal 2001; Mercado 2004; Williams & Blum 2018), OSINT represents the overt equivalent of clandestine collection disciplines.

Exploiting the wide array of tools and methods publicly available on the world wide web requires the analyst to be resourceful and creative.

Imagery Intelligence (IMINT). The case of IMINT is probably one of the best examples of Lowenthal's claim. With the proliferation and growing availability of commercial geographic information systems (GIS) such as Planet Labs, Sentinel Hub and Google Earth, governmental agencies are losing the monopoly on overhead imagery. GIS companies provide mixed quality products at varying price points from high to free. For example, the San Francisco-based Planet Labs operates at least three satellite constellations, enabling the company to provide daily, mostly high-end snapshots of Earth. Since they provide a free-access plan for researchers, Planet Labs tends to be the IMINT-provider of choice for the online OSINT community. Sentinel Hub is another popular GIS provider, which aggregates data from multiple satellite providers in one browser, but lacks the free high-definition service of Planet Labs. Other commercial GIS providers such as Airbus Intelligence or the Israel-based Image Satellite Intelligence (iSi) are also well known IMINT sources in the OSINT realm. However, their less affordable membership plans make them largely inaccessible for the casual researcher.

All private GIS companies allow for customized acquisition (e.g. off-nadir imaging, synthetic aperture radar) and filtered imagery analysis that suits the user's collection needs. These options enable analysts to target their research towards elements of interests such as urban destruction, floods, wildfires etc. These tools are more impactful then they seem. Harel (2018) demonstrates that by using the right configuration, which implies technical know-how, he managed to reveal the locations of the G-band AN/MPQ-53/65 phased array radars used by the MIM-104 Patriot air defence system. As the SAM batteries are always within immediate proximity of their acquisition or engagement radars, Harel (2018) inherently located the U.S. Patriot deployments in the Middle East.



Ascending and Descending orbits converge over Al-Udeid Base in Qatar

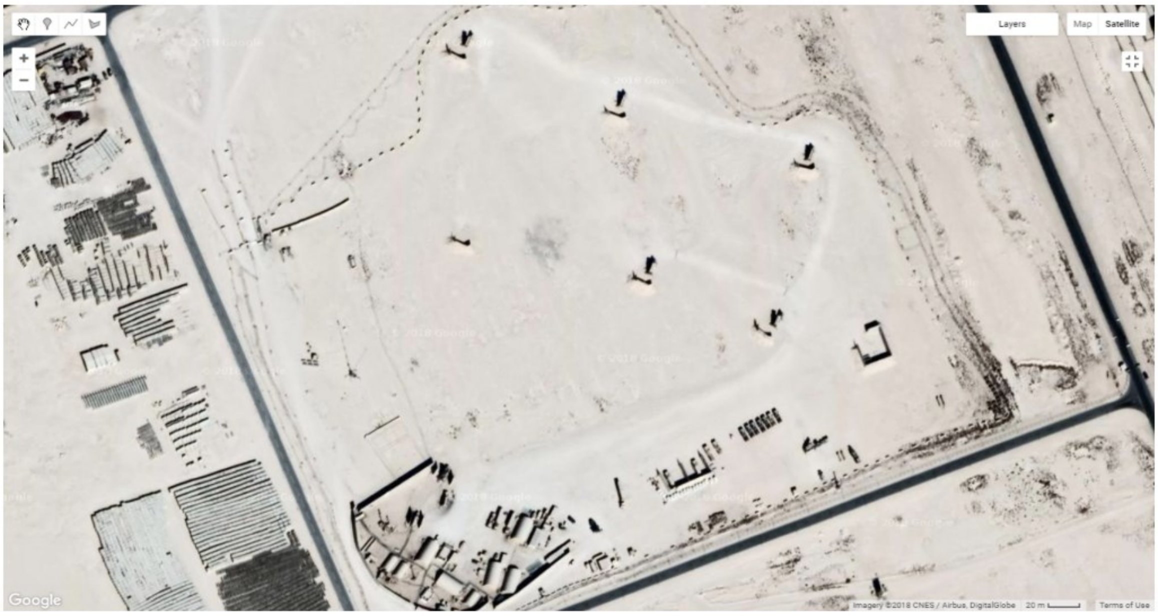


Figure 1 Orbital interference spoils location of Patriot system in Al-Udeid, Qatar (Harel 2018)

While rudimental, Google Earth is a unique IMINT option. Google's 3D-GIS fusion software provides a unique birds-eye-view of the globe. While rare, high-resolution imagery updates sourced by Digital Globe or Landsat satellites allow for before-and-after area comparisons. However, the software's main advantage, compared to the previously listed competitors, is accessibility, rendering it indispensable in any OSINT analysis tool-kit. Google Earth's intruding capabilities stirred up many defence-related controversies in the past decades. In a recent episode, a Google Earth update revealed classified Patriot surface-to-air missile (SAM) systems based around Taipei, the capital of Taiwan (Republic of China). The Taiwanese government prompted

Google to remove the imagery and 3D models of their vital air defence systems (Bacchus 2019). As similar incidents occurred before, governments (e.g. United States, Israel) have regulated the maximum resolution allowed for satellite imagery of selected areas (e.g. military sites, critical infrastructure, governmental buildings) or entire territories. Due to fine patterns and detailed 3D renderings Google Earth is also optimal for the environmental reconnaissance of remote geographical areas (HARM 2019a). From an empirical perspective, combined joint exploitation of low-to-medium resolution, but up-to-date imagery (i.e. Planet Labs, Sentinel Hub) with the high-quality 3D Google Earth data results in comprehensive open-source IMINT or Geospatial Intelligence (GEOINT).

While open-source IMINT options will become increasingly available due to the expanding market, they will remain conditioned on finances, logistically limited, and, in some cases, politically sanctioned so that they cannot top the geospatial and imagery resources of governmental intelligence agencies. In addition, the OSINT community will likely never acquire assets unique to military organizations, which can enable dynamic remote sensing (e.g. long-range unmanned aerial vehicles or other aircraft-types)

Signals Intelligence (SIGINT). While largely associated with communications interceptions and secretive technology, SIGINT also found its way in the OSINT dimension. The most sophisticated tools in the open-source signals domain are arguably the AIS and ADS-B trackers.

The Automatic Information System (AIS) went from being a United Nations International Maritime Organization anti-collision framework in the late 1990s to a maritime domain awareness tool in the present day. In 2002, AIS transmissions, undecrypted and publicly available, became mandatory for vessels above a certain weight, specifically for oil tankers. Currently, all international ships over 300 tons and passenger ships (Weinbaum et al. 2017, 3) are required to emit AIS data. While initially intended for ashore stations, the proliferation of AIS-dedicated satellites not only expanded tracking coverage, but also fused it with remote sensing. Now, there are online applications that show the approximate GPS position of a ship with all of its details directly on a world map. Marine Traffic, Vessel Finder, MyShipTracking and many other websites provide a unique birds-eye-view for OSINT enthusiasts looking for vessels of interests (e.g. military ships, sanction-evading transports). However, as vessels are increasingly engaged in identity manipulation practices, AIS is not fully reliable.

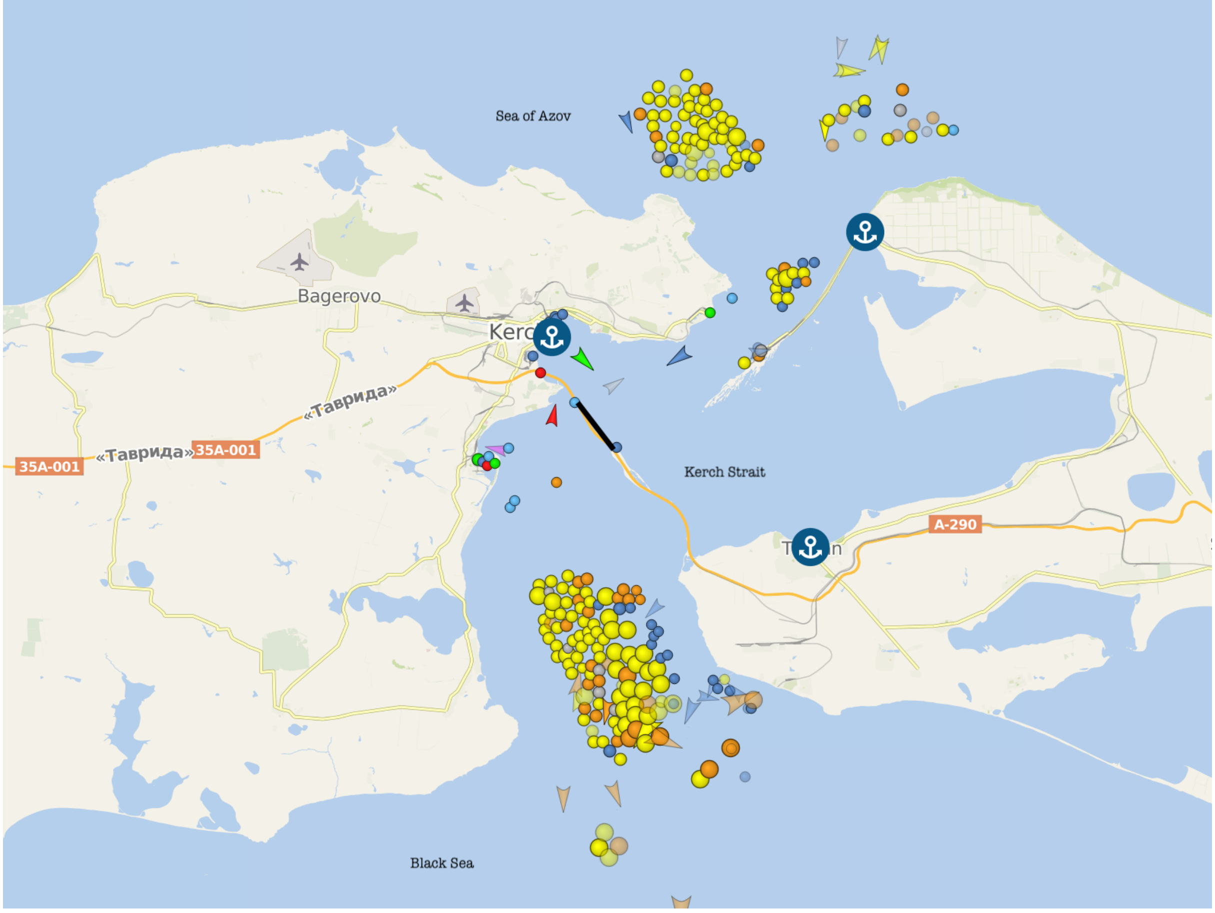


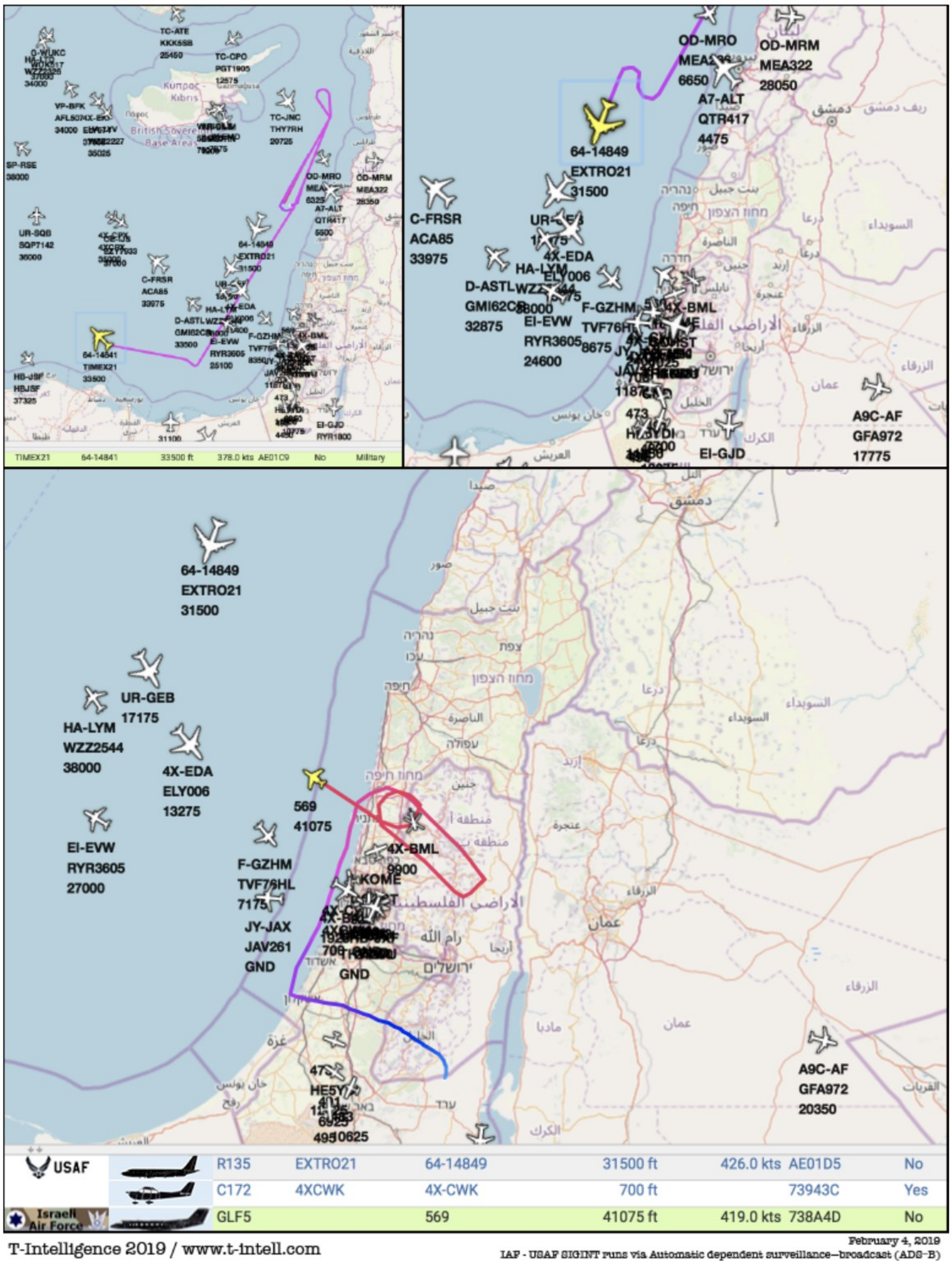
Figure 2 AIS Example: Screenshot from VesselFinder.com during the Russian blockade of the Kerch strait

Since there is no way to validate identification data, many vessels, particularly illegal shipments or military ships, dispatch fake or inaccurate AIS transmissions (e.g. callsign, vessel-type, GPS location). Military vessels may even deactivate their AIS transponders during wartime and go "dark." However, Golaya & Yogeswaran (2019) argue that many of the AIS issues such as GPS-positioning, length of the ship, and next port of call can result from system-design limitation rather than deception (64). Despite these limitations, fusing AIS data with optical and radar imagery can result in the identification or geolocation of "ghost" ships (Weinbaum et al. 2017, 4). Twitter users and Jane's intelligence contributors @CovertShores and @steffanwatkins have demonstrated how AIS limitations can be overcome through technical expertise and multi-source assessments and that AIS provides an overall valuable maritime domain awareness layer for any OSINT analyst.

Automatic dependent surveillance-broadcast (ADS-B) can be viewed as the loose aviation equivalent of the AIS. As an air traffic communication system, ADS-B is used by aircraft “to broadcast their own identity, position, velocity, and additional information such as intents, status or emergency codes” (Strohmeier et al. 2018, 303). ADS-B transmissions use the 1090 MHz radio frequency. What makes ADS-B so valuable for OSINT is that everyone can harvest or exploit the output data, as it is publicly available information. Affordable ADS-B receivers are also widely available and easy to set up. Once functional, the receivers collect output data that users can then chose to share on ADS-B aggregating websites such as ADS-B Exchange, Open Sky Network, FlightAware or FlightRadar 24. While the later only shows commercial and private flights, ADS-B Exchange and Open Sky Network regularly feature military aircraft over conflict zones.

Much like the naval-exclusive AIS, ADS-B has weaknesses that allow operators to manipulate or conceal their output data. While ADS-B data is automatically broadcasted twice per second, it is not uncommon for aircrafts to have undefined information in their flight information – this is a recurring practice among private flights. Furthermore, pilots can deactivate their ADS-B transponders, taking their aircraft position and flight information completely off the grid. While the vast majority of military aircraft operate “incognito,” there are instances when they need to activate their ADS-B transponders. In practice, this only happens when an aircraft intentionally wants to signal its position, either to mitigate collision risk with commercial flights in congested airspaces or as a sign of goodwill to adversarial forces in its proximity.

In addition to spoofing ADS-B transponders, privacy-concerned operators can ask the Blocked Aircraft Registration Request program to hide their aircraft from the public eye. According to Strohmeier et al. (2018) approximately “85 percent of all military aircraft and 61.6 percent of all government aircraft were being filtered on the most popular flight tracking website (FlightRadar24)” (314). However, with patience OSINT analysts can find hidden gems such as U.S. Air Force RQ-4 Global Hawk drone sorties near Crimea (Cenciotti 2018), Israeli SIGINT collection missions off the Syrian coast (HARM 2019b) or a Russian Open Skies Treaty flight over air bases in western Texas (Trevithick 2019). As the aforementioned examples show, Intelligence, Surveillance and Reconnaissance (ISR) sorties are more likely to appear on ADS-B trackers than assets engaged in offensive military operations.



R135	EXTRO21	64-14849	31500 ft	426.0 kts	AE01D5	No
C172	4XCWK	4X-CWK	700 ft		73943C	Yes
GLF5		569	41075 ft	419.0 kts	738A4D	No

T-Intelligence 2019 / www.t-intell.com

February 4, 2019
IAF - USAF SIGINT runs via Automatic dependent surveillance—broadcast (ADS-B)

Figure 3 ADS-B reveals American and Israeli SIGINT platforms airborne (HARM 2019b)

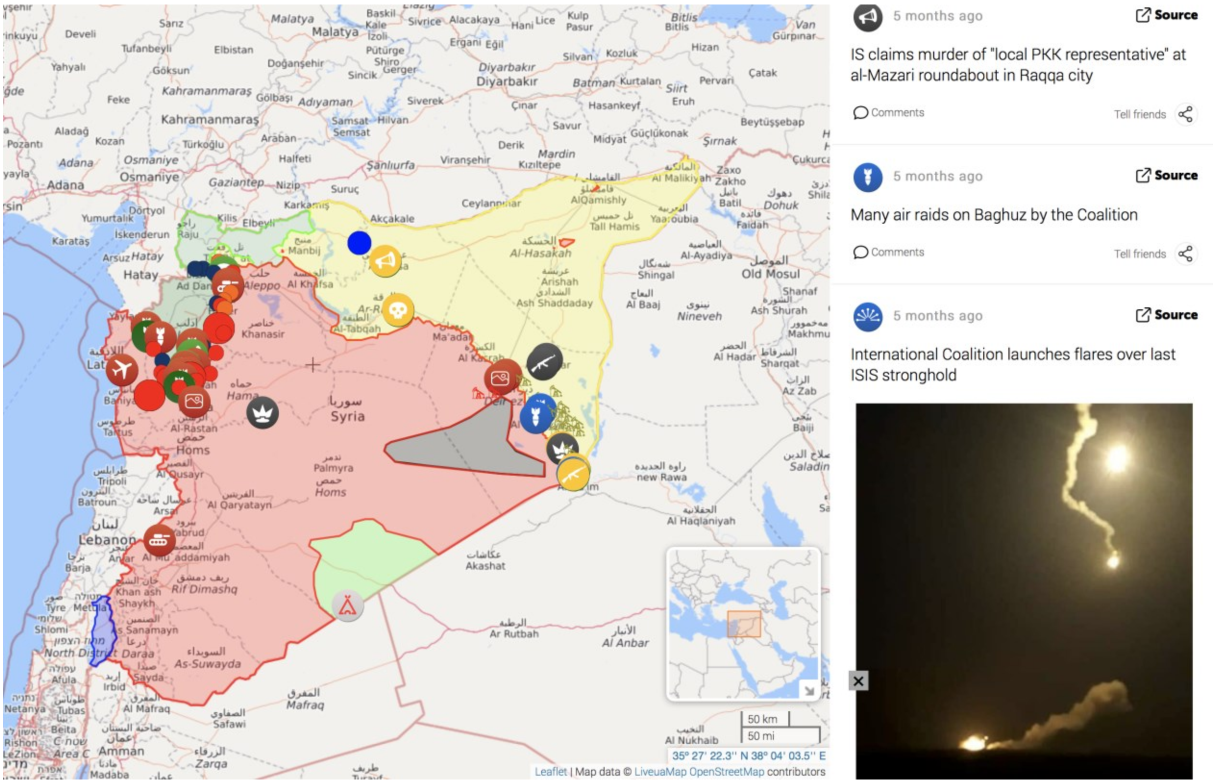
While the AIS and ADS-B protocols mirror the Electronic Intelligence (ELINT) component of SIGINT, the OSINT realm also has a more traditional communications eavesdropping tool to offer. Multiple free-to-use radio receivers exist online, that can provide access to a wide array of frequencies. One such software is the wide-band WebSDR short-wave receiver developed by the University of Twente. While odds of finding military chatter or decrypting conversations are very low, it did happen that OSINT analysts intercepted a coded conversation between a Russian ashore air traffic controller and a bombing crew buzzing the United Kingdom's flight information region (Webb 2015). The incident proved to be real, as the Royal Air Force (RAF) scrambled fighter jets to intercept the approaching bombers. In a similar event, twitter user @MIL_Radar (2019) tweeted a live description of a RAF interception of a Russian bomber pair, using radio-intercepted chatter.

Human Intelligence (HUMINT) and Social Media Intelligence (SOCMINT). The OSINT application of HUMINT largely relates to social media intelligence (SOCMINT). One of the first studies to pioneer the concept, Sir David Omand et al. (2012), consider "intelligence derived from social media" as forming a standalone collection discipline (802). Lombardi et al. (2015) argue that the SOCMINT concept should be fused with the traditional HUMINT to form an integrated collection disciplined styled as Digital HUMINT (6). While there are reasons to support both cases, it is clear that the art of intelligence collection from human sources experienced a remarkable development. In the social media arena, people are willingly transferring the most intimate aspects of their lives to online receivers such as Facebook, Instagram and Twitter. Inherently, nearly all authors engaged in the subject agree that SOCMINT also raised a number of ethical and legitimacy considerations for intelligence exploitation. As social media channels represent a mix of public and private spaces, Bartlett et al.'s (2013) classification system identified four SOCMINT categories, of which only one is truly open-source. The other three, directed surveillance SOCMINT, covert human intelligence sources SOCMINT and intercept/intrusive covert surveillance SOCMINT, rely on deception and clandestine exploitation of social media subjects (Bertlett et al. 2013, 9-11) and therefore do not qualify as overt sources.

Besides providing insights into groups and near real time situational awareness, Sir David Omand et al. (2012) name crowd-sourced information as one of SOCMINT's most prized capabilities – "with access to social media, passive bystanders can become active citizen journalists, providing and relaying information from the ground"

(804). Crowdsourcing as a term was allegedly coined by Howe (2006), who described it as a the “productive potential of millions of plugged-in enthusiasts.” Per Estelles-Arolas & Guevara’s (2012) definition, crowdsourcing is “a participative online activity in which groups of individuals engage in directed work requiring an aggregate of many individuals to complete, for which they receive some personal satisfaction” (9-10). For intelligence application, Stottlemyer (2015) designates HUMINT and OSINT as part of the crowdsourcing environment since it relies “entirely on human activity” (584).

Out of Brabham’s (2013) crowdsourcing typologies, the Knowledge and Discovery Management (KDM) variant is the most widely featured online. KDM refers to situations in which the crowd is tasked by an organization to collect and aggregate information into a shared location (Brabham 2013, 45). Arguably, one of the most preeminent KDM-type of crowdsourcing platforms is the Live Universal Awareness Map (LiveuaMap). Freely accessible online and available for smartphones, the LiveuaMap is a crowdsourcing-based map that aggregates news, media and rumors about different conflict zones around the globe (Hassan & Hijazi 2018, 290). The platform draws most of its information from user tweets. Twitter is almost always the best social media platform for OSINT investigation, as it sometimes proved to be faster than conventional media outlets in reporting a significant event (Sir David Omand et al. 2012, 807). Besides situational awareness, the application provides approximate geo-locations of the aggregated data on a given conflict map. The LiveuaMap’s growing popularity also attracted the attention of defence senior heads. In a journal article, U.S. Air Force Major Atkins (2018) noted that the “openly available LiveuaMap’s coverage of conflicts in Syria and Crimea produced information that often-rivalled classified sources and methods” (36).



5 months ago

Source

IS claims murder of "local PKK representative" at al-Mazari roundabout in Raqqa city

Comments

Tell friends

5 months ago

Source

Many air raids on Baghuz by the Coalition

Comments

Tell friends

5 months ago

Source

International Coalition launches flares over last ISIS stronghold

Figure 4 Screenshot of the Syria crowdsourcing page of the Universal Awareness Map (liveuamap.com)

2.1.3 At OSINT’s Edge: Challenges, Limitations and Ethics

Beyond the glamorous tools and platforms facilitating open-source exploitation, it should not be forgotten that OSINT is a double-edge sword. There are reasons why governmental intelligence agencies are not only conducting arm-chair research of open-sources. The challenges, limitations and ethical considerations of OSINT, likely well known by intelligence professionals, should also be comprehended by every casual independent analyst.

Independent OSINT runners should particularly note that they are attempting to replicate the work of entire governmental agency departments. While it is simply impossible for a “one-man-army” to constantly compete or keep up with conventional intelligence organizations, teams of OSINT analysts (e.g. Belingcat, Black Cube, CITEAM, T-Intelligence) could offset this disadvantage. Moreover, OSINT is not universally accessible. Per Gruters & Gruters (2018), most OSINT analysts are computer-savvy technology-oriented users with intuition (101). This implies that OSINT analysts should be proficient in surfing the world wide web and hold advanced computer skills. Furthermore, the vast amount of open-source data available is overwhelming analysts (Hulnick 2002, 566). The plethora of OSINF with potential actionable intelligence value can raise collection and storage issues. While there are many storage and sorting options available both offline and online, independent OSINT analysts need to show good self-management.

OSINT analysts require cognitive preparedness to mitigate bias, think structurally and solve complex puzzles. These challenges can be relatively offset by the growing public availability of intelligence analysis literature, penned by professionals and scholars. The CIA's Center for Study of Intelligence has plenty to offer, from intelligence writing guidelines to unclassified reports. Canonic literature (e.g. Sherman Kent, Jack Davis, Robert Jervis) should also be periodically consulted. For example, Heuer's (1999) *Psychology of Intelligence Analysis* offers practical and reflective insights on how the analytical process can be improved, namely by "defining the problem, generating hypotheses, collecting information, evaluating hypotheses, selecting the most likely hypothesis, and the ongoing monitoring of new information" (173). In addition, there are numerous peer-reviewed and specialized publishing groups that have amassed an impressive volume of intelligence literature. Within the Taylor & Francis Group, the *Journal of National Security and Intelligence* is particularly useful and insightful, encompassing authors with academic and professional backgrounds.

Beyond collecting, analysing and storing, OSINT is difficult to validate. Since anyone can post anything online, the Internet has become a disinformation-rich, contested spectrum. As the battlefield moved online, our information environment has seen an unprecedented proliferation in subversive operations aimed at media manipulation, disinformation and deception. In light of this, a clear methodological process is required to conduct OSINT analysis (Lowenthal 2014, 3). The open-source investigation group Bellingcat has an impressive collection of tutorials regarding geolocation, reverse image search and cross-referencing techniques. However, intelligence validation is not always possible just through OSINT.

Furthermore, "language ability is critical in intelligence" (Hulnick 2002, 572). Since most OSINF available on the world wide web is in English, a primordial requirement for any self-aspiring OSINT analyst is to know the language. This is however only the beginning, as OSINT acquisition in various other conflicts will be limited, if the analyst does not command local languages or understand the respective cultural context. For example, the case studies in this thesis have deliberately avoided issues relating to the Syrian opposition groups, since the author does not speak Arabic, severely limiting the research. This OSINT limitation is less severe in the public sector as intelligence organizations recruit linguistic experts suited to their needs (e.g. Arabic, Farsi, Mandarin, Kurdish, Russian, Pashto, Ukrainian). In its defence, the community of independent OSINT analysts could argue that self-perfecting online tools, such as Google Translate, are increasingly removing the language barrier between collectors and sources.

While it is generally considered as being the most ethical and legal form of intelligence collection, OSINT is not as innocent as it seems (Hribar et al. 2014, 534). Not all information found online is legally or ethically free for exploitation. This refers to leaked or accidently declassified information (e.g. Wikileaks) or data that was intended for private use (e.g. private social media accounts, closed networks). According to Dedijer's (2005) classification method, there is white information (publicly available), black information (classified information) and grey information (124-129). While a grey area is by definition blurry and difficult to define, OSINT analysts should factor this into their ethical considerations.

However, the issue of ethical OSINT exploitation is far bigger than just the collection stage. Independent OSINT analysts should consider the morality of publishing their findings. While many open-source assessments available online are harmless to state secrets, there are cases when "intelligence minutemen" compromised operations security. In a 2016 anti-terror raid in Brussels, the Belgian police had to urge the public to stop crowdsourcing their movements on Twitter, since the terrorist suspects could use that information to escape (Tangen 2016). Likewise, but hypothetical, documenting and publishing the movements of an U.S. strike carrier group (SCG) via AIS trackers and commercial geospatial imagery could help adversaries such as Russia and China. However, these are just the effects of a deeper social question – why do independent individuals engage in OSINT? Indeed, a small segment of lone wolves exist, who act as force multipliers for nations and organizations. However, many aspiring OSINT analysts are just after some "good sport". Servicemen should take note of this hazard and mitigate the risks of having classified or "grey zone" information exploited by data-miners. For government agencies, maintaining operations security (OPSEC) in the age of OSINT is harder than ever. OPSEC as defined by the US Department of Defense (2019) is "the process by which we protect unclassified information that can be used against us."

The bottom line is that in the information age, the proliferation of open-sources and increase in software availability has catapulted OSINT on the forefront of intelligence in study and practice. This section has demonstrated the vast potential and hazards of OSINT tools, but also drew attention to OSINT's limitation. As a double-edge sword, OSINT can either be a friend (force multiplier) or foe (OPSEC hazard). While the OSINT phenomenon can be expected to grow and further proliferate, it is unlikely that it will ever replace the clandestine collection disciplines. Likewise, arm-chair researchers are unlikely to surpass the preparedness of professional servicemen, as intelligence collection is much more than just googling the right words. The "exotic" online tools will not be of any help if the self-styled OSINT analysts do not master their subject matter.

An analyst, like a hunter, needs to know what he is looking for.

2.2. Military Logistics

"An army without its baggage-train is lost; without provisions it is lost; without bases of supply it is lost" (Sun Tzu 2016, 38). Despite being an ancient practice and playing a central role in all military affairs, the issue of logistics has been overwhelmingly neglected from academic debates. The term itself, now widely used, has barely seen an etymological evolution from the Greek word "logistikos", used to describe someone "skilled in calculations." Without his "logistikoi," Alexander the Great would not have been able to sustain his eight year long campaign from Macedonia to the Hyphasis river on the Indian subcontinent. With better logistical support, the Wehrmacht might have survived the 1942 winter on Soviet territory.

The topic of military logistics will be explored from head to tail. The following section will review and categorize the literature available on the topic and discuss the existing definitions from diverse sources (e.g. academic, governmental). Moreover, this section will outline why logistics are central to military forces and, furthermore, why it plays a large role in OSINT analysis.

2.2.1. What Are Military Logistics?

While sparse, the literature on military logistics can be summarized in three categories. The first, refers to authors that cover major military battles from a logistical perspective (see for example Van Creveld 1980; Van Creveld 1991; Van Creveld 2000; Roth 1998; Engels 1978), the second encompasses governmental publications on logistical doctrines and field manuals, and the third refers to theoretical, largely academic publications that focus on defining logistics and its role in military affairs. The scholarly debate surrounding military logistics can be traced back to the Prussian general-turned-strategic-thinker Claus Von Clausewitz and to Napoleon's General Antoine Henri Jomini. Throughout time, two schools of thought have developed around them.

Jomini viewed logistical operations as enablers of tactical and strategic applications, being a basic and vital military skill (Rogers 1995, 13-14). In the words of Jomini (1971), "strategy decides where to act; logistics bring the troops to this point; grand tactics decides the manner of execution and the employment of the troops" (69). In contrast, the Prussian perspective did not perceive logistics as equal to tactics and strategies (Jomini 1971, 33-45). However, Clausewitz (1976) overall agreed that there was nothing more important than the sufficient supply of the armed units (14). Strategic culture and historical experiences could be the reason why Clausewitz did not see logistics as equal or interlinked to tactics and strategies. The Prussian Army experienced only European battles, which required significantly shorter supply lines than the French overseas expeditions in the Atlantic and Africa.

Apart from the Clausewitz-Jomini debate, the question of military logistics has been largely neglected in the field of Strategic Studies. As Erbel & Kinsey (2015) rightly point out, the supply of military operations is virtually absent from scholarly debates, despite playing a central role in “every aspect of military operations, including and particularly for strategy” (519). The sparse literature available on military logistics is a confirmation of this fact (Prebilic 2006, 159). Why the lack of literature? The U.S. Army (1993) claims that scholars simply do not take interest in logistics, as it is a less exciting aspect of military affairs (5). Another reason might be that logistics is a technical, mostly application-oriented aspect that is monopolized by perspectives anchored in management studies.

The literature available focuses mainly on defining military logistics. This mostly refers to the third category of literature (academic) identified on the subject matter. While it is a tricky concept to narrow down, the majority of academic authors provide very broad definitions. For example, Prebilic (2006) defines military logistics as “a group of different activities that systematically, wholly and continually support the needs of the defence–military system” (166). As a semantical joker card, the author makes use of the terms “different activities” and “defence-military system” to provide an unrestricted meaning to military logistics. This trend is continued and furthermore expanded by other authors. Some works claim that “logistics is not only about the supply of materiel to an army” but also include national infrastructure, national transportation and the nation’s manufacturing base (WhitehAll 2000, 1). Similarly phrased, but directed towards lines of efforts, Uttley & Kinsey (2012) claim that the concept of military logistics is best described by “what military force can be delivered to an operational theatre, the time it will take to deliver that force, the scale of forces that can be supported once there, and the tempo of operations” (401).

However, one definition stands out in most academic texts. Leveraging his defence-oriented scholarship, Moshe Kress (2002) strikes a balance between theory and practice. In his view, military logistics refer to the resources the military requires for an operation to achieve its objectives, including “planning, managing, treating and controlling these resources” (Kress 2002, 7). By directly linking logistics to the operational art and strategy, he discreetly sides his work with the French argument of the historical Clausewitz-Jomini debate. Furthermore, his definition comes the closest to how the defence sector views military logistics.

As a fundamental common denominator, defence organizations reject the assumption suggested by Clausewitz – the separation of logistics from tactics and strategy. Since the late 19th century, European armies and later the U.S. Army considered logistics as inseparable from the overall operational art (Leighton & Coakley 1995, 9). Practical and purpose-oriented by nature, the military definitions of logistics are more narrow and detailed than their academic counterparts. NATO's (2018) *Allied Joint Doctrine for Logistics* defines logistics as "the science of planning and carrying out the movement and maintenance of forces." It encompasses all military affairs related to acquisition, storage, development, distribution, maintenance, evacuation, disposition of material; transport of personnel etc. (1). The NATO definition is overall reflected across all defence bodies of the 29-member states. Augmenting the consensus, the U.S. Joint Chiefs of Staff (2019) add that the provision of logistics and personnel services are not only imperative to maintaining operations, but also enablers of the military's seven doctrinal joint functions (command & control, information, intelligence, fires, movement and manoeuvre, protection and sustainment) (1).

2.2.2. Logistical Support Operations (LSO)

It is no coincidence that the U.S. defence sector pays most attention to logisticians and the value of their work. Throughout history, the role of military logistics has been consistently present in the American strategic mindset. General Eisenhower famously said, "you will not find it difficult to prove that battles, campaigns, and even wars have been won and lost primary because of logistics" (quoted in Scott et al. 2000, 115). Eisenhower's words echo the aforementioned NATO and U.S. Joint Chiefs of Staff definitions, which anti-climatically frame logistics as a paradoxical entity. On one hand logistics enable military operations and on the other hand they determine what is possible to achieve.

Logistical Support Operations (LSO) is one of the many terms used by the American defence community to describe military logistics. As identified by Lt. (ret.) Henderson (2008), there are four types of LSOs: manoeuvre, sustainment, management and administrative (15-19). The first two, manoeuvre and sustainment operations, are mainly employed in support of offensive and defensive combat postures. Sustainment operations begin, when a combatant defensive posture ends. As the battlefield shifts from offensive-defensive operations to stability and support, LSOs also transition to management and administrative operations (Henderson 2008, 19). LSO refer to a rhythmic change concerning supply tempo and resource requirement. While in the active engagement phases (offensive or defensive operations) combat elements require lengthy and uninterrupted LSO, in management and administrative operations, LSO is imperative to drawdown troops and last only for a short period of time. Otherwise, LSOs could hamper capacity building efforts by making the local community overdependent on external support (Henderson 2008, 17). An example of an overextended management and administrative LSO can be found in Afghanistan, where after more than two decades of NATO training, assist, and advice, local forces are still unable to assume full security duties.

Much like intelligence and warfare, LSOs or military logistics are separated in tactical, operational and strategic levels. Strategic logistics refer to the process of building and maintaining the national defence infrastructure, including the technological, industrial, inventorial, storage and transportation sectors. The aforementioned strategic logistical sectors represent the source of an army’s capabilities and overall means of existence. Within the process of strategic LSOs, the national support base (e.g. people, resources and industries) is fused with the military’s war effort (U.S. Army 1999, 12-1). Operational logistics consist of all activities and resources needed to enable campaigns and major operations as part of an armed conflict. The strategic and tactical levels are bridged by operational logistics (Wright & Reese 2008, 494). This logistical sector focuses on in-theatre infrastructure development (housing, health services, force reception) and capability management (personnel, resources, materiel) (U.S. Army 1999, 12-3). Last but not least, tactical logistics encompass all LSO assets and activities required to sustain the soldiers and their weapons systems during operations (Wright & Reese 2008, 494). Tactical logistics inherently refers to frontline supply efforts and is strongly linked to a soldier's quality of life (US Army 1999, 12-3).

As Kress (2002) points out, LSOs can be summarized in three basic options: obtain (source resources from the area of operations), carry (combat elements transport the resources themselves) and send (enabled by the industrial revolution, troops could now be supplied and re-supplied from rear staging areas or from the homeland directly to the frontline) (10-12). Reminiscent of ancient and pre-medieval times, obtain-type of LSOs are credited for fuelling most of Alexander the Great's transcontinental campaign to India (Engels 1978, 1). Obtain-type LSOs are largely vulnerable to scorched earth tactics, as German forces famously discovered in the 1941-42 campaigns on Soviet soil (Kress 2002, 11). Carry-type LSOs were particularly used by heavy infantry - Byzantine and Roman cavalrymen were known to have carried their own food ration in their saddlebags (Roth 1999, 78). To a certain extent, soldiers are still carrying provisions with them, but most armed forces do not dependent on their units to physically carry logistics from staging points to the frontline. Since the 19th century, send-type operations dominated the logistical doctrines and preferences of armed forces. Nowadays, heavy-lift cargo aircraft, trucks caravans and large vessel-containers are on the forefront of military supply.

In a send-type LSO option, transportation assets move through what the military calls "lines of communications" (LOCs). LOCs refer to all corridors (land, sea and air) that link a deployed combat force to a base of operations, through which personnel and cargo move in and evacuated soldiers move out (U.S. Army 1999, 12-9). Within this process, LOCs link source (homeland facilities), intermediate (in-theatre facilities) and destination (frontline tactical units) nodes, forming a logistics network (Kress 2002, 29).

While vital for all armies, securing and maintaining LOCs is especially seen as a matter of life and death in the American strategic culture. It was General Douglas MacArthur who famously said that "the history of war proves that nine out of ten times an army has been destroyed because its supply lines have been cut off." It is not only ingenuity that catapulted the role of LSOs on the forefront of American defence planning, but also the magnitude of the U.S. overseas military engagements.

American forces sustain a semi-permanent rotational presence in 500 locations throughout more than 30 countries (Department of Defense 2018b, 18, 50). Those deployments range from radar maintenance units, medical servicemen, airfield-support units, trainers and advisers to combat personnel engaged in contingency or covert operations. In 2018 alone, the U.S. Department of Defense had a $639 billion budget. Much of these funds are constantly allocated to procurement, maintenance and logistical operations.

In contrast, European armed forces are significantly less capable of deploying substantial troop numbers to other countries. As an infamous RAND report found, the United Kingdom, France and Germany could each marshal a battalion sized formation (500 to 800 soldiers) to the Baltic states in a matter of weeks to months (Shurkin 2017, 1). Besides being insufficient and arriving too late to counter a hypothetical Russian offensive, the combined British-French-German force will require American support – particularly airlift capability – for LSO sustainment of operations in the long-run (Shurkin 2017, 9-10).

Part of the reason why American LSOs are able to keep up with the multitude of worldwide military engagements is partner capacity. LSOs, particularly in crisis response and limited contingency operations, “involve a combination of military forces, the private sector, and capabilities in close cooperation with other U.S. Government departments and agencies, international organizations, and NGOs” (U.S. Joint Chiefs of Staff 2019, V2). Interagency cooperation and public-private associations are now more or less common practice across all armed forces, particularly when it comes to the sealift and airlift of low-value cargo such as consumer goods. While a force multiplier when it comes to distribution, private-public associations in military logistics can also lead to security breaches. Erbel & Kinsey (2018) argue that by introducing an additional layer (private sector) into the supply chain, the military is extending operations security (OPSEC) requirements to less controllable third parties (526). This can prove particularly concerning when private-operators are tasked with the bulwark of overseas send-type of LSOs.

2.2.3. Spoilers of War: Using LSO for OSINT

Overall, LSOs (particularly send-type) are vulnerable to OSINT acquisition. While not easily observable, the synergy of military logistics know-how with OSINT tools forms a recipe for OPSEC cracks. By understanding LSO procedures and doctrines, OSINT analysts can gain valuable insight into the operational design and preparations of military action, sharpening their target-acquisition process. With this LSO knowledge, ship-spotting (AIS transmissions) and air monitoring (ADS-B trackers) applications become infinitely more revealing. As an OSINT collector becomes acquainted with military hardware, lines of communications (LOCs), logistics nodes, and means of transportation, he or she learns where to look, what to look for and furthermore what it means when a certain asset is spotted. By following the breadcrumbs left behind by military logistical operations, OSINT collectors can discover covert overseas facilities, forecast an impeding air strike, or observe a military situation as it unveils.

Decision-makers should consider the OPSEC vulnerabilities of their LSO practices as well as defence intelligence availability and take measures to mitigate the risk of OSINT exposure. Aside from individual observations of military officers (see for example Atkins 2019, 35-36), the U.S. has yet to develop a defence logistical doctrine, which outlines the LSO-OSINT risk and recommends best practices to maintain OPSEC. From an empirical perspective, it is exceedingly important to recognize that logistical preparations almost always have the potential of spoiling military movements.

A simple demonstration of LSO vulnerability via open-sources was done by HARM (2018a) in a *T-Intelligence* investigation. The online OSINT-platform has repeatedly observed a Djibouti outbound turboprop commuter airliner flying with incomplete ADS-B data that always “disappeared” over Southern Yemen, after descending for landing. A simple investigation on the aircraft type, possible inbound and outbound locations provided valuable information. The investigators learned from a quick Google search that the U.S. military operates a near identical version of the Dornier 328, called the C-146 Wolfhound, modified to enable cargo and missions. As the D328 was suspected to actually be a C-146 Wolfhound active with spoofed ADS-B data, the investigators looked for logistics nodes. The flight crew always switched off their transponder upon approaching the same area in Southern Yemen. The nearest airfield in that region is the Ryan Airport near Mukalla city. Background research shows that the area was liberated from al-Qa'ida control by a coalition of local militiamen and the United Arab Emirates (UAE) military with direct support (e.g. special operators, air and artillery support) from the United States. Besides containing Iran, Washington's main stake in Yemen is to track and kill senior leaders of the al-Qa'ida in the Arabian Peninsula (AQAP) terrorist group.

With direct American involvement in the Southern Yemen area of operations (AO) one might suspect that ground forces have also been deployed in Mukalla, requiring constant re-supply. By applying the aforementioned logistics network model, the author assessed that Ryan Airport in Mukalla serves as a destination node, while Djibouti (likely the U.S. Naval Expeditionary Base "Camp Lemonier") represents the intermediate node for LSOs. The two nodes form a Line of Communication (LOC) for distributing tactical logistics to deployed personnel, enabling raids against AQAP in Yemen. The logistics network is traversed by the Dornier-328-impersonating C-146 Wolfhound, the sole asset identified as using the airborne LOC.

The sustained U.S. combat posture in Yemen is furthermore supported by a Transportation Command (TRANSCOM) commercial listing (GovTribe 2018). As a publicly visible contract, the USTRANSCOM is in search for private operators for airborne casualty evacuation (CASEVAC) and medical evacuation (MEDEVAC) sorties in Yemen and the Horn of Africa AO. The listing mentions that the U.S. special operations elements will be the main beneficiary of these services.

Furthermore, the OSINT investigators then proceeded to recon Ryan Airport using openly available GEOINT/ IMINT tools, revealing special operations related assets, such as unmanned aerial vehicles and attack or transport helicopters sitting on the airport's tarmac - some of them exclusively used by the U.S. military (i.e. MH-6 Little Bird). Leaving aside the remote sensing effort, this example demonstrates how easily OSINT users can spoil sensitive military operations by tracking their logistical footprint. This example was particularly comprehensive as it intercepted LSOs in planning (i.e. USTRANSCOM listing) and execution (i.e. D328 flight).

Jane's Intelligence Review contributor Sean O'Connor (2010a) provides another example, which highlights the importance of background knowledge on military assets for OSINT. Using only Google Earth, the author identified 41 active surface-to-air missile systems and 24 early warning and surveillance radars that make up Iran's integrated air defence network. Drawing on O'Connor's (2010a) work, Amir (2017) of the *Iran GeoMil* blog updated the open-source record on the Iranian air defences and observed that seven SAM sites were cleared since 2010. In 2018, HARM (2018b) also updated the inventory with a more comprehensive research that included high-resolution IMINT analysis of strategically important SAM deployments such as the long-range S-300PMU2 near the Persian Gulf and the tactical MIM-23 SAM guarding one of Iran's uranium enrichment and nuclear reactor plants. All IMINT/GEOINT assessments discussed contain Google Earth-based maps showcasing the location of Iran's SAMs and their estimated engagement range "bubbles." While the OSINT work is not deception-proof (e.g. cannot always distinguish dummy sites from active ones), it still provides a valuable baseline log of the country's air defence capabilities. These details are critical for potential aggressor states, when plotting kinetic strike options against Iran's military, regime, or nuclear facilities.

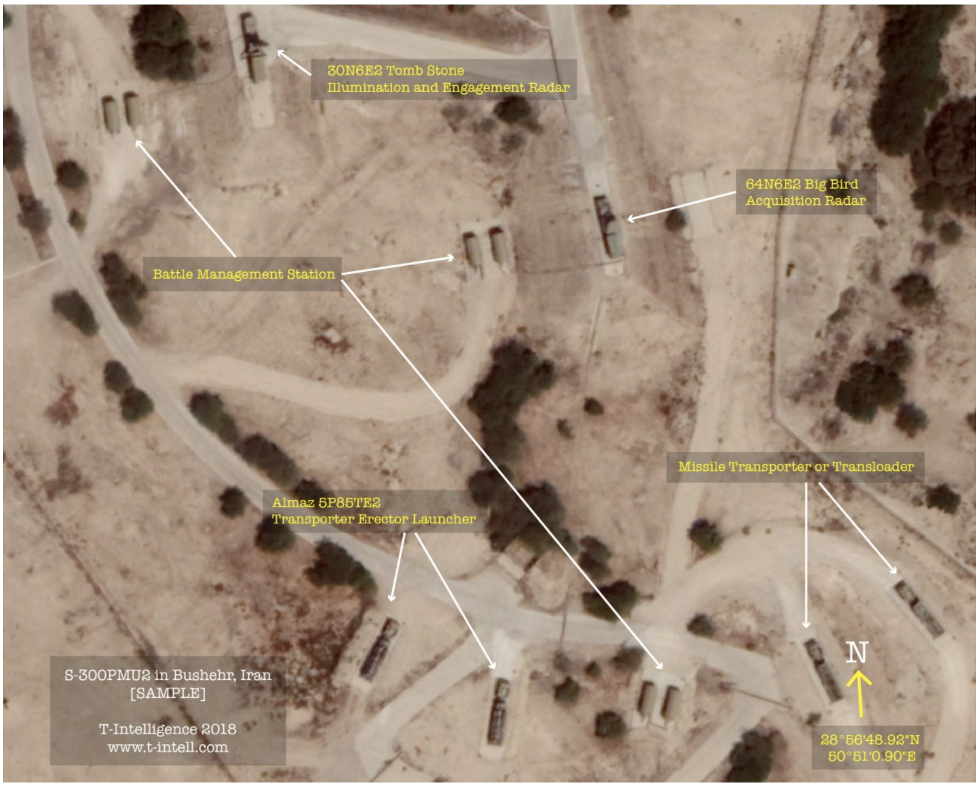

30N6E2 Tomb Stone
Illumination and Engagement Radar
64N6E2 Big Bird
Acquisition Radar
Battle Management Station
Missile Transporter or Transloader
Almaz 5P85TE2
Transporter Erector Launcher
S-300PMU2 in Bushehr, Iran
[SAMPLE]
T-Intelligence 2018
www.t-intell.com
N
28°56'48.92"N
50°51'0.90"E

Figure 5 Iranian S-300PMU2 position (HARM 2018b)

In comparison with the previous example, in which OSINT users uncovered a tactical-level operation in Yemen, using LSOs, this example reveals strategic intelligence related to Iranian national security. This begs the question of how the intelligence minutemen uncovered such secrets? As argued throughout this study, OSINT analysis is far more than just handling exotic online tools and googling the right key words. OSINT, as an intelligence practice, also requires background knowledge, intuition and puzzle-solving capacity. In this case, the OSINT analysts either possessed or obtained the technical knowledge needed to search and correctly identify the equipment related to SAM systems and air defences. However, the literature requires to conduct asset recognition remains very sparse or inexistent. The CIA has unclassified a large volume of intelligence on Soviet military capabilities, including on SAM site design and imagery interpretation (see for example CIA 1965). Customer manuals and advertising brochures released online by defence companies also provide information on weapons systems that can help in imagery interpretation process (see for example Raytheon, Lockheed Martin, Almaz-Antey etc.). Defence analysis and military website are another source of specialized insights (see for example Deagle.com, Australia Air Power, Army Recognition, Jane's Intelligence Review). The *IMINT & Analysis* blog deserves special recognition, as it compiled a vast media database of SAM site layouts, grouped by type and country (see for example O'Connor 2007a; 2007b; 2010b). Three-dimensional (3D) modelling websites (e.g. Sketchfab.com) are an unorthodox, but very resourceful way for amateurs and semi-professionals to familiarize themselves with the design of a weapons system and to visualize it from different angles (see for example CSIS 2017).

In conclusion, OSINT analysis is as much about methodologies, techniques and "geeky" tools as it is about background knowledge, know-how and analytical skills. After outlining the theory and practice of military logistics, infused with some examples of OSINT applications, we can assess that it is imperative for analysts to familiarize themselves with their collection subject. Likewise, it is necessary for the military to consider these loopholes and vulnerabilities, explicitly on send-type LSOs, and improve OPSEC procedures.

3. Case Study: The OSINT-LSO Nexus in Syria

Based on the theoretical discussion above, the following section provides an in-depth case study of how OSINT analysts are tracking military logistics. The case chosen is the Syrian Civil War, as this is the most suitable example of how open-sources have tracked an ongoing conflict with unrivalled precision. First and foremost, the multifaced Syrian conflict has received unprecedented coverage, which went beyond the so-called “CNN effect.” As Doucet (2018) argues “Syria’s war is arguably the first social media war” (142). For most part of the conflict, mainstream journalists were kept off the frontline, catapulting social media users on the forefront of war reporting. There is no more suitable battlefield than Syria to demonstrate the power of OSINT in a military application.

Furthermore, the Syrian conflict consists of an overlap between a civil war with transnational ramifications and a great power geopolitical confrontation with subsequent proxy warfare. The plethora of state and non-state actors, the varying degrees of military interventions, and the inherent overcrowded battlefield have provided this research with a unique opportunity not only to demonstrate the efficiency of OSINT, but also its multipurpose characteristics. The aforementioned OSINT-LSO nexus is highly practical for observing developments in all traditional battlespaces (sea, air, land) and applicable to all fronts of the Syrian theatre of operations (south, west, east, north).

Capitalizing on the multifaced dynamics and diverse engagements, the following case study is divided into three focal points. Each of the three focal points is based on different episodes within the conflict, demonstrating that the OSINT-LSO nexus can produce varying types of intelligence analytical products. The first focal point is an estimate of the enemy capabilities and refers to collecting and analysing all known factors that affect the enemy’s objective: “time, space, whether, terrain, strength and disposition of enemy forces” (Datz 2008, 538). This intelligence product is described in a CIA publication as being the most significant part of a military intelligence officer’s work (Smith 1994). Based on the Russian military intervention in the Syrian Civil War, this focal point demonstrates how OSINT users have assessed the

Russian military's order of battle in Syria, with emphasis on its fighter aircraft and aerial defence battery deployments.

The second focal point is forecasting. As an integral part of intelligence analysis, forecasts have the role of reducing uncertainty for decision makers by providing knowledge about the future (Mandel & Barnes 2014, 1). This section follows the trilateral American-British-French limited strike on the Syrian Arab Republic's chemical weapons' sites in April 2018, showcasing how OSINT tools have enabled amateur analysts to estimate the assets mobilized for the operation and to correctly predict the timeframe of action.

The third and final part is centred on battle damage assessments (BDAs). As defined by the U.S. Department of Defense (2018), a BDA is "the estimate of damage resulting from the application of lethal or nonlethal military force" (12). BDAs are crucial for decision makers, planners, and implementing entities. A BDA's conclusion decides whether the mission objectives were achieved or whether the mission failed (Sopko 1999, 12). This section will show how OSINT analysts were able to conduct their own, purely open-source BDAs of Israel's air strikes on Iranian-affiliated targets in Syria, but also how they "reversed-engineered" the operational design to guess which aircraft was scrambled, which bombs were dropped, which flying path was used and which target was bombed. In addition, this discussion will show how OSINT observers were able to follow the secret confrontation between Israel and Iran in Syria. While all of the aforementioned focal points represent different episodes and theatre of operations of the same conflict, this separation is important to accurately disseminate the multifaced and complex war and subsequent OSINT reporting.

3.1. The Syrian Civil War

After decades of sectarian instability during the French Mandate and power struggle in the post-independence era, Syrian Air Force general Hafeez al-Assad ended the wave of successive military coups with his own. Following the 1971 coup, the Syrian Arab Republic was built around the Assad dynasty, which drew strong support from its community, the coastline-based Allawis (a distant branch of Shi'a Islam). Currently estimated at 12 percent of the Syrian population, the Allawis dominate the republic's government and senior military positions at the expense of the 64 percent Sunni Muslims (Phillips 2015, 337). Syria's internal sectarian tensions increased, culminating in the 1982 Hama massacre, when the Syrian security forces crushed a seven-year long Sunni Muslim uprising. Furthermore, Syria fought several conflicts with Israel, intervened in the Lebanese Civil War, and sponsored the Kurdish Workers Party (PKK), a Turkey-based separatist Marxist terror group in its guerrilla struggle against the Turkish state. In this process, Syria became one of the Soviet Union's strongest allies in the Middle East.

In 1999, Bashar, Hafez's youngest son, succeeded his father to the throne. While a self-styled reformist, Bashar al-Assad did little to reverse the nation's sectarian discord and brought only cosmetic changes to Syria's foreign and security policy. By sectarian discord or sectarianism, we refer to a state of discrimination, hatred or tension between ethno-religious sects (Haddad 2011, 31).

The Spark

In early 2011, large-scale peaceful protests emerged in Da'ara, one of Syria's largest and more cosmopolitan cities. While mobilized around freedom and liberation in the context of the Arab Spring movements throughout North Africa and the Middle East, the Syrian demonstrators also protested against the arrest and torture of a group of teenagers who were caught spraying dissident graffities. Instead of promising reforms, Damascus violently and indiscriminately suppressed the crowds. Known as the "Spark of the Revolution," the regime's wave of escalatory violence produced dozens of popular self-protection militias throughout the country. United under the Free Syrian Army (FSA) banner and led by defector General Riad al-Assad, Syria headed towards an all-out civil war. Based on Turkish soil and strongly supported by Western and Gulf State countries, the FSA caused massive defections in the Syrian Arab Armed Forces. This forced Damascus to disband the Syrian Arab Air Defence Force and merge the remaining units in the Syrian Arab Air Force (SyAAF). Moreover, under Iranian advice and assistance, the military established government-affiliated militias (e.g. National Defence Force) inspired by the Iranian Revolutionary Guards Corps (IRGC) structure. These militias were to draw recruits from the regime's loyal populations (e.g. the Allawite-coastline, Shi'a and some Christian communities).

The FSA was formed by diverse Sunni Arab militias, ranging from defecting servicemen to secularists, Islamists and Salafists. While all militant groups converged on the aim of overthrowing Assad, their post-conflict agendas differed. Some envisioned transforming Syria into a strict Sharia-based Islamic emirate (i.e. Salafists), others into a Western-aligned democracy. Starting with early 2012, Jabhat al-Nusra (JS) claimed its first attacks in Damascus. JS was initially associated with al-Qai'da (AQ) and closely aligned with the emerging Islamic State of Iraq (ISI) next door. However, JS-leader Muhammad al-Jowlani pledged allegiance to AQ's top emir Ayman al-Zawahiri, after publically falling out with ISI (U.S. Department of State 2017). As JS became the strongest opposition group in Syria, it re-branded twice and is currently known as Hayat Tahrir al-Sham (HTS). However, back in 2012, due to the rapid emergence of JS, Ahrar al-Sham, Liwa al-Islam and Suqor al-Sham, the Syrian jihadist component became an integral part of the opposition (Lister 2014, 87).

Iranian intervention

By 2012, the FSA inflicted serious territorial losses to the Syrian Arab Army (SAA). In response, Hezbollah, a Lebanese Shiite militia, deployed thousands of fighters to combat the opposition in Syria (Sullivan 2014, 11). Besides Hezbollah, the Iranian Revolutionary Guards Corps (IRGC) sponsored and coordinated the deployment of numerous other Shiite paramilitary units from Iraq, Afghanistan and Pakistan (e.g. Imam Ali Brigade). However, Iran's spearhead force in Syria has been the external branch of the IRGC, known as the al-Quds Force (Arabic name for Jerusalem). The IRGC-Quds Force is tasked with the sole objective of "exporting the [Islamic] revolution to the world," spreading Ayatollah Khomeini's fundamental interpretation of Shiism (Wigginton et al. 2015, 162). Besides the ideological component, Iran's strategic objective is to establish a land corridor linking Iran to the Mediterranean Sea. Coined by the Jordanian king as the "Shi'a Crescent" (Barzegar 2008, 87-88), Iran seeks to achieve this corridor by keeping Lebanon under Hezbollah's dominance, maintaining Bashar al-Assad sovereignty over the Syrian territory, while seeking to evict the U.S. forces from Iraq and control it via proxy political parties and their military wings. The Shi’a Crescent would also play the role of a military logistics network for supplying its allied militias during war with Israel.

Spread of ISIS and the Kurdish Resistance

In 2013, the neighbouring Islamic State of Iraq (ISI) expanded into Eastern Syria and drove JS and other FSA groups out of Raqqa city. Militarily unopposed, ISIS (includes “Syria” or “al-Sham”) captured nearly the entire Turkish borderlands and besieged a number of Kurdish and Arab self-protection units in the frontier town of Kobani. In late 2013, the U.S. expanded close air support operations from Iraq to Syria, aiding the joint Kurdish-Arab militias in fighting off the ISIS assault. The efforts payed off in early 2014, when the siege was lifted and ISIS experienced its first defeat. Under U.S. leadership, but with the support of over 40 countries, the U.S. founded the Global Coalition against ISIS. Through this framework, the Kurdish Self-Protection Units (YPG in Kurdish) and select local Sunni Arab militias received direct training, arms and air support from the Coalition to recapture the expansive ISIS territory. Later on, the Arab-Kurdish militias united under a common banner, called the Syrian Democratic Force (SDF). As argued by many, the SDF brand is an attempt at appeasing Turkey, by watering down the YPG’s ties to Ankara’s archenemy, the PKK (Stewart, 2017).

The Russian Intervention

Disturbed by the growing Western presence in Syria and daring to further its geopolitical resurgence, Russia made a crucial entrance into the war. In September 2015, Russia deployed air squadrons, ground elements, and a naval task force to support Syria’s pro-governmental forces. While officially branded as an anti-terror intervention, Russia directed over 80 percent of its air strikes on groups other than ISIS (Stubbs 2015). Its indiscriminate bombing campaign is credited with bringing the opposition to its knees in the battle for Aleppo (2015 to December 2016) and overall for saving the Assad regime (Martin 2018, 1).

Weakened and boxed into small territorial pockets throughout western Syria, the FSA and Islamist groups entered the Astana agreements in 2017. The Astana agreements refer to a trilateral Turkish-Russian-Iranian platform that sought to de-escalate the battlefronts in Da’ara, Suweida, Hama and Idlib province. Within this framework, Turkey deployed additional forces to Idlib province to protect the opposition groups, expanding its military presence in Syria, after having launched two land operations in the past (e.g. Operation Euphrates Shield in 2016 and Operation Olive Branch in 2017).

The Fall of ISIS

In October 2017, under a massive U.S. air campaign, the Coalition-backed SDF ousted ISIS from its self-proclaimed capital (Harp 2018). With the remnants of ISIS condensed in the sparsely populated Eastern Syria, the pro-governmental camp and the SDF raced each other to liberate the Mid-Euphrates River Valley (MERV) and recapture the Iraqi border. Iran completed its strategic objective in 2018, after liberating the strategic border town of Abu Kamal, opening a terrestrial supply line between Iran, Iraq and Syria (Mansharof 2019). The SDF liberated its (eastern) part of the MERV only in early 2019, after capturing the last square meters controlled by ISIS in a makeshift camp near Baghuz al-Faqwani village (Wedeman & Said-Moorhouse 2019).

Israel's Covert Raids

Against this backdrop, Israel, who seeks to avoid an Iranian entrenchment in Syria by all costs, has regularly and covertly prosecuted positions of the IRGC-Quds Force and its proxies. The over 200 bombings executed by the Israeli Air Force (IAF) hit missile depots, logistics nodes, intelligence stations, and fighting positions in Damascus, Hama, Latakia and Aleppo (Gross 2018). Currently, the Israeli-Iranian confrontation is on the forefront of tensions in Syria, with Russia trying to act as mediator, while consolidating its military gains (e.g. Naval Support Facility in Tartus and Hmeimim Air Base in Latakia).

At the time of this writing: The U.S. is in the process of a slow troop drawdown, while the SDF and Turkey remain in near-war tensions. While still in disarray, ISIS has slowly regenerated its networks across Syria and has used its residual presence to stage bombings, assassinations, and ambushes across SDF- and regime-held territories. On the opposition-regime front, the pro-governmental camp has recaptured almost all of the Syrian territory, including the country's most populated areas (i.e. the West). Turkey continues to assert firm political and military control over

North-Western Aleppo province, following its 2016 and 2017 offensives in al-Bab and Afrin. After years of deteriorating conditions and divisions, JS-turned-HTS has become the strongest opposition group in Syria. Alongside Turkey, HTS is at the forefront of deterring an impeding governmental offensive in Idlib, the militants' last stronghold.

What has been said about the war

Despite the inherent military nature of the conflict, few peer-reviewed articles and books have given attention to defence-related developments in Syria. The few ones that do, have largely covered the military campaigns of select actors from a strategic and political perspective (see for example Juneau 2018; Zhou 2019; Byman 2018). Overall, the conflict's complex geopolitical, proxy and insurgency manifestations have been extensively covered (see for example Hughes 2014; Gupta 2016; Antonyan 2017; Byman 2018; Niu & Ali 2018). The very few scholarly endeavours that covered a military campaign from top to bottom and from logistics to operations are Tom Cooper's (2018) *Moscow's Game of Poker: Russian Military Intervention in Syria (2015-2017)* and Tim Ripley's *Operation Aleppo: Russia's War in Syria* (2018). The vast majority of academic texts focus on social and political aspects (see for example Dakhli 2013; Dixon 2017; Zisser 2017; Hinnebusch 2018; Colasanti et al. 2018; O'Leary & Heras 2019). In particular, the topics of religious mobilization (see for example Lister 2014) and sectarian discord (see for example Phillips 2015; Kerr & Larkin (eds.) 2015; Tomass 2016) have received the most attention.

The visible literature gap on the military developments of the armed conflict has been filled by media outlets, think tanks, OSINT platforms (e.g. Belingcat) and a vast array of Twitter users. The Institute for the Study of War (ISW) has produced particularly reliable and comprehensive map-based situation reports on Syria, published on a monthly or bi-monthly basis (see for example ISW 2019). SETA, a Turkish think tank, periodically issues tactical and technical reports, regarding Turkey's military operations in Syria (see for example Yesiltas 2017), which provide valuable insight in a topic sparsely covered by mainstream Anglo-Saxon organizations. As a firebrand military analysis centre, Jane's by IHS Markit has also been a constant source of defence commentary on the conflict. While comprehensive and well researched, think tank and academic publications did not come close to the timeliness and insights of products issued by OSINT platforms or by Twitter users with dual military and OSINT knowledge.

As demonstrated by McKeever (2019), Bellingcat, the open-source investigation website, managed to track the Kurdish insurgency in Afrin exclusively via social media. Enlisting SOCMINT support, the author determined the militias involved in operations, the operation-types (e.g. hit-and-run, ambush, assassinations) and quantitatively assessed the amount of anti-tank guided missile (ATGM) attacks launched by the insurgents. Bellingcat has conducted similar investigations in the past, and one concerning Turkey's offensive on al-Bab in particular, and even managed to accurately geolocate the sites of ISIS' ATGM attacks where Turkish Leopard tanks were lost (Triebert 2017). While they have different biases and areas of focus, Twitter users have frequently surpassed media outlets in speed and accuracy of reports. To list a few, @QalaatAlMudiq, @WyvernReport, @LuftwaffeAS and @GeromanAT are known for their insightful tweets on active battlefronts throughout Syria. Other users, such as @IntelCrab, @ELINTNews, @OBSIL and @ConflictsW are self-proclaimed OSINT aggregators, collecting all chatter and information regarding active conflicts.

There are also users with specific areas of expertise, who are applying their skills and knowledge to the Syrian Civil War. Aviation historian @BabakTaghvaee and aviation enthusiasts @CivMilAir, @redandblackattack, @CardiffOTT, @AIRFORCEFREAK and @GDarkconrad periodically share suspicious flights observed on ADS-B trackers or provide behind-the-scenes information on ongoing military movements. @YorukIsik, a Turkish self-proclaimed ship spotter, does not only track vessels on AIS monitors, but also photographs military-related ships as they pass through the Bosporus strait. He then shares his photos and findings online. The Turkish shipspotter's special coverage of the Russian Navy's transits to Syria received widespread media attention (see for example Sharkov 2016). Other maritime-oriented Twitter users are @D_Mitch, @CovertShores @steffanwatkins.

With an unmatched GOINT/IMINT expertise, users @obretix, @reutersanders, @intellipus and @border9999 are famous for geolocation all types of military events or equipment, using the sparsest photos and videos surfacing from active conflict zones. Self-proclaimed Syrian conflict cartographers @Syria_map, @Suriyakmaps, @A7_Mirza, @deSyracuseand @EmmanulGMay regularly tweet images with daily or weekly updates of ongoing military operations in Syria.

How are they doing it? By fusing the two major components discussed in the first section of this research: OSINT tools and knowledge on military logistics. As the following sections will show, the OSINT-LSO nexus can produce a wide variety of intelligence analytical products, which sometimes top the quality of classified intelligence.

3.2. Intelligence on Enemy Capabilities: Russian Military Deployments to Tartus Naval Facility and Hmeimim Air Base

In its first major military intervention overseas since the Cold War, Russia deployed a plethora of air, naval, and land forces in support of the pro-government forces in Syria. The deployment began in September 2015, following a bilateral agreement signed with the Syria Arab Republic a month before, which grants Russia access to Hmeymim Air Base, an airfield adjacent to Basil al-Assad International Airport in Latakia. In addition to the airfield, Russia also built up forces in the Naval Support Facility in Tartus, a logistical maintenance port leased to the USSR by Hafeez al-Assad in 1971. Prior to its full-blown intervention, Russia had consistently aided the Assad regime throughout diplomatic and military-technical means (Antonyan 2017, 341). For example, as an OSINT analysis by Oryx (2014) revealed, Russia's Military Intelligence Directorate (known as GRU) operated at least one major SIGINT radio-interception facility (Center-S) in Southern Syria, until it was stormed and captured by the FSA in 2014.

As for motivations, on the one hand, Moscow wanted to prevent the collapse of its strongest ally in the Middle East at the hands of another Western intervention. In addition to being one of Moscow's oldest partners, Syria is also a main buyer of Russian arms and is the only foreign government to host a Russian military base on its soil. On the other hand, Russia feared the growing radicalization of its Muslim minorities, particularly in the Caucasus. By 2015, over 2,000 Russian citizens had already joined ISIS in Syria (Bulos et al. 2015). Later estimates show that as many as 5,000 Russian citizens emigrated to fight in Syria (Sanderson et al 2017, 12). As stated by President Vladimir Putin, Russia felt the need to pro-actively combat the rising jihadist threat that could eventually re-direct to its own soil. Overall, the military intervention in Syria reflected Russia's pathway towards a geopolitical resurgence and facilitated a new issue to negotiate with the West (Antonyan 2017, 342). Russia has furthermore used the Syrian theatre of war to battle-test and advertise its new weapons systems, ranging from cruise missiles launched by its Caspian vessels to experimental fifth generation Su-57 stealth jets.

While officially branded as an anti-terror intervention, the first sorties conducted by the Russian Aerospace Forces (RuAF) on September 30, 2015 targeted the opposition in Homs, Hama and Latakia provinces (Casagrande 2016). A Reuters data analysis of the 780 sorties conducted in the first month concludes that "almost 80 percent of Russia's declared targets in Syria have been in areas not held by the Islamic State" (Stubbs 2015). This trend was sustained in the following years, as Russia primarily targeted the Syrian opposition groups, particularly those affiliated with the U.S. Central Intelligence Agency's (CIA) train-and-equip program, codenamed "Timber Sycamore" (Heneghan & Perry 2015).

From early to mid-November 2015, Russia surged its sorties against ISIS in retaliation for the downing of Russian Metrojet Flight 9568 over the Sinai Peninsula. A myriad of dumb bombs and laser guided missile were used to target infrastructure, command and control nodes, and fighting positions of ISIS in its self-proclaimed capital of Raqqa and other locations. Increased coordination between the Syrian and Russia militaries also enable the RuAF to provide close air support sorties for two major government offensives towards Aleppo and Palmyra (Lavrov 2018, 5-6).

In late November 2015, Turkey downed a Russian Su-24, after it had repeatedly violated its airspace and harassed its aerial interceptors in the past weeks. This prompted Russia to deploy its advanced long-range S-400 SAM system in Latakia and to direct more air strikes against Turkish-backed groups, specifically the Turkmen formations in northern Latakia. By early 2016, Russia helped the SAA to secure most of those areas and pushed the militants away from Russian military bases and the regime's support base.

Before the battle of Aleppo, the pro-governmental camp aided by the RuAF cut the main supply line between Turkey and opposition groups inside Aleppo. After blocking their logistical lines of communications (LOCs), the RuAF besieged Aleppo with a campaign of maximum aerial pressure. In some instances, over 100 bombings were launched within 48 hours (Lavrov 2018, 10). Following a small-scale force drawdown, the RuAF temporarily re-directed its efforts to aid the SAA's offensive on Palmyra. Located in Syria's eastern desert, Palmyra was frequently exchanged between ISIS and the SAA. The final liberation, also aided by Russia, came only in early 2017.

By December 15, 2016, the over 10,000 opposition fighters trapped in Aleppo's eastern neighbourhoods surrendered, following months-long attrition combined with intensive RuAF air raids flown from Hmeymim Air Base, Admiral Kuznetzov aircraft carrier in the Mediterranean Sea, and temporarily from Iran's Hamedan Air Base. With the surrendering fighters evacuated towards Idlib province, the pro-governmental camp focused on a new counter-offensive in Palmyra and later on, pushed towards the Mid-Euphrates River Valley (MERV). As the U.S.-backed SDF was engaging ISIS in its "capital" of Raqqa and the Turkish-backed Euphrates Shield stormed the jihadists in northern Aleppo, the pro-governmental camp profited and attacked ISIS in Deir ez-Zor province. In September 2017, the SAA supported by the RuAF lifted the three-year-long ISIS siege on the desert "enclave" of Deir ez-Zor city and the adjacent air base.

The second-half of 2017 was marked by clearing operations on the MERV banks and by the gradual de-escalation of the other battlefronts via the Astana accords, mediated between Russia, Turkey and Iran. Russia furthermore forward deployed attack and transport helicopters to Syrian Arab Air Force (SyAAF) airfields and mobilized its motorized infantry units in expeditionary operations. However, the parallel SAA and SDF offensives on the western and eastern sides of the Euphrates were not free of incidents. In October 2017, Syrian armoured units, augmented by over 100 Russian private contractors of Wagner Group acting as light infantry, crossed the Euphrates in an attempt to storm an SDF outpost and capture the nearby oilfields. This attack prompted a massive U.S. aerial counterattack, involving gunships, attack helicopters, fighter jets, and bombers, that obliterated the advancing force. While Russia rejected having any connection with the notorious Wagner Group, this incident shed light on the large-scale presence of Russian private contractors in the war.

In 2018, the Russian mission in Syria surged with tactical fighter aircraft reinforcements. Most assets were tasked with supporting the SAA siege on Eastern Ghouta, an opposition-held suburb in Damascus. As the Astana and later Sochi mediation talks continued, all opposition groups were re-directed to the Idlib de-escalation zone – an area encompassing Idlib province, northern Hama province, western Aleppo province and north-eastern Latakia province. Throughout the rest of the year, Russia alongside its Syrian, Iranian and transnational allies have been readying forces for an all-out offensive on the last opposition stronghold. However, in 2018 Russia also experienced severe combat aviation losses due to friendly and enemy ground fire.

Moreover, as Israel escalated its operations against the IRGC and allied militias in Syria, Russia has been caught been rock and hard place in its delicate balancing act. In September 2018, a Russian Il-20 maritime surveillance plane was accidently downed by a Syrian S-200 surface to air missile (SAM). The Syrian SAM was targeting an Israeli F-16 operating in the area (Lewis et al. 2018) and had mistakenly locked on the larger aircraft. After a brief moment of tensions, by the time of this writing, Russia and Israel are still in coordination over the IAF's counter-Iran operations in Syria.

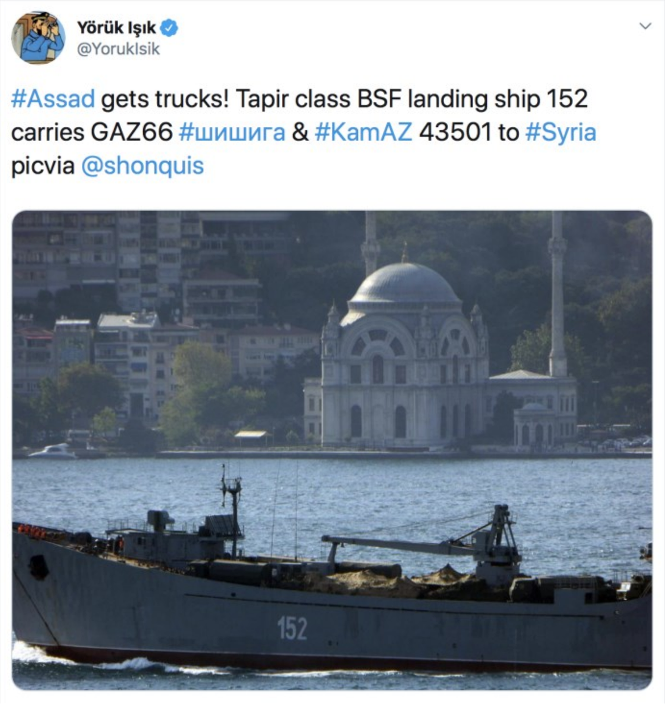
Furthermore, Russia has neither signalled the intention nor provided a timeframe for an eventual withdrawal of all Russian troops from Syria. In fact, the Russian government had secured a multi-decade control over both its military installations in Syria (Tartus Naval Facility and Hmeymim Air Base).

Based on this overview, the forthcoming sections will detail how the LSO-OSINT nexus revealed and uncovered Russia's military movements in Syria throughout the aforementioned stages of the war.

3.2.1. Force Deployment: Spoiling Russia’s “Syria Express” LOC

Even before Russia publicly announced the military deployment to Syria, OSINT users have been monitoring its logistical networks for clues. Russia relied on two main lines-of-communications (LOCs), seaborn and airborne. The maritime LOC ran from the Black Sea Fleet (BSF) headquarters in Sevastopol (Crimean Peninsula) to the Tartus Naval Facility on the Syrian coastline. The primary airbridge linked Mozdok Air Base in Russia’s Southern Military District to Hmeymim Air Base in Latakia.

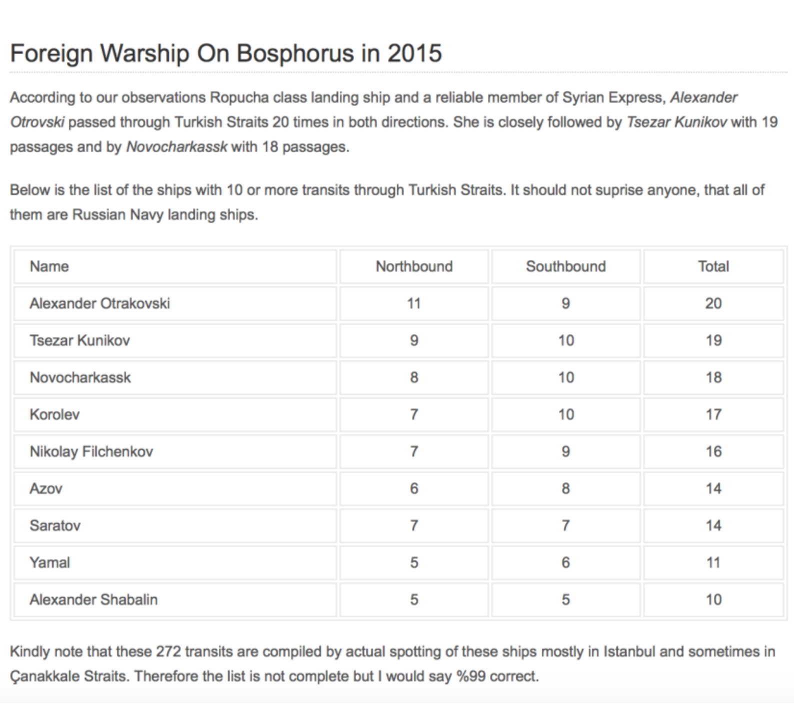
SOCMINT acquired from Twitter users @YorukIsik and other shipspotters aggregated by the website “Bosphorus Naval News” (2015a) showed very early logistical shipments from Sevastopol (Crimea) to Tartus (Syria) via the Turkish straits. Based on high-resolution photography that surfaced on Twitter, the “intelligence minutemen” detected the southbound sail of six large landing ships between August 20 and September 10, 2015 (four Ropucha-class, one Alligator-class and one Kashtan-class vessel). Moreover, with 99% accuracy, the *Bosporus Naval News* compiled a dataset of 272 visually confirmed foreign ships that transited the Bosporus. The overwhelming majority represented Russian military vessels commissioned from Crimea for southbound sails. The vessels conducting most of these supply runs were the large landing ships *Alexander Otrakovski* (20), *Tsezar Kunikov* (19), *Novocharkassk* (18) and *Korelov* (17) (Bosporus Naval News 2015b), specialized in cargo transport and launch on shore. While usually the cargo on deck was hidden under camouflage nets and in containers, in some instances, OSINT observers identified the equipment on board. For example, on August 20, 2015 a Tapir-class Black Sea Fleet (BSF) vessel shipped GAZ66 and KamAZ 43501 military logistics trucks to Syria (@YorukIsik 2015a). While not classified, the SOCMINT on naval movements in the Bosporus undeniably spoiled Russia’s preparation for military operations in Syria weeks in advance.



Yörük Işık
@YorukIsik

#Assad gets trucks! Tapir class BSF landing ship 152 carries GAZ66 #шишига & #KamAZ 43501 to #Syria picvia @shonquis

Figure 7 Russian vessel carrying KamAZ trucks to Syria (@YorukIsik 2015a)



Foreign Warship On Bosphorus in 2015

According to our observations Ropucha class landing ship and a reliable member of Syrian Express, *Alexander Otrovski* passed through Turkish Straits 20 times in both directions. She is closely followed by *Tsezar Kunikov* with 19 passages and by *Novocharkassk* with 18 passages.

Below is the list of the ships with 10 or more transits through Turkish Straits. It should not suprise anyone, that all of them are Russian Navy landing ships.

Name	Northbound	Southbound	Total
Alexander Otrakovski	11	9	20
Tsezar Kunikov	9	10	19
Novocharkassk	8	10	18
Korolev	7	10	17
Nikolay Filchenkov	7	9	16
Azov	6	8	14
Saratov	7	7	14
Yamal	5	6	11
Alexander Shabalin	5	5	10

Kindly note that these 272 transits are compiled by actual spotting of these ships mostly in Istanbul and sometimes in Çanakkale Straits. Therefore the list is not complete but I would say %99 correct.

Figure 6 OSINT inventory of Russian sails through the Bosphorus in 2015 (Bosphorus Naval News 2015b)

Between late August and early September, Twitter accounts shared dozens of photos posted by Russian servicemen on their social media accounts, proving their presence in Syria (see for example @Paradoxy13 2015; @bdrhmnhrk 2015; @JulianRoepcke 2015). The first photos of cargo being unload from military transports on the Hmeymim Air Base tarmac surfaced on August 21 (@green_lemonnn 2015). Continued SOCMINT reports of infrastructure build-ups in Latakia drew the attention of other OSINT observers, media outlets, and think tanks. With commercial GEOINT/IMINT ordered from Airbus, both Stratfor (2015) and *Foreign Policy* (Lewis 2015) identified runway improvements and the construction of helicopter pads, new taxiways, and hangars as part of Russia's enhancement of the Latakia airfield. Visible on ADS-B trackers, Ilyushin Il-62M and other RuAF cargo planes were establishing Russia's airborne LOC towards Hmeymim Air Base, starting with early September (@trbrtc 2015).

In an analysis tilted "Are Russian Troops in Syria?" *Bellingcat* aggregated and examined various open-source content related to this topic (Leviev 2015). The authors conducted forensic analysis of videos that surfaced on Twitter and that showed Russian military assets operating in Syria. In particular, one Russian-made Pchela 1T drone and three silhouettes resembling MiG-29/Su-34 or Su-27 aircraft were filmed over Idlib province. Land-based weapons systems such as the BTR-82A were also captured in various photographs that made their way online. Furthermore, *Bellingcat* profited from social media OPSEC leaks and compiled conclusive SOCMINT on Russian personnel, particularly sailors, dispatched for long-term deployment (three to eight months) in Syria.

U.S. officials with knowledge of classified intelligence anonymously described the situation in August and September 2015, stating that “there are some worrisome movements – logistical, preparatory types of things” (Gordon & Schmitt 2015). This suggests that the American intelligence agencies, much like the OSINT community online, was on the lookout for logistical movements and likely saw the same assets being moved and the same LOCs being used that the Twitter users were monitoring. At that point the Kremlin was still denying that it had plans to engage in combat operations, vowing that its military is only acting in an advisory capacity (BBC 2015).

More than a week before the RuAF launched its first bombings on targets in Syria, IMINT/GEOINT acquired from a commercial provider and shared on Twitter revealed the type, number, and extent of Russia’s aircraft deployments in Hmeymim Air Base (@galandecZP 2015). The satellite imagery was dated from September 21, 2015 and showed – with basic military hardware knowledge and interpretation skills required – the presence of 28 aircraft lined up on the air base taxiway (four Su-30SM air superiority fighters, 12 Su-25SM and 12 Su-24 attack aircraft). OSINT users identified the aircraft type, using publicly available design schematics and matching the aircrafts’ unique colour scheme (camouflage pattern) with other aircraft photos from the world wide web. As revealed by CNN’s U.S. government sources, the 28 Russian jets flew with their transponder off and hid behind the radar signature of a larger transport aircraft that was accompanying the formation, in an attempt to avoid detection (Starr & Levitt 2015). While the RuAF tried to build-up its forces in silence, a simple and universally accessible satellite image spoiled it all.

Furthermore, a second deployment formation of Russian jets was uncovered, as they flew to Hmeymim Air Base on September 28, 2015. Consisting of six Su-34 strike fighters, Twitter users @ain92ru (2015) and @capach28 photographed two of them as they left Mozdok Air Base (Russia), while @LuftwaffeAS (2015a) shared of photo of one Su-34 descending for Hmeymim’s runway. A second photo shared by

@LuftwaffeAS (2015b) shows a large transporter leading a formation of six other small aircraft over Syria. As OSINT analysts suspected that the RuAF might be using the same procedure to sneak its assets into Syria, as revealed by the CNN sources, they looked over ADS-B trackers. Coincidentally, they found a RuAF Tu-154 (callsign RFF7085) jet airliner flying from Russia’s Southern Military District to Hmeymim Air Base with its transponder on (Cenciotti 2015). Following the insertion-pattern of the previous deployment, this likely revealed the flight path followed by the six Su-34 outbound from Mozdok Air Base, photographed and reported in formation with a large transporter.

By the time Russia launched its first air strikes on September 31, 2015, OSINT users had thus managed to establish the RuAF’s initial order of battle.

3.2.2. Keeping Up With the Russian Order of Battle

The OSINT game of cat-and-mouse continued throughout Russia’s entire deployment in Syria. One collection focus was to periodically recon the Hmeymim Air Base, using commercial GEOINT/IMINT, and to update the open-source record of the RuAF’s order of battle.

Shortly after the air strikes commenced, in mid November, the RuAF ordered a series of home-launched long-range bombings in Syria. While the bombers rarely made stops at Hmeymim Air Base, which would have allowed them to be photographed by satellites, Twitter users managed to document their journeys. Using official footage released by the Russian Ministry of Defense, the users were able to confirm the aircraft-type (five Tu-160s, six Tu-95M and 14 Tu-22M3 strategic bombers) and retrace the origin of some to Mozdok Air Base. Furthermore, by conducting forensic media analysis of the aircrafts’ underbelly and photographed debris from the ground, Twitter users were able to identity the types of ammunition expanded (@JosephHDempsey 2015). In many bombings, they observed the launch of the experimental low-observable Kh-101 cruise missiles, likely from a Tu-160, and the heavy use of unguided dumb bombs.

On February 6, 2016, Digital Globe imagery interpreted by Stratfor (2016) showed eight Su-24s, five Su-25s, six Su-34s and four Su-35s on the taxiway. Satellite images taken on November 20, 2016 and interpreted by Jane by HIS Markit, confirmed the transfer of assets from Russia's aircraft carrier, which was deployed in the Mediterranean Sea at that time, to Hmeymim Air Base. IMINT analysis suggested the presence of seven Su-24Ms, eight Su-33s, two Su-34s, two Su-35s and one MiG-29K multirole fighter jet (Neff 2016). Based on colour patterns, the authors assessed that the eight Su-33s belonged to the Russian Navy (RuN) and, together with the MiG-29, were re-deployed from the RuN-operated Keznetsov aircraft carrier. The discovery drew attention to the level of problems experienced by Russia's sole flattop.

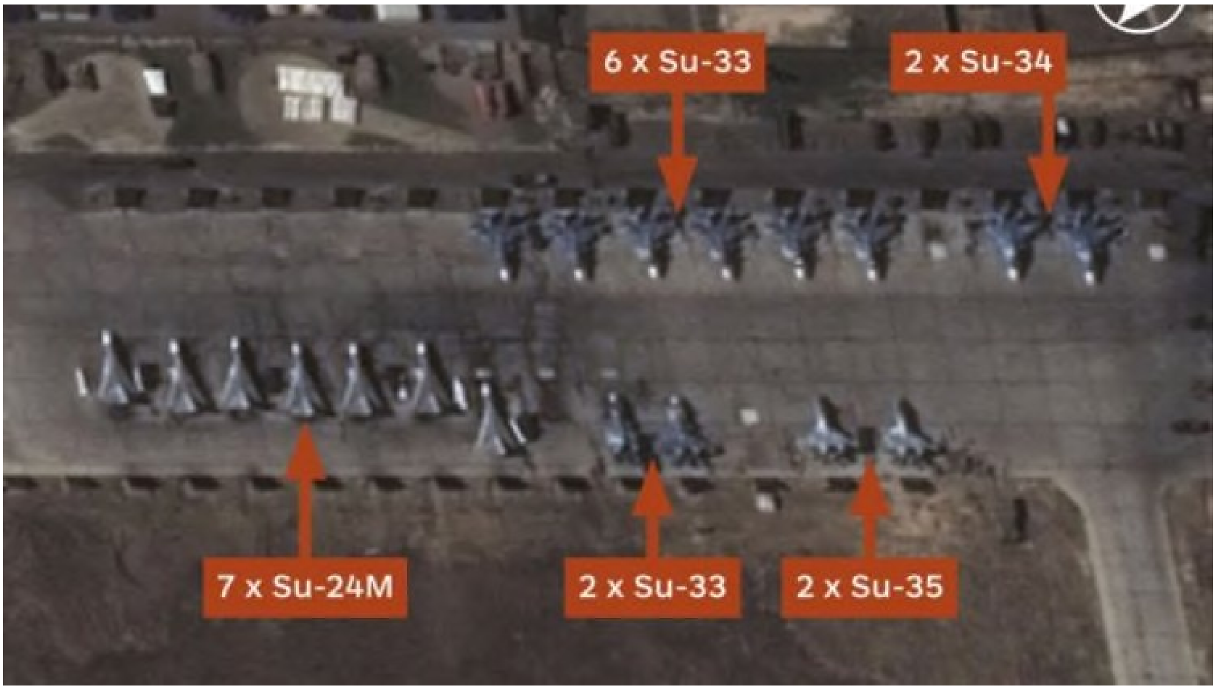
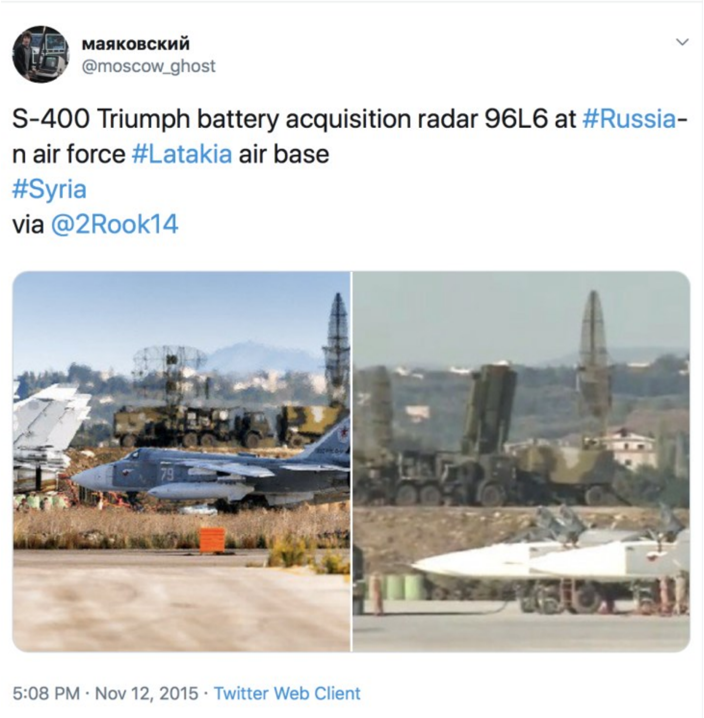


Figure 8 IMINT shows Russian air order of battle in Syria (Neff 2016)

On January 19, 2017, IMINT published by Bellingcat (2017) showed the presence of three Su-30Ms, three Su-34Ms, four Su-35s, four Su-25s and 11 Su-24s at Hmeymim Air Base. This contradicted Russia's official announcement that it will affect a partial withdrawal of its forces as victory over Aleppo was achieved. While Russia withdrew four Su-24s, it supplemented its posture effectively by re-deploying four Su-25s shortly afterwards (Lavrov 2018, 14). As the RuAF has periodically forward-deployed smaller air assets to semi-prepared airfields throughout Syria, one notable discovery made through OSINT was the presence of a Forepost unmanned aerial vehicle (UAV) in SyAAF’sT-4 air base on May 1, 2019 (@obretix 2019a).

IMINT from August 29, 2018, shared by @obretix (2018a), showed eight Su-24s, four Su-34s and four Su-35s on the air base tarmac. One A-50, two An-26/30 and three Il-22 cargo planes were also spotted on an eastern apron. The imagery furthermore revealed the construction of aircraft shelters. While aircraft shelters conceal fighter aircraft from GOINT/IMINT-collection, even after their completion, satellite imagery shared by @obretix (2019b) on January 30, 2019 showed seven Su-24s, four Su-30s and four Su-34s parked outdoor. Eight helicopters and two large aircraft (A-50 and Il-20) were also visible on the tarmac.

In addition to air assets, OSINT users have also focused on Russia’s surface-to-air missile (SAM) systems, naval assets, and ground-based striking capabilities that form the anti-access area denial (A2/AD) zone over western Syria. While Russia officially announced the deployment of its elite S-400 system to Syria only after Turkey downed one of its jets on November 25, 2015 (Marcus 2015), the S-400’s 96L9 “Cheeseboard” acquisition radar was photographed in Hmeymim Air Base since November 12, 2015 (@moscow_ghost, 2015). While parading the S-400 deployment to Hmeymim in front of the media, Russia (accidentally or deliberately) leaked the presence of the Pantsir S-1 short-range self-propelled air defence system in some official photos (@towersight 2015).


маяковский
@moscow_ghost

S-400 Triumph battery acquisition radar 96L6 at #Russian air force #Latakia air base
#Syria
via @2Rook14

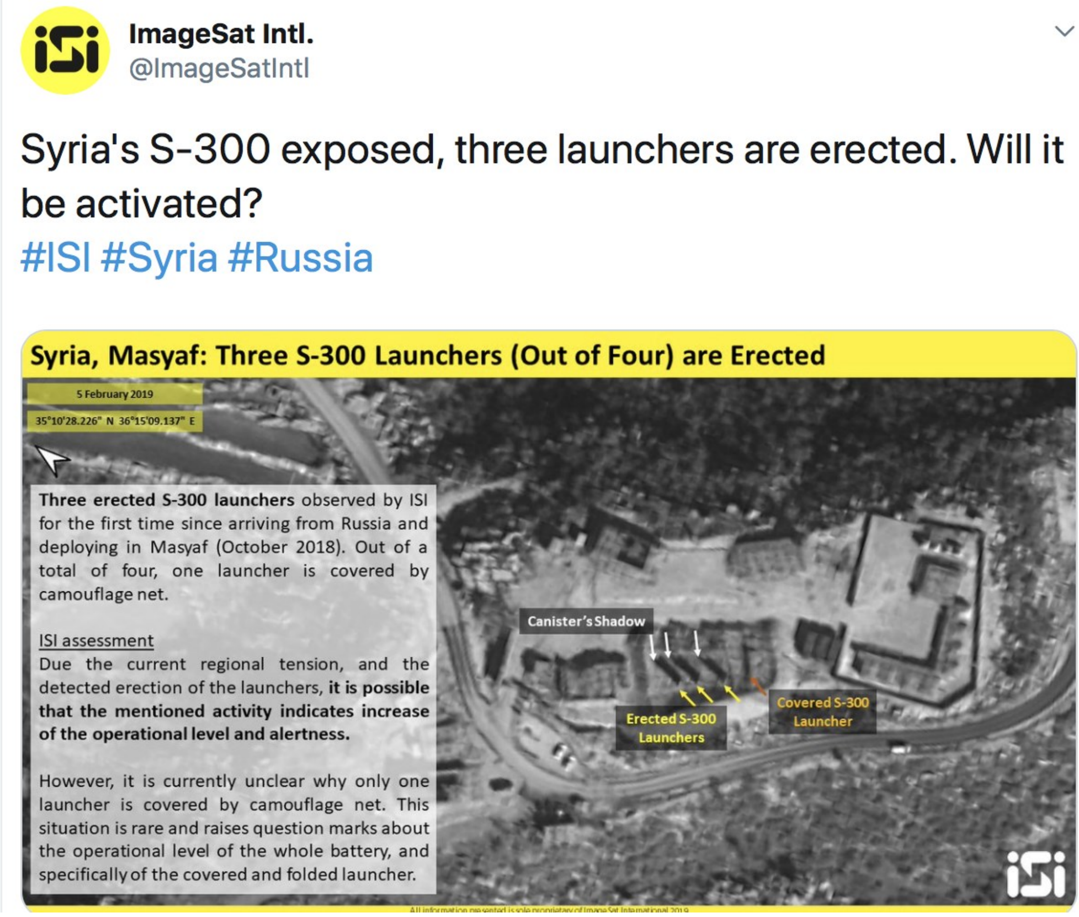
5:08 PM · Nov 12, 2015 · Twitter Web Client

Figure 9 The S-400's 96L6 acquisition radar spotted in Syria (@moscow_ghost 2015)

At some point in early 2017, Russia deployed a second S-400 battalion set in Syria. By September, Jane's by IHS Markit satellite imagery analysis detected the precise location of the S-400 deployment (35°9'55"N 36°15'41"E). The SAM system assumed combat-duty in the Masyaf hills air defence revetments in Tartus province (Binnie & O'Connor 2017). With the anti-air nests from the Masyaf hills receiving public attention, OSINT users also revealed the presence of the SyAAF's obsolete S-200 SAM batteries just meters away from the Russian S-400. As discussed in the previous section of this research, IMINT interpretation was guided by entity recognition (e.g. radar type, tractor erector launcher) and site layout.

Following a press tour of Russia's military bases in Syria in April 2018, a Russian military analysis website discovered and photographed at least one Tor M-2 aerial defence system on the grounds of Hmeymim air base (@ecoross1 2018). Previously, there was no information regarding a Tor deployment in Syria. This revealed that Russia had been enhancing its point air defence posture, constantly strengthening its anti-air capabilities in Syria.

Furthermore, OSINT revealed Russia's newest strategic SAM deployment in Syria. After the September 2018 incident, when a SyAAF S-200 SAM accidentally downed Russia's Il-20 aircraft, while trying to shoot down an Israeli jet, Moscow vowed to overhaul the Syrian air defences. Russia deployed four battalion sets of the S-300PM2 (domestic, non-export version) with the supposed intention of donating them to the SyAAF (BBC 2018). Using ADS-B, OSINT observers tracked six heavy-lift RuAF planes active on the air bridge between the Southern Military District and Hmeymim base between September 29 and October 1, 2018 (@avischarf 2018). On October 3, Russia released official footage of S-300 battery elements being unloaded from two of the An-124 planes monitored online over the past days (@EmbassyofRussia 2018). On November 1, photos emerged on social media showing Russia servicemen instructing their Syrian counterparts on how to operate the S-300PM2 system (@TheHawkOps 2018). In early 2019, commercial satellite imagery shared on Twitter showed that the newly-delivered S-300PM2 was deployed in the Masyaf hills, next to one of Russia's S-400 SAMs (@ImageSatIntl 2019a).



ImageSat Intl.
@ImageSatIntl

Syria's S-300 exposed, three launchers are erected. Will it be activated?
#ISI #Syria #Russia

Syria, Masyaf: Three S-300 Launchers (Out of Four) are Erected

5 February 2019

35°10'28.226" N 36°15'09.137" E

Three erected S-300 launchers observed by ISI for the first time since arriving from Russia and deploying in Masyaf (October 2018). Out of a total of four, one launcher is covered by camouflage net.

ISI assessment
Due the current regional tension, and the detected erection of the launchers, **it is possible that the mentioned activity indicates increase of the operational level and alertness.**

However, it is currently unclear why only one launcher is covered by camouflage net. This situation is rare and raises question marks about the operational level of the whole battery, and specifically of the covered and folded launcher.

Canister's Shadow
Erected S-300 Launchers
Covered S-300 Launcher
iSi
All information presented is sole proprietary of ImageSat International 2019

Figure 10 Syrian S-300 detected in Masyaf (@ImageSatIntl 2019a)

Being a matter of power projection and armament demonstration, Russia's sea-based operations have been widely advertised by the Kremlin itself. Likewise, Russia has been transparent regarding the establishment of the Fifth Operational Squadron (a permanent Mediterranean Task Force) based in Tartus and under the command of the Black Sea Fleet (BSF) (Russian Ministry of Defense 2017). However, the intelligence minutemen managed to impress again, when the RuN was amassing forces near the Syrian coastline in preparation for a planned offensive on the Idlib de-escalation zone. Starting with August 22, 2018, @YorukIsik spotted an increase in Russian military marine traffic towards the Mediterranean Sea. First, he noticed the Kashtan-class buoy tender KIL158 on a southbound sail, closely monitored by the Turkish coast guard (@YorukIsik 2018a) and, later on, other logistic and cargo ships. Two days later, three RuN vessels, one armed Krivak II-class frigate and two Alligator-class vessels loaded with infantry fighting vehicles simultaneously transited the Bosporus (@YorkIsik 2018b). On August 25, two Admiral Grigorovich-class frigates (*Admiral Grigorovich* and *Admiral Essen*), visibly armed with Kalibr anti-ship missiles, transited the Turkish straits on route to the Mediterranean (YorukIsik 2018c).

By August 25, 2018 the RuN had dispatched 13 warships and two submarines, which were armed to the teeth, near Tartus, all documented via OSINT channels (@Capt_Navy 2018). On August 29, NATO confirmed the large-scale naval build-up reported by open sources (Haaretz 2018). The RuN later issued a notice to airmen, closing the airspace and international waters in the Eastern Mediterranean to conduct war games. At least one U.S. Navy P-8 Poseidon (@GDarkconrad 2018a) anti-submarine aircraft and one E-3 Aries II SIGINT collection plane (@GDarkconrad 2018b) were constantly monitoring the Russian naval drills throughout September with their transponders on.

Russia's surface-to-surface capabilities in Syria also attracted the curiosity of OSINT observers. Moscow's in-theatre assets mostly consisted of the infamous Iskandar short-range ballistic missile (SRBM) system and the Bastion-P, a coastal battery developed for both ship and ground attack. While Russia confirmed the Bastion-P presence in November 2016 by demonstrating its multipurpose land-attack capability (Defense Blog 2016), the Iskandar deployment remained in the dark. However, Russia's shady Iskandar deployment in Syria was first detected by a private satellite imagery provider on December 28, 2016, and announced in January 2017. At least two Iskandar tractor erector launchers were spotted near the runway in Hmeymim Air Base. Additional batteries were believed to be on site; however, they remained covered by camouflage nets (ISI 2017). On December 18, 2018, the Russian Ministry of Defense admitted using the Iskander SRBM system in Syria, confirming its deployment. The Iskandar systems were still present in Hmeymim Air Base in April 2019, as shown by the same IMINT provider (@ImageSatIntl 2019b).

3.3. Forecast: Operational Design and Timeframe of the American-British-French Strike on Syria's Chemical Weapons Facilities

On April 7, 2018, open-source reports emerged of a chemical attack in Douma, an opposition-held suburb of Damascus. Rescue workers found over 40 people dead of asphyxiation in an apartment block and a large gas cylinder expanded in a bedroom (Hubbard 2018). The compressed gas cylinder had pierced through the roof, suggesting that it was released from an airborne delivery platform, and glided into the building. As Bellingcat's (2018) exclusive OSINT investigation found, the gas cylinder contained a deadly chloride composite and was most likely delivered by a SyAAF Mi-8 Hip helicopter, seen operating in the area around the time of the attack. Later on, the Organization for the Prohibition of Chemical Weapons (OPCW) also concluded that a chemical attack did happen on April 7, 2018 and involved the use of molecular chloride (OPCW 2019).

The international community rallied against the Assad regime, widely accused of carrying out the attack. On the forefront of these accusations were the United States, the United Kingdom, and France (Hubbard 2018), as both their legitimacy in the conflict and national interest dictated the need to discourage the proliferation of weapons of mass destruction. On Twitter, U.S. President Donald J. Trump (@realDonaldTrump 2018) was quick to announce the possibility of military action against the Syrian regime in retaliation for the chemical weapons (CW) attack. The U.K. and France also expressed punitive intentions (Kuenssberg 2018).

On April 14, between 4-5 a.m., Washington, London, and Paris commenced with a joint military strike on regime targets in Syria. The combined American-British-French allied force launched over 100 land attack cruise missiles from fixed-wing aircraft, surface ships, and submarines operating in the Mediterranean Sea, Persian Gulf, and the Red Sea (Rogoway 2018). The ordnance destroyed three sites specifically associated with Syria's CW program: Barzah Research and Development Center (Rural Damascus province), Him Shinshar CW storage site and bunker (Homs province).

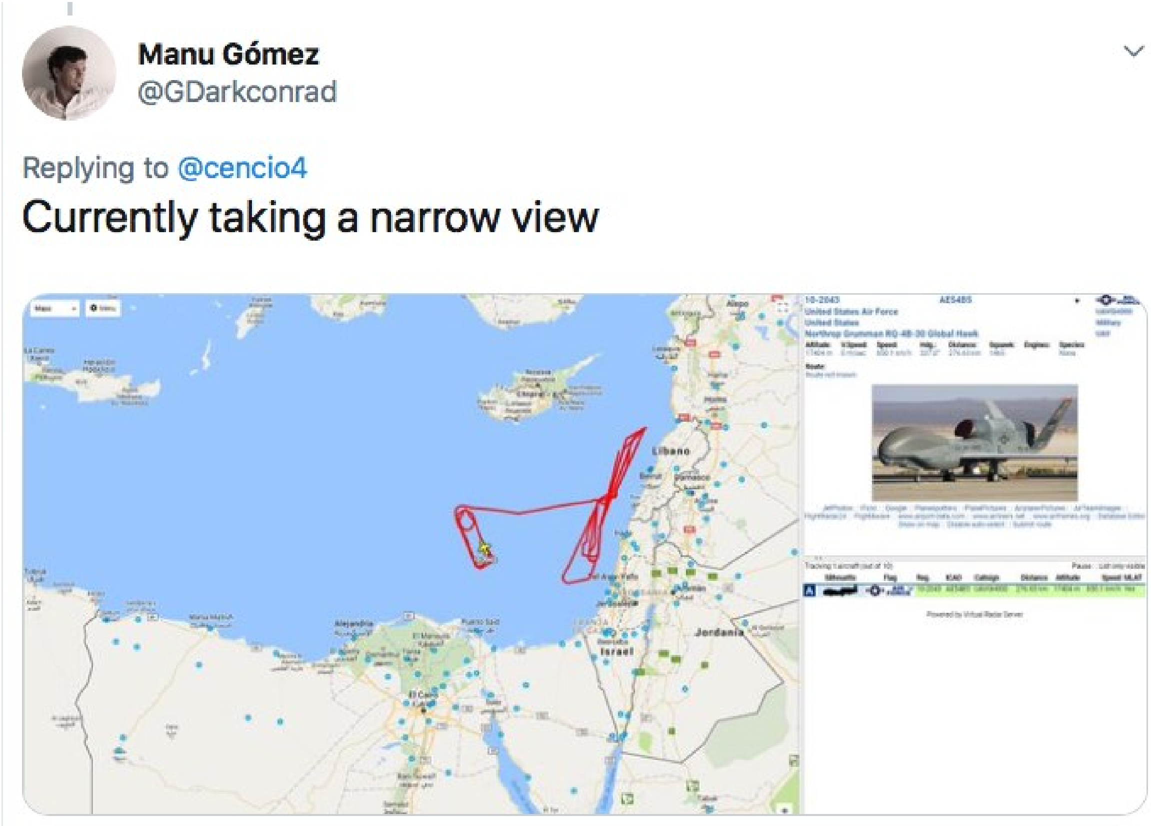
The U.S. Navy (USN) *USS Monterey* and *USS Laboon*, operating out of the Red Sea, fired 37 Tomahawk land attack missiles (TALMs), the secretive Virginia-class *John Warner* submarine launched six TALMs from the Eastern Mediterranean, and two USAF B1b bombers deployed from al-Udeid Air Base (Qatar) expanded 19 JASSM low-observable cruise missiles from Jordanian airspace. USAF F-16C and F-15C fighter squadrons from Aviano (Italy) and four F-22As stealth air superiority jets from al-Dharfa Air Base (United Arab Emirates), armed with air-to-air missiles, provided the Defensive Counter Air (DCA) escort for the bombing crews. The *USS Higgins* also fired 23 TALMS from the Persian Gulf.

British Royal Air Force (RAF) Typhoon and Tornado fighter jets expanded eight Storm Shadow air-launched cruise missiles towards Homs province. France fired nine cruise missiles from Rafale and Mirage fighter jets. Both the British and French jets operated out of the RAF Akrotiri Air Base (Cyprus). In addition, a French Aquitaine-class frigate also fired three "Missile de Criosiere Naval," the French indigenous equivalent of the American TALM.

Despite the secrecy surrounding the operation, OSINT users were hard at work to monitor aviation activity, marine traffic, and social media signs that might indicate the logistical build-up or LSO for such a strike. Focal points were the logistics nodes in the Eastern Mediterranean and the Persian Gulf. In two cables shared on Facebook by *T-intelligence*, the OSINT platform correctly predicted that a military operation would happen and estimated the 12-14 April timeframe at the crack of dawn as being the likely time of execution (HARM 2018c). The platform based its estimate on a notice-to-airmen (NOTAM), issued by the U.S. to commercial operators, urging them to avoid the Syrian airspace. Furthermore, the *T-Intelligence* assessment forecasted collective action (i.e. French and British involvement), a large concentration of forces in the Mediterranean Sea (naming the Sigonella air base as being key) and intense multi-platform intelligence collection sorties off Syria's coast.

3.3.1. Eavesdropping on Intelligence, Surveillance, Target-Acquisition and Reconnaissance (ISTAR) Sorties

Starting with April 11, the U.S. Air Force (USAF) launched several intelligence collection sorties off the Syrian and Lebanese coasts per day from Sigonella and Aviano air bases (Italy). One of the most featured aircraft was the "submarine-killer" maritime security plane P-8 Poseidon, which was frequently spotted on ADS-B Exchange over the Eastern Mediterranean between April 11-13, 2018 (see for example @AicraftSpots 2018a; @GDarkconrad 2018c). Having a naval aviation focus, the P-8 Poseidon was likely monitoring the RuN drills in the Mediterranean Sea (@CivMilAir 2018a). The RuN drills conveniently emptied Tartus of all Russian military vessels, serving as a strong indicator of an imminent Western military operation. The RuAF responded with its own surveillance rounds, launching Su-24s to buzz the French naval build-up in the Mediterranean (@BabakTaghvaee 2018a). In a similar move, the SyAAF also redeployed aircraft from its airbases to the "sanctuary" of Russia's Hmeymim Air Base.



Manu Gómez
@GDarkconrad

Replying to @cencio4
Currently taking a narrow view

Figure 11 RQ-4 drone flight path near the Syrian coast (@GDarkconrad 2018d)

One of the first assets to be observed and widely featured was an U.S. Air Force RQ-4 Global Hawk UAV conducting sorties off the Lebanese and Syrian coast. Call-sign FORTE 10 was tracked and shared on Twitter by user @AircraftSpots (2018b), as it was on station for ISTAR collection duty throughout April 13, 2018. FORTE 10 was replaced or supplemented after midnight by another RQ-4 UAV, call sign UAVGH000 (GDarkconrad 2018d). Based on the drone's GPS position transmitted via ADS-B, twitter user @cencio4 (2018) was able to estimate the RQ-4's sensor suite coverage at a 200-300 km range and a 45-degree angle. This brought parts of western Syria within range and narrowed the possible target-list that the U.S. defence intelligence was likely considering. Around 4 A.M. an SIGINT intelligence RC-135V plane, operated by the USAF, appeared on ADS-B trackers over the Eastern Mediterranean

(@AircraftSpots 2018c). As the "V" version of the RC-135 is purposed for tracking and geo-locating signals within the electromagnetic spectrum (US Air Force 2011), the plane was likely collecting radar spikes of the Syrian and Russian air defences. Another RQ-4 drone outbound from Sigonella Air Base (Italy) returned to the Eastern Mediterranean shortly after the offensive operations ceased (AircraftSpots 2018d). Callsign FORTE11 likely scouted the targeted areas for battle damage assessment (before and after comparison).

3.3.2 Fuel for "Thirsty" Fighters

Probably the clearest logistical indicator of an upcoming aerial operation was the spike in aerial refuelling traffic from the U.S. to Europe and later towards the Mediterranean region. As fuel is a key tactical logistics good, it needs to be provided directly to the frontline. Social media users were again quick to pick-up the flow of aerial refuelling assets and logistical preparations conducted by the USAF. On April 10, @StratSentinel (2018) published an ADS-B-acquired list showing 42 "flying gas stations" (i.e. KC-135 Stratotanker aircraft) airborne over the continental U.S. One day later, on April 11, user @hdevreij (2018) shared an ADS-B Exchange screengrab of five USAF KC-135s forward deploying from the United Kingdom via France to the Eastern Mediterranean. While they later made sparse appearances on trackers, it became clear that many of the aerial refuelling aircraft were dispatched from the U.S. to Europe as part of LSOs. The KC-135s re-appeared on ADS-B Exchange immediately after the conclusion of the trilateral American-British-French strikes on Syria (@Buzz6868 2018). Some of them were still circling the area of operations, likely refuelling the F-16s and F-15s returning from DCA duty, while others were bound for their home base

Impressed by the power of OSINT during the American-British-French punitive strike, Major Atkins (2019) emphasized in a USAF journal the minute-by-minute account and in-depth tracking of tanker and ISR support aircraft by amateur analysts as the operation was unfolding (35). While OSINT analysts were successful in identifying the LOCs, tracking some of the assets populating the supply lines, and forecasting the timeframe of the operation, they remained overly focused on the Eastern Mediterranean. There was virtually no mention of the USN vessels operating in the

Red Sea or about logistical preparations in the USAF’s major Persian Gulf bases (al-Udeid and al-Dharfa). The latter played a major role in the campaign. Furthermore, in this case, OSINT analysts were not to be blamed for spoiling military OPSEC, as President Trump has repeatedly signalled (deliberately or not) his intention to punish the Assad regime for the Douma CW attack. However, this episode does show that even in OSINT austere situations, such as classified military operations, “intelligence minutemen” can prove resourceful in their collection and creative in their assessments.

3.4. Battle Damage Assessment: Israeli Air Force Raids on the IRGC

Despite its apparent neutrality in the conflict, Israel was not indifferent to the developments in Syria. Jerusalem’s main security threat is the entrancement of Iran and its affiliated transnational militias in Syria (e.g. force build-up, missile deployments) and the smuggling of advanced weaponry to the Shiite Lebanese Hezbollah. Founded in 1982 with Iranian assistance and funds, Hezbollah blends the Khomeinist interpretation of Shiism with the IRGC’s proficiency in unconventional warfare. Israel has already fought a pyrrhic open conflict with Hezbollah in 2006 and has since remained in near-war tensions with its neighbour from the north. Throughout the years, Hezbollah has stockpiled short- and medium-range unguided rockets as a deterrence policy against Israel. In 2015, Israeli Intelligence estimated Hezbollah’s rocket stockpile at 150,000 (Issacharoff 2015). Furthermore, Jerusalem likely believed that Iran had transferred sophisticated weaponry such as ballistic missiles and aerial defence systems to Hezbollah under the cover of the Syrian Civil War.

Ever since the beginning of the Syrian Civil War, Israel engaged in a covert action campaign in Syria, tasking its intelligence organizations and air force to neutralize tactical objectives. The Israeli covert action campaign has mostly engaged high-value targets (e.g. weapons, supplies, equipment) airlifted from Iran into Syria. The attacks followed an established pattern. Following target identification and assessment, the IAF scrambles fighter jets to neutralize the HVT, the Israeli jets, mostly outfitted with standoff missiles, then engage the targets from Lebanese airspace, avoiding the engagement range of Syrian air defences. While Syrian air defences sometimes responded with ordnance interception, no attack was ever repelled. While Jerusalem has mostly been secretive about its military activities in Syria, Israeli Intelligence Minister Israel Katz revealed in 2018 that Israeli forces have conducted over 200 strikes in Syria over the past two years (Williams 2018). As Israeli covert raids in Syria proved to be highly effective, Tehran stopped delivering sophisticated missiles and instead provided GPS kits for Hezbollah to convert its existing stockpile of rockets from “dumb” munition to precision-guided missiles (Zilber 2019).

Despite the tight-lip secrecy surrounding the raids, OSINT analysts have repeatedly and methodically shed light on the IAF’s covert activities in Syria. Fusing SOCMINT with open-source GEOINT/IMINT, “intelligence minutemen” have followed air strikes as they happened. By constantly scanning known IRGC logistics nodes, specifically airfields that form the Iranian air LOC (i.e. airbridge) and SAA’s military bases, using GEOINT/IMINT, open-source observers have managed to determine the site and target objective of the Israeli kinetic strikes.

Contrasting with the previous entries, this section of the case study will discuss the covert Israeli involvement in the Syrian Civil War and will focus on a different intelligence product, called Battle Damage Assessment (BDA). While a BDA is a mechanism for measuring the success of an operation by assessing the damage inflicted on an enemy target, OSINT users have used BDAs to back-track kinetic strikes, reverse engineering their operational design. By identifying kinetic targets and estimating the extent of the damage, OSINT users could tell who did it – and to a certain extent, how and why. The following entries show how different aerial engagements on diverse IRGC-related targets were backtracked to the IAF, enabling online users to estimate a myriad of tactical details, such as ammunition type, aircraft and flight path. Moreover, the OSINT research also shed light on the equally shadowy Iranian involvement in Syria and the transfer of advanced weaponry to rogue groups, some of which are designated as terrorist groups. The section chronologically discusses some of the most important IAF raids, with a view to the LSO-based open-source collection efforts around them.

3.4.1. The T4 Air Base Attacks

While the IAF has been combat-applying its counter-Iranian strategy since 2013, the covert confrontation between the two countries swiftly escalated in early 2018. After the IRGC established an intermediate logistics node on the grounds of the SyAAF's T-4 Air Base (AB), Israeli intelligence focused collection efforts on this target. On February 10, 2018, an Iranian-made UAV, launched from T-4 AB, violated Israeli airspace for several kilometres to recon the Israeli Defence Forces' positions in the Golan Heights. Not only was the Iranian UAV destroyed, but the incident also prompted a swift retaliation. The IAF scrambled F-16I Sufa fighter jets, which successfully raided targets in Syria, including the T4 AB (Barrington & Balmforth 2018). While these events were unfolding in complete secrecy, the confrontation was spoiled online, when a Syrian S-200 long-range SAM managed to down one of the Israeli F-16s returning from the sortie.

On April 8, 2018, the IAF targeted the launching point of the Iranian UAV, the T-4 AB. As soon as the Syrian state media complained about unidentified planes attacking its base, social media users shared videos reportedly showing air-launched missiles expanding outside of the city of Palmyra (see for example @BabakTaghvaee 2018b; @QalaatAlMudiq 2018a). Photos surfacing on social media showed a hangar inside the air base shred to pieces by what it looks to be precision munition (@ErshadAlijani 2018). Analysts were quick to name the Israel-made "Delilah" missile cruise as being responsible for the blast and to furthermore link the T-4 AB attack to the February incident (@BabakTaghvaee 2018c). On April 11, Iranian media revealed that seven IRGC members were killed in the attack. Commercial satellite before-and-after imagery showed visible, yet surgical damage to the structures on the airfield grounds (Times of Israel 2018). While Israel never commented on this attack, the evidence was enough to point towards Jerusalem. Unconfirmed information suggested that the IAF targeted and destroyed a short-range Tor-M1 SAM system deployed at the T-4 by the IRGC-Aerospace Forces (Trevithick 2018).

3.4.2. Pre-empting Retaliation

Expecting retaliation for the T-4 raid, Israel prosecuted two IRGC-affiliated targets deep in north-western Syria. In a wave of unclaimed air strikes, logistics depots from the SAA's 47th Brigade base (Hama province) and an industrial site near Aleppo International Airport (Aleppo province) were bombed overnight on April 29, 2018. Again, videos posted online show a large explosion followed by several secondary bursts, indicating that a weapon depot had been struck (@Syrianzo 2018) near Hama. The next day, private satellite imagery provider ISI issued a before and after comparison of the SAA's 47th Brigade base, showing at least ten different structures destroyed (@newsisrael13 2018).

User @markito0171 (2018) geolocated the photos of the Aleppo site, using basic mapping services, with pinpoint accuracy (36°11′18″N, 37°14′25″E). Furthermore, Twitter users matched the missile debris seen in the photos from the Aleppo bombing site with the U.S.-made GBU-39 small diameter bomb (SBD) (see for example @Atlantide4world 2018), narrowing down the list of possible perpetrators to a handful of armed forces, including the IAF. Knowing that the perpetrators had used the GBU-39, another analyst estimated the aircrafts' approaching path, using publicly available data on the SBD's engagement range (@intellipus 2018). Users monitoring ADS-B Exchange also spotted the presence of a USAF RQ-4 Global Hawk UAV airborne for at least nine hours during the unclaimed strike in Hama and Aleppo (see for example @CivMilAir 2018b). This suggested that Washington was informed about the operation and that it possibly provided ISR support to the advancing Israeli jets.

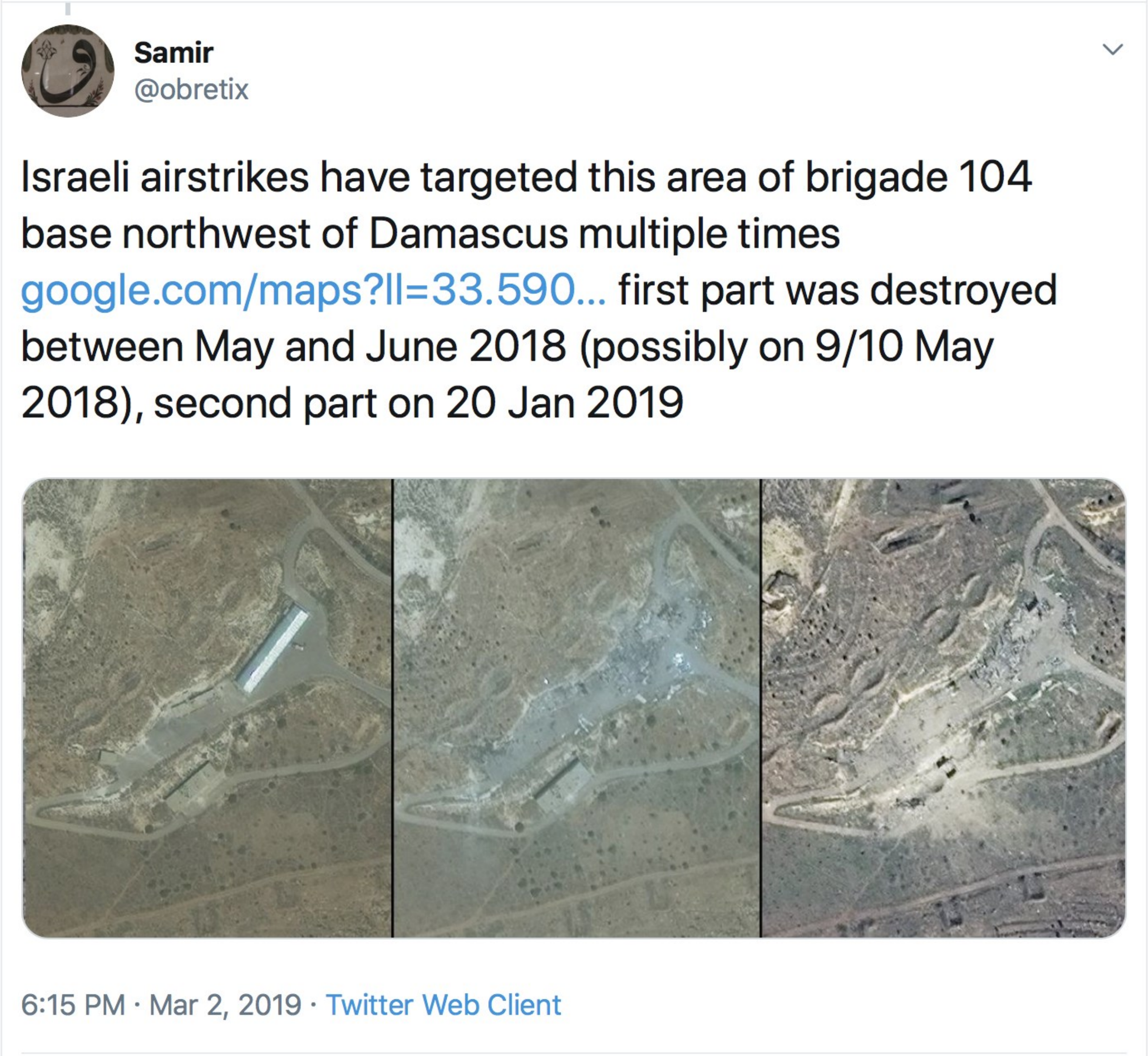
After assessing the likely weapons system used in the strike and the subsequent target location as part of the BDA, OSINT users uncovered the possible target. Users monitoring FlightRadar24 spotted an Il-76T strategic airlifter operated by the SyAAF 585th Transport Squadron flying from Tehran Mehrabad Airport to the Hama military airfield (see for example @YorukIsik 2018d) hours before the alleged strike. Besides naming the IAF as the perpetrator, many have drawn the conclusion that Israel targeted newly shipped weapons systems that the IRGC and its allies were planning to use against Israel in revenge for the T-4 raid from April (see for example HARM 2018d). According to this logic, the capabilities airlifted by the SyAAF Il-76T cargo plane were stored in the SAA military base and in an IRGC covert site as a counter-surveillance tactic.

3.4.3. Operation House of Cards

Despite attempts to pre-empt an Iranian attack on Israel, the IRGC launched a salvo of surface-to-surface missiles (SSM) from Southern Syria to the Golan Heights on May 9, 2018 (Morris 2018). Immediately afterwards, the IAF launched a series of air strikes on SAA and IRGC-Quds Force targets throughout Syria. The Operation, called “House of Cards”, was Israel’s largest military operation in Syria since 1974 (Lahad et al. 2018). The IAF made use of 28 aircraft - mostly the multi-role F-16Is and air superiority F-15Is - and employed hundreds of intelligence officers to assess, exploit, and target objectives in Syria. Operation “House of Cards” had two main mission profiles. The first mission profile was the suppression of enemy air defences (SEAD), focused on the SyAAF’s air defence batteries, while the second was a conventional ground attack campaign targeting the IRGC and affiliated militias.

Like in the previous examples, the operation was thoroughly followed via open-source channels. Twitter users documented all aspects of the operation with a much greater speed than conventional media outlets, beginning with videos showing the Iranian SSM salvo towards Israel (see for example @BabakTaghvaee 2018d) and including the first air raid reports (see for example @QalaatAlMudiq 2018b), retaliation strikes over Damascus (see for example @Dannymakkisyria 2018), and alleged ordnance wreckage (see for example @Syria_Protector 2018). As observed in the case of the trilateral strike against Assad’s CW sites, OSINT observers noticed ISR platforms and aerial tankers with active transponders in the course of the ongoing military operation. As @GDarkconrad (2018e) shared, one IAF KC-707 3J6C tanker and one King Air B200 SIGINT were conducting “donut” rounds over central Israel during Operation House of Cards.

In a very rare move, the Israeli Defence Forces (IDF) made part of their internal BDA public, showing scores of before-and-after target sites to the world. Israeli Defence Minister Avigdor Liberman stated that the IDF destroyed almost all of Iran’s military sites in Syria (Gross 2018). However, even in this case, OSINT users found strike locations undisclosed by the IAF. ISI provided GEOINT on the IRGC headquarters in Syria, located in Damascus International Airport and known as the Glasshouse (Frantzman 2018), while Twitter analysts, using only Google Earth’s history layer, discovered several damaged structures on the SAA's 104th base (@obretix 2018b) and a destroyed S-200 radar (@obretix2018c) near Damascus.



Samir
@obretix

Israeli airstrikes have targeted this area of brigade 104 base northwest of Damascus multiple times google.com/maps?ll=33.590... first part was destroyed between May and June 2018 (possibly on 9/10 May 2018), second part on 20 Jan 2019

6:15 PM · Mar 2, 2019 · Twitter Web Client

Figure 12 Syrian Brigade 104 headquarters after Israeli airstrikes (@obretix2019)

3.4.4.The Christmas Raid

The Israeli-Iranian shadow war in Syria continued throughout the year, with limited escalatory moments. The accidental downing of a RuAF Il-20 on September 17, 2018 halted Israeli air operations in Syria for several months, pending mediation with Russia. However, the IAF resumed operations with a daring raid on December 25, 2018. Following the established pattern, social media users reported anti-air activity over Syria and shared photos of smoke trails and missiles in flight (see for example the entire thread of @aghiad_alkheder 2018). IAF jets likely followed the same strike path via Lebanon and engaged targets in the wider Damascus region, using standoff weaponry. Less than 48 hours after the attack, open-source BDA's emerged (see for example @ImageSatIntl 2018b; @ImageSatIntel 2018c). Satellite imagery showed a storehouse and parking lot destroyed in the SAA's fourth division camp. The sites were believed to be housing Iranian-made Fajr-5 SSMs. OSINT analysts, using Google Earth's measurement tool, determined the diameter of the bomb craters in the parking lot (see for example @yarinah1 2018) and assessed that at least a GBU-39 type of ordnance was used (@Bodheesattva 2018). This indicated that either F-16 or F-15 fighter aircraft of the IAF had delivered the payload.

3.4.5. Missile Exchange over Damascus

The next attack came less than a month later. On January 20, 2019, tourists skiing down the slopes of Mount Hermon filmed and tweeted the launch of several Iron Dome SAM missiles over the Golan Heights (see for example @HillelNeuer 2019). Over night, locals tweeted videos showing missile fire and interceptions over Damascus (see for example @HoseinMortada 2019a; HoseinMortada 2019b; @RisboLensky 2019). It became clear that a new large-scale IAF operation was underway in Syria and that the Syrian forces had mobilized their air defences.

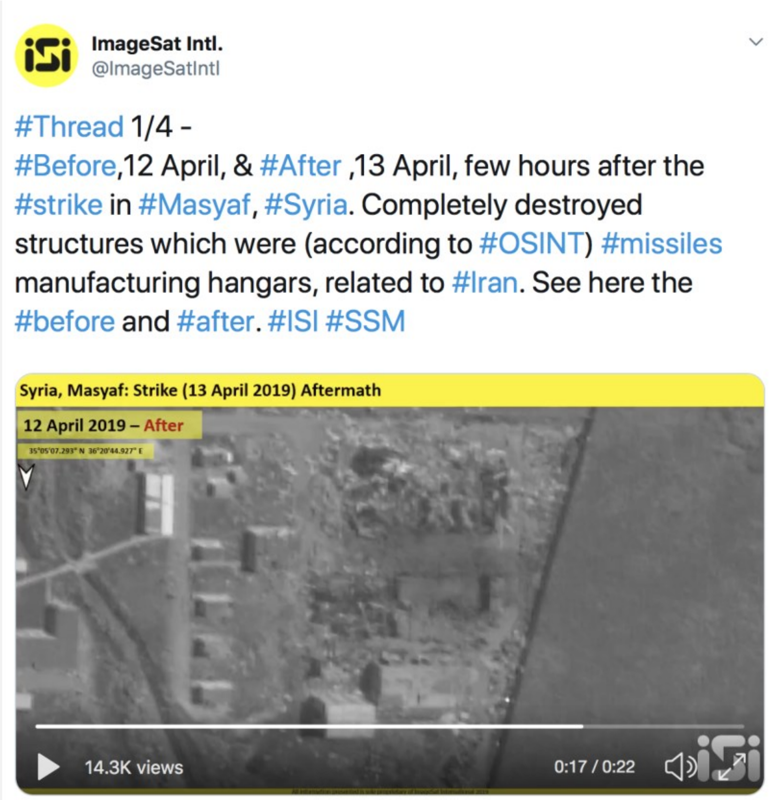
The IDF again showed transparency by sharing a target list on Twitter, featuring photos of Iranian logistical, military, and intelligence sites targeted in the night (@IDF 2019a). Moreover, the IDF showed two videos filmed by their TV missiles, as they glided towards and destroyed two SyAAF aerial defence batteries (@IDF 2019b). OSINT users later determined that the equipment featured was the Russian-made Pantsir S-1/S-2 system. As soon as cloud-free imagery became available on commercial IMINT/GEOINT providers, *T-Intelligence* geolocated one of the Pantsir S-1s destroyed on Damascus International Airport and conducted a BDA showing the before-and-after comparison (@T_intell 2019a). The "usual victim" Damascus International Airport is a key logistics node of the IRGC's air-bridge LOC to Syria and is therefore constantly monitored by OSINT analysts. Other OSINT analysts have pointed out that Israel used a high-end suicide anti-radiation drone, known as IAI Harop to destroy the Syrian air defence batteries (see for example Roblin 2019; @M_S_Alftayeh 2019; HARM 2019b).

3.4.6. Sustained Hostilities in 2019

As the SyAAF was rumoured to have operationalized the Russian-supplied S-300PM2 SAM system, Israel again paused operations over Syria. However, as negotiations between Israeli Prime Minister Netanyahu and Russian President Putin were reportedly fruitful, Twitter users expected an imminent resumption of IAF strikes. User @BabakTaghvaee (2019a) even announced that the resumption would follow the IAF's March exercise. During the night between March 27 and 28, 2019, the IAF raided a target in Aleppo province and social media videos confirmed that an explosion had happened (@BabakTaghvaee 2019b; @babakTaghvaee 2019c). Forensic image analysis of the photos from the bombing site conducted by OSINT analysts suggests that the IAF used a GBU-39 SDB for targeting an industrial park in north-eastern Aleppo (@Obs_IL 2019a). The relative geolocation was validated as soon as commercial satellite imagery became available for BDA. The OSINT BDA shows two structures (a large building and a hangar) "surgically" bombed in Aleppo's Sheik Najjar Industrial Area (see for example @AmichaiStein1 2019; @ImageSatIntl 2019d). The press later reported that the structures covertly targeted by Israel were Iranian ammunition storage depots (Times of Israel 2019).

The next air raid followed swiftly in the next month. Hoping to deter Israeli adventurism, the IRGC withdrew its military capabilities and logistical nodes to Hama, Homs and Aleppo province. North-western Syria falls under the engagement range of Russia's long-range SAM systems and of the new S-300PM2 supplied to the SyAAF. However, the IAF continued to prosecute HVT all over Syria. On the night between March 12 and 13, reports of SAM fire in response to Israeli aerial incursions over Hama province emerged again (see for example @ELINTNews 2019; @no_itsmyturn 2019; @auroraintel 2019). Several Iranian-affiliated sites were photographed under fire and shared online (@Step_Agency 2019). In a thread tweeted by @Syrian_MC (2019), the user claims that Israeli F-16s flew in from southern Beirut at high altitude to mimic an ISR sortie and then egressed at full speed towards Syria to launch SDBs at several targets (a warehouse north of Masyaf and a warehouse west of Homs).

The OSINT community was either working on BDAs or waiting for updated, cloud-free satellite images to surface on social media. @ImageSatIntl (2019c) tweeted a four-part BDA thread detailing the Masyaf target, a complex of five to eight destroyed buildings. The complex was believed to be a missile manufacturing base. Augmenting the ISI thread, account @T_Intell (2019b) issued a BDA of the second target, a building in Umm Haratim located just west of Homs city, fully validating the target claims made by @Syrian_MC. The building was suspected to be logistics depot for military hardware unloaded from the near-by T-4 AB (Homs province).

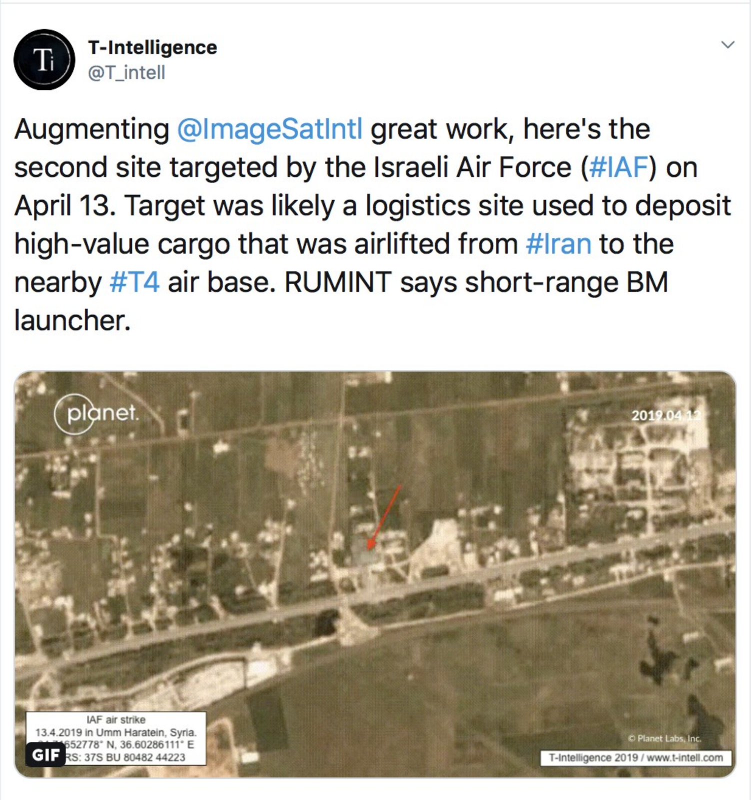


ImageSat Intl.
@ImageSatIntl

#Thread 1/4 -
#Before,12 April, & #After ,13 April, few hours after the #strike in #Masyaf, #Syria. Completely destroyed structures which were (according to #OSINT) #missiles manufacturing hangars, related to #Iran. See here the #before and #after. #ISI #SSM

Syria, Masyaf: Strike (13 April 2019) Aftermath
12 April 2019 – After
35°05'07.293" N 36°20'44.927" E
14.3K views
0:17 / 0:22

Figure 14 First target of the IAF's 2019 strike in Masyaf (@ImageSatIntl 2019c)

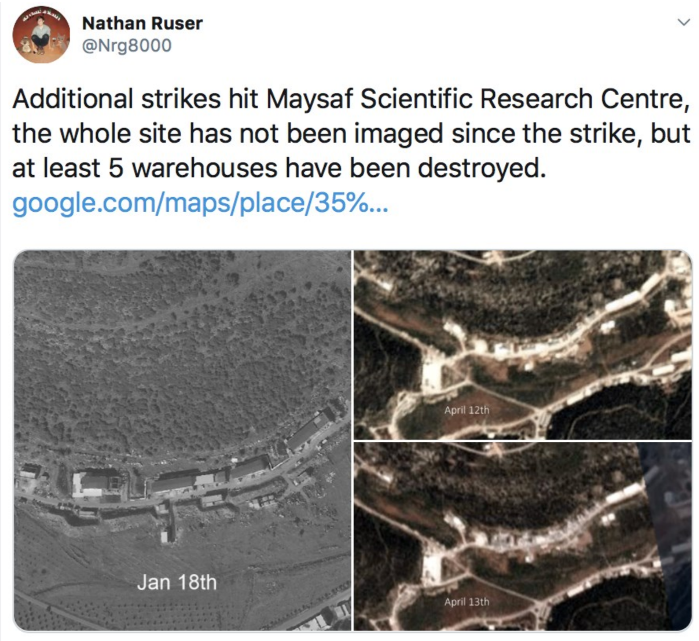


T-Intelligence
@T_intell

Augmenting @ImageSatIntl great work, here's the second site targeted by the Israeli Air Force (#IAF) on April 13. Target was likely a logistics site used to deposit high-value cargo that was airlifted from #Iran to the nearby #T4 air base. RUMINT says short-range BM launcher.

planet.
2019.04.12
IAF air strike
13.4.2019 in Umm Haratein, Syria.
652778° N, 36.60286111° E
RS: 37S BU 80482 44223
GIF
© Planet Labs, Inc.
T-Intelligence 2019 / www.t-intell.com

Figure 13 Second target of the IAF's 2019 strike in Masyaf (@T_Intell 2019b)

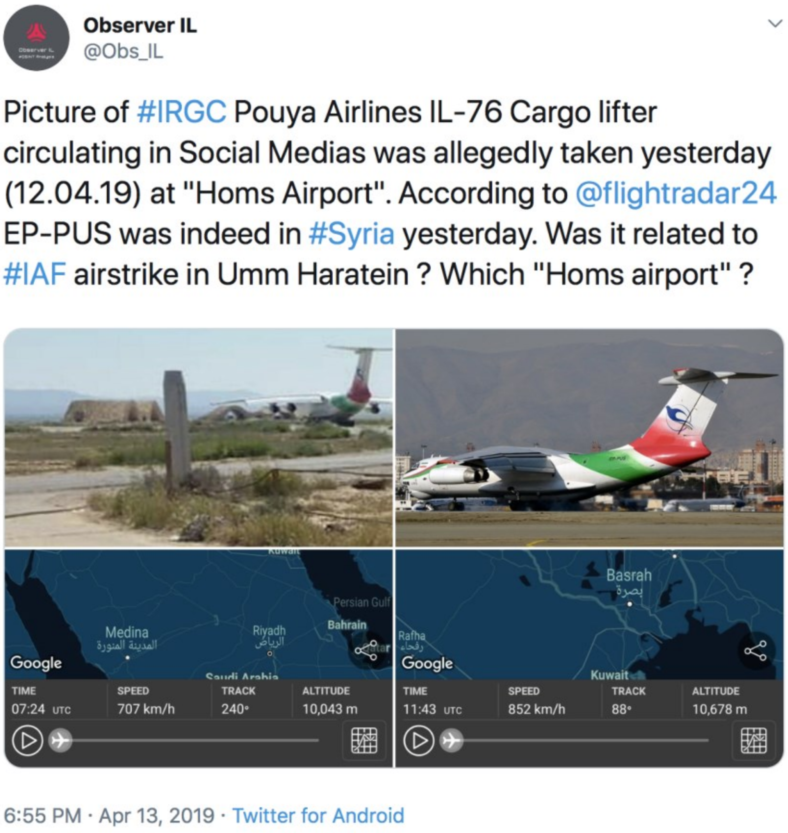


Nathan Ruser
@Nrg8000

Additional strikes hit Maysaf Scientific Research Centre, the whole site has not been imaged since the strike, but at least 5 warehouses have been destroyed. google.com/maps/place/35%...

Figure 15 Third target of the IAF's 2019 strike in Masyaf (@Nrg8000 2019)

Coincidental or not, @Obs_IL (2019b) discovered via FlightRadar24 that an IRGC-owned (Pouya Airlines) Il-76 cargo plane landed on “Homs Airport” (T-4 AB is the only airfield in Homs province) on April 12, 2019 – just hours before the IAF attack. It is likely that the Il-76 flight was airlifting an HVT, which was later deposited in the Umm Haratim building.



Observer IL
@Obs_IL

Picture of #IRGC Pouya Airlines IL-76 Cargo lifter circulating in Social Medias was allegedly taken yesterday (12.04.19) at "Homs Airport". According to @flightradar24 EP-PUS was indeed in #Syria yesterday. Was it related to #IAF airstrike in Umm Haratein ? Which "Homs airport" ?

TIME	SPEED	TRACK	ALTITUDE
07:24 UTC	707 km/h	240°	10,043 m

TIME	SPEED	TRACK	ALTITUDE
11:43 UTC	852 km/h	88°	10,678 m

6:55 PM · Apr 13, 2019 · Twitter for Android

Figure 16 HVT package airlifted by IRGC Il-76 plane in Syria (@Obs_IL 2019b)

In addition, using imagery from PlanetLabs, user @Nrg8000 (2019) tweeted a BDA of a third target, the Masyaf Scientific Research Centre. IMINT/GEOINT showed that at least five buildings of the expansive complex “disappeared” between 12 and 13 April, 2019. This represents one of the fastest BDA efforts spearheaded by the OSINT community. Twitter users identified and scouted the SOCMINT-reported strike locations in less than 48 hours after the IAF operation. In addition to the building-by-building, site-by-site in-depth BDAs, OSINT analysts also assessed that this operation was likely conducted by more assets than just two F-16s. Furthermore, since this strike was less than 20 kilometres from the S-300PM2 in the Masyaf hills, OSINT analysts concluded that the use of the long-range SAM system is politically conditioned on Russian approval. This inherently suggests that the Russian-Israeli agreement over Syria trumps Moscow’s loose alliance with Iran. OSINT efforts have not only revealed tactical military developments between Israel and Iran, but also shed light on strategic geopolitical aspects of the Syrian Civil War.

As demonstrated throughout this section of the case study, OSINT analysts have tracked both Iranian and Israeli military logistics to monitor the shadow-war between the two actors. For monitoring Iran, the OSINT community periodically scanned the IRGC's primary LOC (i.e. the airbridge) and its logistics nods (e.g. Damascus International Airport, Mezzeh Airfield, T-4 AB, Aleppo International Airport etc.) for suspicious activity. Regarding Israel, the IAF's ISR platforms, tankers, and expanded munition perpetually indicated air strike preparation or the action itself. Forensic media analysis followed by GEOINT/ IMINT tools enabled the analysts to geolocate and later assess the damage of the IAF strike and to furthermore guess the assets employed in the attack.

3.5. Evaluation and Discussion: Challenges, Limitations and Opportunities

As the above case study demonstrated, OSINT analysts have been successful in producing three different types of intelligence analytical products, looking at different geographical and operational areas of the Syrian Civil War. These results affect an in-depth and methodical understanding on how military logistics, particularly send-type LSOs, are exposed to open-source collectors. The chain reaction leading to OPSEC degradation from initial LSO exposure is swift and worrisome for decision-makers, as it has the capacity to reveal more than just an ongoing military operation or deployment. As particularly shown by the Russian example, once acquired by OSINT analysts, the targeted data remains on the world wide web for further exploitation. The mass proliferation of OSINT tools due to the growing availability of sophisticated software and the enriching knowledge pool on varying topics such as military hardware will further render LSOs vulnerable. While OSINT acquisition has become easier than before, there have been limitations in compiling and assessing the above case study. The vast data sets available online, the proliferation of fake information, retroactive research, and linguistical bubbles have been some of the main limitations of the case study.

The OSINT "white noise" is real. The amount of open source information and chatter available online is overwhelming. This research has repeatedly stumbled on a "looking for a needle in a needle stack" dilemma, while surfing through the target-rich environment of social media. There is simply too much content available on a given topic for easy acquisition. In many cases, the bulk of data was irrelevant to the research objective, becoming a time-consuming obstacle. In other cases, the surplus data permanently covered the desired piece of information. This issue repeatedly surfaced, when conducting retrospective research. Most of the case study information, in particularly from social media, was published between 2015 and 2018, yet the collection for this research was mostly conducted in 2019. Twitter and other social media are challenging for retrospective collection, especially on information dense topics such as the Syrian Civil War. However, this does not limit the scope of this research, as the case study's purpose is to provide "snapshots" of OSINF that facilitated OSINT on a given topic in a given timeframe. Recreating an information environment in its entirely would have overstretched the scope of this research.

The open-source coverage of the Syrian Civil War is incredibly polarized, in particular on social media channels. Being a disinformation-rich environment, social media mass-proliferates fake news and rumours. Especially in this case, Twitter has turned into a battling ground between propagandists and "fan-boys" of the diverse factions engaged in the war. In most cases, propagandists are easy to spot based on their social media content (producing or retweeting content favourable to his/her camp) and behaviour (positive interaction with peers, hostile to individuals outside his/her echo-chamber). Propagandists are regularly open about their allegiance, yet the most effective ones are those engaged in deception. Nonetheless, this does not disqualify them as a legitimate OSINT collection target. In many cases, propagandist Twitter accounts have been the source of exclusive content related to their supported faction. It should also not be discredited that governments can and are often times actively involved in the information battle sphere. By spreading deceptive information, governmental intelligence agencies can direct OSINT analysts on the wrong path or "influence the influencer" for their own tactical interests.

The issue of rumours and unsubstantial claims has no easy fix. This required the researcher's analytical abilities to separate "the good from the bad." A method of coping with the amount of disinformation/fake news on the world wide web was ironically provided by one of the previously named challenges, retrospective research. Looking through the present lens at past social media chatter, the researcher could filter out false information based on what came true and what did not. This procedure worked best for predictions and claims of imminent military aggressions. Using critical thinking and background knowledge, some information was easier to discard that the other. In other situation, there was no telling.

As addressed in the theoretical framework, the linguistical factor remains an undeniably major issue in all phases of the intelligence cycle – obvert and covert. The vast majority of the case study's data is based on English language content. While many sources are direct translations and aggregations of native, local-language speaking sources, this is not the complete picture of the OSINT chatter and information environment surrounding the events discussed. However, this does not defy the aim of the thesis, since this is an overview aimed at demonstrating how OSINT collection on LSOs works.

4. Conclusion

This research aims to foster understanding among decision makers regarding the OSINT capacity to track, fix, follow, and compromise sensitive military activities based on their logistical footprint. As outlined in the theoretical framework, OSINT has pros and cons. However, the consensus among scholars, practitioners and analysts is that this form of obvert intelligence will unavoidably proliferate and refine. The open-source equivalents of HUMINT, IMINT/GEOINT and SIGINT are undeniably practical, as the growing OSINT community online has proven to be resourceful and computer-savvy. Furthermore, as identified, the link between OSINT analysis and military logistics is unexplored in the existent literature. This is both an opportunity and a disadvantage in bridging the understanding between the two topics of intelligence and strategic studies.

As shown, military logistics and send type LSOs are particularly vulnerable to OSINT acquisition. The events presented in the case study have demonstrated how the fusion between the myriad of open-source tools existent and known line-of-communications (LOCs), assets, and logistics nodes used by armed forces can lead to the exposure of operations security (OPSEC) and furthermore to declassifying other secrets such as the presence of sensitive defence hardware, military action, or preparations for such. The first focal point of the case study has outlined how intelligence minutemen have estimated Russia's order of battle in Syria by tracking their air and naval LOCs and periodically scanning the inventory of Russian assets deployed to the logistics nodes. The second focal point showed how similar LSO activity spoiled the preparations for a joint multinational American-British-French strike against the Syrian government in western Syria and allowed the OSINT community to forecast most details of the impeding action. The third and final point focused on the covert Israeli-Iranian confrontation in Syria. This section further demonstrated how open-sources can facilitate the most diverse intelligence products, including battle damage assessments, by fusing SOCMINT and GEOINT/IMINT, and how resourceful OSINT analysts used this type of assessment to determine who did what, using which asset, how, and why.

Since the aim of this dissertation is to foster a better understanding of OSINT for decision makers, this study focused on one case study. Further research is required to determine how OSINT works or has worked in different cases and whether there are environmental factors that determine the success of open-source investigations, specifically tailored to target the flow of military assets and logistics. In regard to the practical utility of this research, decision-makers including policymakers, logistician heads, and military field commanders, should take appropriate measures to minimize the risk of OPSEC exposure to OSINT collection. The first and most important step is to acknowledge the changing informational environment and the inherent consequences on modern war and covert/sensitive actions. As social media channels and open-source tools are becoming more accessible and more widely used, a wider discussion within the defence community on how OSINT affects day-to-day combat operations is required. The subsequent conclusions should affect changes in doctrinal texts and tactical applications. Although the LSO-OSINT nexus is an OPSEC-vulnerability, it should be remembered, that in some instances, OSINT can act as a force multiplier for intelligence collection and analysis. For a masterful and adapted leader, commander or decision-maker, OSINT should only and always be a force multiplier and not a liability.

Bibliography

“Are There Russian Troops Fighting in Syria?” 2015. Bellingcat. September 7, 2015. https://www.bellingcat.com/news/mena/2015/09/07/are-there-russian-troops-fighting-in-syria/.

“Dreamliner on Twitter: ‘@Alexfly35 а Вот и Фото Http://T.Co/Im9g61e3S4’ / Twitter.” n.d. Twitter. Accessed May 23, 2019. https://twitter.com/capach28/status/647859925964689408.

“Russia Deploys Cutting-Edge S-400 Air Defense System to Syrian Base after Su-24 Downing.” n.d. RT International. Accessed May 23, 2019. https://www.rt.com/news/323596-s400-russia-syria-airbase-turkey/.

“Russia Deploys Missile Cruiser off Syria Coast, Ordered to Destroy Any Target Posing Danger.” n.d. RT International. Accessed May 23, 2019. https://www.rt.com/news/323329-russia-suspend-military-turkey/.

“Russian MoD Confirms Use of Iskander-M SRBM in Syria.” 2018. Missile Threat. December 18, 2018. https://missilethreat.csis.org/russian-mod-confirms-use-of-iskander-m-srbm-in-syria/.

“Second Russian S-400 in Syria Confirmed | Jane’s 360.” 2017. October 2, 2017. https://web.archive.org/web/20171002012653/http://www.janes.com/article/74500/second-russian-s-400-in-syria-confirmed.

@aghiad_alkheder. 2018. “Local Sources Report That the Air Defense System Are Engage Targets over South Syria and #Damascus #Syria.” [Twitter]. Accessed May 28, 2019. https://twitter.com/aghiad_alkheder/status/1077656109459165185.

@ain92ru. 2015. “@LuftwaffeAS Wait for Su-34 Fullbacks, They Were Flying over Mozdok on Sep 26.” [Twitter]. Accessed May 20, 2019. https://twitter.com/ain92ru/status/648272118300442625.

@AircraftSpots. 2018a. “US Navy P-8A 168439 PS246 Is Operating Low-Level over the Eastern Mediterranean - West of Tartus, Syria.” [Twitter]. Accessed May 24, 2019. https://twitter.com/AircraftSpots/status/984108681926139904.

@AircraftSpots. 2018b. “15 Hours after Departure from NAS Sigonella - FORTE10 Continues to Carry out It’s Task in the Eastern Mediterranean West of Lebanon & Syria at 56,000 Feet.” [Twitter]. Accessed May 24, 2019. https://twitter.com/AircraftSpots/status/984879346916601857.

@AircraftSpots. 2018c. “USAF RC-135V 64-14846 FIXX74 Departed Souda Bay - On Task over the Eastern Mediterranean North of Egypt.” [Twitter]. Accessed May 24, 2019. https://twitter.com/AircraftSpots/status/984970672475484162.

@AircraftSpots. 2018d. “USAF RQ-4B 11-2047 FORTE11 Departed Sigonella at 2335z - On Task West of Lebanon & Syria Likely Conducting a Post Battle Damage Assessment Task.” [Twitter]. Accessed May 24, 2019. https://twitter.com/AircraftSpots/status/985069281829314560.

@AmichaiStein. 2019. “Syria: @ImageSatIntl Publishes Pictures of the Attack Attributed to Israel in Aleppo on 27 March.” [Twitter]. Accessed May 28, 2019. https://twitter.com/AmichaiStein1/status/1113732417154686978.

@Atlantide4world. 2018. “#Siria: L’attacco al Deposito Di #Aleppo è Stato Compiuto Con Bombe Guidate Di Precisione GBU-39 Giá Usate Da #Israele Nell’attacco Alla Base T4.Tuttavia Anche i Jets #Usa Le Utilizzano.” [Twitter]. Accessed May 27, 2019. https://twitter.com/Atlantide4world/status/990909973654917120.

@AuroraIntel. 2019. “Video from #Syria, Fighter Jets Can Be Heard Overhead. Reports Indicate That #Israel Carried out a Strike against #Iran|ian Targets in Syria.” [Twitter]. Accessed May 28, 2019. https://twitter.com/AuroraIntel/status/1116862756383277056.

@avischarf. 2018. “‘Update: Sixth Russian Heavy Lift AN-124 Arriving Latakia, Syria in 4 Days. RA-82035 via Caspian, Iran, Iraq #S300 ? #Syria” [Twitter]. Accessed May 24, 2019. https://twitter.com/avischarf/status/1046859759389954048.

@BabakTaghvaee. 2018. “Earlier I Reported about Flights of #RuAF’s Fighter Jets over #Syria|n Shoreline, #Tartus & Eastern #MediterraneanSea on Sunday 8th April 2018. These Are the Airplanes Flew in Low Altitude Close to French Navy #MarineNationale Aquitaine Frigate D650.” [Twitter]. Accessed May 24, 2019. https://twitter.com/BabakTaghvaee/status/983720713726152704.

@BabakTaghvaee. 2018b. “The Moment at-Least 20 Delilah Cruise Missiles Launched by #Israel Air Force F-16Is &amp; F-15Is Hit Various Targets in #Tiyas / T4 AB of #Syria|n Arab Air Force in #Homs in Early Hours of 09/04/2018. #Syria|n Army Was on High Alert & They Have Shot down Eight Other Dalilah Missiles.” [Twitter]. Accessed May 27, 2019. https://twitter.com/BabakTaghvaee/status/983250239917363200.

@BabakTaghvaee. 2018c. “T4 / #Tiyas AB’s Maintenance Hangars Which Were Targeted by Dalilah Cruise Missiles Launched by #Israel Air Force’s F-15Is on

09/04/2018. One Was Still in Use for Repair of Su-24MK2s of #Syria Air Force’s 819th Fighter Sq While the Other Was Occupied by #IRGC Air & Space Force.” [Twitter]. Accessed May 27, 2019. https://twitter.com/BabakTaghvaee/status/983830599122194432.

@BabakTaghvaee. 2018d. “BREAKING: These Rockets Were Launched by #IRGC Qods Force at #IDF Positions in #GolanHeights from #Damascus Suburbs, #Syria. This Site Is Now Destroyed by Dalilah Cruise Missiles Launched by #Israel Air Force (#IAF) F-16Is Now.” [Twitter]. Accessed May 27, 2019. https://twitter.com/BabakTaghvaee/status/994363105474990080.

@BabakTaghvaee. 2019a. “BREAKING: #Israel PM #Netanyahu Has Received Green Light of #Russia’s President #Putin to Resume Airstrikes against #IRGC &amp; #Hezbollah Targets in #Syria as Well as a New Weapon Factory Which Produces Rockets for Syrian Arab Army Most Probably in March after the #IAF’s Exercise.” [Twitter]. Accessed May 28, 2019. https://twitter.com/BabakTaghvaee/status/1100755174774263808.

@BabakTaghvaee. 2019b. ‘#BREAKING: #Israel Air Force Carried-out an Airstrike against a Rocket Manufacturing Workshop at Sheikh Najar Industrial Zone, near the #Aleppo International Airport. It Is Reported That #IRGC Was Producing Fajr-5C Precision Guided Rockets for #Syria Arab Army There.” [Twitter]. Accessed May 28, 2019. https://twitter.com/BabakTaghvaee/status/1111031615944302592.

@BabakTaghvaee. 2019c: “#BREAKING: This Is the Latest Video Showing Aftermath of the #Israel Airstrike at the Weapon Workshop in Sheikh Najar Industrial Zone Located in Northeast of the #Aleppo International Airport. The Rockets in Can Be Heard Exploding Due to Fire!” [Twitter]. Accessed May 28, 2019. https://twitter.com/BabakTaghvaee/status/1111033387693891584.

@bdrhmnhrk. 2015. “#Russia’n Soldiers in #Syria.” [Twitter]. Accessed May 22, 2019. https://twitter.com/bdrhmnhrk/status/640088105282895872.

@Bodheesattva. 2018. “@yarinah1 @ImageSatIntl Thx! And the Ground Is Paved. That Means Something Bigger than GBU-39 from Ru MoD Statement.” [Twitter]. Accessed May 28, 2019. https://twitter.com/Bodheesattva/status/1078274374464167936.

@Buzz6868. 2018. “UPDATE 2: 13 Tankers Now up This Morning QUID290+291 KC-135’s Abeam Lyon QUID292+295 Sicily QUID21 Adriatic QUID282+283 +QUID11 Southern Italy QUID288/289/290 KC-10’s near Cyprus & FAF4018/4042

@planesonthenet @KalteMalte53 @ItaMilRadar @Andy007_SR_A @Su39frogfoot @cencio4.” [Twitter]. Accessed May 24, 2019. https://twitter.com/Buzz6868/status/985033590466580481.

@Capt_Navy. 2018. “Now in Med Sea: CG Marshal Ustinov DDG Severomorsk DDG Yaroslav Mudryy FFG Admiral Grigorovich FFG Admiral Essen FFL Pytlivyy FSG Vyshniy Volochek FSG Grad Sviyazhsk FSG Velikiy Ustyug LST Orsk LST Nikolay Fil’chenkov MS Turbinist MS Valentin Pikul SS Kolpino SS Velikiy Novgorod.” [Twitter]. Accessed May 23, 2019. https://twitter.com/Capt_Navy/status/1033347451279876096.

@cencio4. 2018. “A Quick Photoshop Work Just to Have a Rough Idea of the Area Potentially Covered by the Global Hawk Using a EO/IR Sensor Suite Range of 200km (According to Some Sources, at +53K Ft the Range Should Be 250-300km). The Area Surveilled Is Not Circular: +/- 45° Field of Regard (FOR).” [Twitter]. Accessed May 24, 2019. https://twitter.com/cencio4/status/984932306027720707.

@CivMilAir. 2018. “#NOTAM Navigation Warnings in Force around Cyprus for Thu 12th April ‘RUSSIAN NAVY EXERCISE’ off the #Syria Coast - Surface to 66,000ft.” [Twitter]. Accessed May 24, 2019. https://twitter.com/CivMilAir/status/984187237045764096.

@CivMilAir. 2018b. “UAVGH000” - 51,000ft over the Eastern Med, Tracking off the Coast of Lebanon US Air Force RQ-4 Global Hawk 10-2043.” [Twitter]. Accessed May 27, 2019. https://twitter.com/CivMilAir/status/990129026688798720.

@Dannymakkisyria. 2018. “Breaking - Video of #Damascus Skyline Just Now, Air Defenses Firing, Reports of Possible Israeli Strikes.” [Twitter]. Accessed May 27, 2019. https://twitter.com/Dannymakkisyria/status/994365630915719168.

@ELINTNews. 2019. “BREAKING: First Video Shows Israeli Warplane Racing over the Skies near the Syrian-Lebanese Border as Reports of Israeli Airstrikes Emerge near Maysaf.” [Twitter]. Accessed May 28, 2019. https://twitter.com/ELINTNews/status/1116859536546119680.

@EmbassyofRussia. 2018. “Russian Defence Ministry Shares First Photos and Video Footage of the Russian S-300 Air Defence Systems Arriving in #Syria. Its Purpose Is to Help Keep Syrian Skies Safe.” [Twitter]. Accessed May 24, 2019. https://twitter.com/EmbassyofRussia/status/1047347965000597505.

@ErshadAlijani. 2018. “First Images of #T4Airbase [#Tiyas Military Airbase] in #Syria after Missile Attack.” [Twitter]. Accessed May 27, 2019. https://twitter.com/ErshadAlijani/status/983977179502530560.

@galandecZP. 2015. “Записки Охотника on Twitter: ‘Новое Фото Аэродрома Латакия 4 x Cy-30,12 x Cy-25,12 x Cy-24 #Syria #SyriaCrisis #Russia.” [Twitter]. Accessed May 23, 2019. https://twitter.com/galandecZP/status/646371967403229184.

@GDarkconrad. 2018a. “US Navy P8 Poseidon 168858 Patrolling Eastern Mediterranean.” [Twitter]. Accessed May 23, 2019. https://twitter.com/GDarkconrad/status/1039825004542734337.

@GDarkconrad. 2018b. “US Navy EP-3E Aries II 157326 Patrolling Eastern Mediterranean.” [Twitter]. Accessed May 23, 2019. https://twitter.com/GDarkconrad/status/1039478643062390784.

@GDarkconrad. 2018c. “Manu Gómez on Twitter: ‘US Navy P8 Poseidon 168431 off the Coast of Lebanon 168439 Departed Sigonella. #Syria.” [Twitter]. Accessed May 24, 2019. https://twitter.com/GDarkconrad/status/984506457684172801.

@GDarkconrad. 2018d. “@cencio4 Currently Taking a Narrow View.” [Twitter]. Accessed May 24, 2019. https://twitter.com/GDarkconrad/status/984934350541279232.

@GDarkconrad. 2018e. “IAF KC-707 3J6C Tanker and King Air B200 Zufit Active over #Israel.” [Twitter]. Accessed May 27, 2019. https://twitter.com/GDarkconrad/status/994287726714335235.

@green_lemonnn. 2015. “Syria Russia to Open a New Military Base in Syria. Russian IL-76 Landed in Lattakia via @MashreghNews” [Twitter]. Accessed May 22, 2019. https://twitter.com/green_lemonnn/status/634670814965665792.

@hdevreij. 2018. “Shaping the Battlefield... Five US Air Force KC-135 Stratotankers (Refueling Aircraft) Currently Flying from the UK, Now over France in the Direction of the Mediterranean. Two KDC-10’s Reportedly in the Western Mediterranean, Flying East towards Syria.” [Twitter]. Accessed May 24, 2019. https://twitter.com/hdevreij/status/984047557625221121.

@HillelNeuer. 2019. “Thousands of Israelis Skiing down the Slopes of Mount Hermon Today in the Golan Heights Suddenly Saw in Front of Them an Iron Dome Air Defense Missile Launch toward the Sky to Take out an Incoming Syrian Rocket

Attack. Here in Switzerland, This Has yet to Happen.” [Twitter]. Accessed May 28, 2019. https://twitter.com/HillelNeuer/status/1087093984894300160.

@HoseinMortada. 2019a. “#حسين_مرتضى الدفاعات الجوية السورية تطلق عددا من الصواريخ بأتجاه اجسام في سماء دمشق” [Twitter]. Accessed May 28, 2019. https://twitter.com/HoseinMortada/status/1087128201237803008.

@HoseinMortada. 2019b. “#حسين_مرتضى هكذا شجع طلاب السكن الجامعي في دمشق منتخب الدفاعات الجوية ليل امس عندما تصدى للعدوان الصهيوني” [Twitter]. Accessed May 28, 2019. https://twitter.com/HoseinMortada/status/1087347663928995840.

@IDF. 2019a. “These Are the Iranian Quds Military Sites in Syria That We Targeted in Response: Munition Storage Sites Military Site Located in the Damascus International Airport Iranian Intelligence Site Iranian Military Training Camp.” [Twitter]. Accessed May 28, 2019. https://twitter.com/IDF/status/1087208743018917888.

@IDF. 2019b. “During Our Strike, Dozens of Syrian Surface-to-Air Missiles Were Launched, despite Clear Warnings to Avoid Such Fire. In Response, We Also Targeted Several of the Syrian Armed Forces’’ Aerial Defense Batteries.” [Twitter]. Accessed May 28, 2019. https://twitter.com/IDF/status/1087208824182919168.

@ImageSatIntl. 2018b. “Fresh from #ISI Oven: An Image Took from Our #satellite Few Minutes Ago Reveals Four #bomb Craters in a #military Vehicle Parking Lot, within the 4th Division #camp, West to #Damascus. #Folloup #snaptasking.” [Twitter]. Accessed May 28, 2019. https://twitter.com/ImageSatIntl/status/1078262818535890948.

@ImageSatIntl. 2018c. “#BREAKING: The #attacked (25 December 2018) Site in the #Syrian 4th Division Camp Is Completely #destroyed. According to Media Reports, It Was an Iranian #Fajr-5 Rockets Storehouse, Located in an #Iranian Base, Only 40 Km from the Border with #Israel.” [Twitter]. Accessed May 28, 2019. https://twitter.com/ImageSatIntl/status/1078243920767844352.

@ImageSatIntl. 2019a. “Syria’s S-300 Exposed, Three Launchers Are Erected. Will It Be Activated? #ISI #Syria #Russia.” [Twitter]. Accessed May 24, 2019. https://twitter.com/ImageSatIntl/status/1092846663646040064.

@ImageSatIntl. 2019b. “#NOW: an #SS26 #Iskander #SSM practice in #Hmeimim, the #Russian airbase in #Syria. #SnapTasking and high-revisit advantage.” [Twitter]. Accessed May 24, 2019. https://twitter.com/ImageSatIntl/status/1118505688882458625/photo/1.

@ImageSatIntl. 2019c. “#Thread 1/4 - #Before,12 April, &amp; #After ,13 April, Few Hours after the #strike in #Masyaf, #Syria. Completely Destroyed Structures Which Were (According to #OSINT) #missiles Manufacturing Hangars, Related to #Iran. See Here the #before and #after. #ISI #SSM” [Twitter]. Accessed May 28, 2019. https://twitter.com/ImageSatIntl/status/1117473176005545984.

@ImageSatIntl. 2019d. “3/5 - The Bombed #Building - 70x35 Meters, Located 450 Meters West to the #bombed Hangar. #ISI #Syria #Aleppo #BDA.” [Twitter]. Accessed May 28, 2019. https://twitter.com/ImageSatIntl/status/1113767239117885440.

@intellipus. 2018. “IAF Uses Delilah Missiles and GBU-39 SDBs as Standoff Weapons for Striking Targets in Syria. Using Publicly Available Ranges, This Is What the Target Release Ranges for Both Types Look like for Aleppo and Tiyas Airbase. Unsure of What Release Altitude They Are Actually Using.” [Twitter]. Accessed May 27, 2019. https://twitter.com/intellipus/status/1111030696255127552.

@JosephHDempsey. 2015. “Unverified #Syria Imagery Assessed to Show #Russia Kh-101 Low-Observable Cruise Missile Wreckage.” [Twitter]. Accessed May 23, 2019. https://twitter.com/JosephHDempsey/status/666671216569241601.

@JulianRoepcke. 2015. “#News #Putin and #Assad = Brothers in Arms. #Russia Sends BTR-82A and GAZ Tigr to the Butcher of #Syria. W Reaction?!” [Twitter]. Accessed May 22, 2019. https://twitter.com/JulianRoepcke/status/635541972711833600.

@LuftwaffeAS. 2015a. “@ain92ru @pfc_joker @oryxspioenkop They Arrived!” [Twitter]. Accessed May 23, 2019. https://twitter.com/LuftwaffeAS/status/648555699727826944.

@LuftwaffeAS. 2015b. “Said to Be an Airliner/Transporter Accompanied with 6 Fighters Crossing over Hama Country Side”. [Twitter]. Accessed May 23, 2019. https://twitter.com/LuftwaffeAS/status/648557345543356416.

@M_S_Alftayeh. 2019. “This Time #Israel Destroyed a Modernized Version of the #Pantsir, the S-2 Version. In May 2018, It Destroyed the Older S-1 Version. It’s Very Likely That Israel Used the IAI Harop Loitering Munition. Just like the Last Attack, the Pantsir Wasn’t Operational &amp; Reloading.” [Twitter]. Accessed May 28, 2019. https://twitter.com/M_S_Alftayeh/status/1087290992993189889.

@markito0171. 2018. “#Syria Pics from Alleged #Israel’i Airstrikes on #Aleppo’s Malikiyah Industrial Area near Airport.” [Twitter]. Accessed May 27, 2019. https://twitter.com/markito0171/status/990874386453487617.

@MIL_Radar. 2019. “1208z: RuAF Tu-160s Now Heading North West Heading 320 Degrees.” [Twitter post]. Accessed May 7, 2019. https://twitter.com/MIL_Radar/status/1113413615925780480.

@moscow_ghost. 2015. “S-400 Triumph Battery Acquisition Radar 96L6 at #Russia-n Air Force #Latakia Air Base #Syria via @2Rook14.” [Twitter]. Accessed May 23, 2019. https://twitter.com/moscow_ghost/status/664822101614985217.

@newsisrael13. 2018. “‘התקיפה בסוריה: תמונות לווין של בסיס חטיבה 47 שהותקף @alonbd צילום: אימג׳סאט.” [Twitter]. Accessed May 27, 2019. https://twitter.com/newsisrael13/status/990989391752499200.

@no_itsmyturn. 2019. “Unconfirmed: #IAF Warplanes Are Striking at Masyaf (Hama,Syria).” [Twitter]. Accessed May 28, 2019. https://twitter.com/no_itsmyturn/status/1116852477792542721.

@Nrg8000. 2019. “Additional Strikes Hit Maysaf Scientific Research Centre, the Whole Site Has Not Been Imaged since the Strike, but at Least 5 Warehouses Have Been Destroyed.” [Twitter]. Accessed May 28, 2019. https://twitter.com/Nrg8000/status/1117380277498593283.

@obretix. 2018a. “Russian Air Force at Hmeymim Airbase in Latakia with 8 Su-24, 4 Su-34 and 4 Su-35 on 29 Aug 2018. an A-50, 2 An-26/30 and 3 Il-20/22 on the Eastern Apron. Still Working on Aircraft Shelters and Refurbishing the Western Runway.” [Twitter]. Accessed May 23, 2019. https://twitter.com/obretix/status/1040259508734517249.

@obretix. 2018b. “Israeli Airstrikes Have Targeted This Area of Brigade 104 Base Northwest of Damascus Multiple Times. First Part Was Destroyed between May and June 2018 (Possibly on 9/10 May 2018), Second Part on 20 Jan 2019.” [Twitter]. Accessed May 27, 2019. https://twitter.com/obretix/status/1101878702936338435.

@obretix. 2018c. ‘Radar at the S-200 Air Defense Site East of Damascus. Possibly Destroyed by Israeli Airstrike on 10 May 2018.” [Twitter]. Accessed May 27, 2019. https://twitter.com/obretix/status/1000536633563901952.

@obretix. 2019a. “Russian Forpost UAV at T4 Airbase.” [Twitter]. Accessed May 23, 2019. https://twitter.com/obretix/status/1121835010821099521.

@obretix. 2019b. “RuAF at Hmeymim Airbase in Latakia on 30 Jan 2019. New Aircraft Shelters Done, Jets (7 Su-24, 4 Su-30, 4 Su-34) Still Parked Outdoors.” [Twitter]. Accessed May 23, 2019. https://twitter.com/obretix/status/1096474133716701185.

@Obs_IL. 2019b. “Picture of #IRGC Pouya Airlines IL-76 Cargo Lifter Circulating in Social Medias Was Allegedly Taken Yesterday (12.04.19) at “Homs Airport”. According to @flightradar24 EP-PUS Was Indeed in #Syria Yesterday. Was It Related to #IAF Airstrike in Umm Haratein ? Which “Homs Airport” ?” [Twitter]. Accessed May 28, 2019. https://twitter.com/Obs_IL/status/1117093890228654080.

@Paradoxy13. 2015. “Collection of Photos Showing #Russia|n Forces in #Syria Providing Support to Assad’s Regime.” [Twitter]. Accessed May 22, 2019. https://twitter.com/Paradoxy13/status/640114173121331200.

@QalaatAlMudiq. 2018a. “Syria: #Israel Carried out 1st Airstrikes on Regime Targets since the F-16 Was Shot down in February. Multiple Missiles Hit #Tiyas Airbase W. of #Palmyra.” [Twitter]. Accessed May 27, 2019. https://twitter.com/QalaatAlMudiq/status/983261874677600256.

@QalaatAlMudiq. 2018b. “#Syria: Intense Aerial Activity Again on Border with #Golan. Reports a Warplane Crossed Border Few Ago.” [Twitter]. Accessed May 27, 2019. https://twitter.com/QalaatAlMudiq/status/994275149301125136.

@realDonaldTrump. 2018. “Donald J. Trump on Twitter: ‘Russia Vows to Shoot down Any and All Missiles Fired at Syria. Get Ready Russia, Because They Will Be Coming, Nice and New and “Smart!” You Shouldn’t Be Partners with a Gas Killing Animal Who Kills His People and Enjoys It!” [Twitter]. Accessed May 24, 2019. https://twitter.com/realDonaldTrump/status/984022625440747520.

@RisboLensky. 2019. ‘Fierce Missile Battle over #Damascus They Are Flying Everywhere. Some Reached Occupied Golan and Galilee Video via @Syria_Protector.” [Twitter]. Accessed May 28, 2019. https://twitter.com/RisboLensky/status/1087137353012035584.

@Step_Agency. 2019. “ عاجل || مصدر لوكالة #ستيب: إحدى #الغارات_الاسرائيلية استهدفت معسكر الطلائع في منطقة الشيخ غضبان بمحيط #مصياف غرب #حماه والتي تقيم فيه الميليشيات الإيرانية دورات تدريبية لعناصرها” [Twitter]. Accessed May 28, 2019. https://twitter.com/Step_Agency/status/1116855319915892736.

@StratSentinel. 2018. “A Healthy Number of Flying Gas Stations Are Airborne This Afternoon over CONUS.” [Twitter]. Accessed May 24, 2019. https://twitter.com/StratSentinel/status/983748424439943168.

@Syria_Protector. 2018. “Wreckage of #Israeli Missile Was Shot down by #Syrian Air-Defenses over Southern #Damascus Countryside.” [Twitter]. Accessed May 27, 2019. https://twitter.com/Syria_Protector/status/994364756759842816.

@Syrian_MC. 2019. “1-About the Recent Israeli Attack on Syria 1-the Strike Was Expected by the SAA 2-This Particular Strike Shows That Israel Now Is Targeting the SAA Directly 3-the Russian/Iranian Interest Conflict in Syria Effected Directly the Outcomes of Yesterday’s Strike.” [Twitter]. Accessed May 28, 2019. https://twitter.com/Syrian_MC/status/1116988812624891904.

@Syrianzo. 2018. “Huge Explosions in #Salhab in #Hama Province as Iranian and Syrian Military Sites Were Targeted by Israeli Warplanes.” [Twitter]. Accessed May 27, 2019. https://twitter.com/Syrianzo/status/990697743067897856.

@T_intell. 2019a. “Battle Damage Assessment via @sentinel_hub of the #SyAAF’s Pantsir S-1/ SA-22 Prosecuted by the @IAFsite on January 20, 2019. Location Is Damascus International Airport.” [Twitter]. Accessed May 28, 2019. https://twitter.com/T_intell/status/1089916103768395776.

@T_intell. 2019b.”Augmenting @ImageSatIntl Great Work, Here’s the Second Site Targeted by the Israeli Air Force (#IAF) on April 13. Target Was Likely a Logistics Site Used to Deposit High-Value Cargo That Was Airlifted from #Iran to the Nearby #T4 Air Base. RUMINT Says Short-Range BM Launcher.” [Twitter]. Accessed July 16, 2019. https://twitter.com/T_intell/status/1117489664594722817.

@TheHawkOps. 2018. “Images of #Syrian Air Defense Teams Receiving S-300 Training. #Syria #Russia #S300” [Twitter]. Accessed May 24, 2019. https://twitter.com/TheHawksOps/status/1058059301758160896.

@towersight. 2015. “uh Combo #RuAF’’ S-400s &amp; Pantsir S-1 ‘SPAAGM’ on Hmeymim Air Base #Syria.” [Twitter]. Accessed May 23, 2019. https://twitter.com/towersight/status/669922236091015168.

@trbrtc. 2015. “Route of Russian Military Aircraft from Moscow, Russia, to Base in Latakia, Syria, Has an Interesting Flight Route.” [Twitter]. Accessed May 22, 2019. https://twitter.com/trbrtc/status/640968495258279936.

@yarinah1. 2018. “@Bodheesattva @ImageSatIntl I Would Say 10-12 Meters.” [Twitter]. Accessed May 28, 2019. https://twitter.com/yarinah1/status/1078270271721783297.

@YorukIsik. 2015a. “Assad Gets Trucks! Tapir Class BSF Landing Ship 152 Carries GAZ66 #шишига &amp; #KamAZ 43501 to #Syria.” [Twitter]. Accessed May 22, 2019. https://twitter.com/YorukIsik/status/634399137186881536.

@YorukIsik. 2018a. “#ВМФ Project 141 Kashtan Class Buoy Tender KIL158 Redeployed to the Mediterranean after 22 Days: KIL-158 Departed the Black Sea at 05:00Z; Transited Bosphorus towards Mediterranean En Route to #Tartus #Syria.” [Twitter]. Accessed May 23, 2019. https://twitter.com/YorukIsik/status/1032137859963281408.

@YorukIsik. 2018b. “Final Showdown in #Syria: First Time in 2years, Russian Navy Transited Bosphorus with 3ships at the Same Time. #ВМФ #ЧФ BSF Krivak II Class Frigate Pytlivy and #ЧФ BSF Tapir Class LSTs Orsk &amp; Nikolay Filchenkov Transited Bosphorus En Route to #Tartus. My Pics via @reuterspictures.” [Twitter]. Accessed May 23, 2019. https://twitter.com/YorukIsik/status/1032947900056326144.

@YorukIsik. 2018c. “Russia Builds up in Preparation for the Final Chapter of the #Syria War: Armed with Kalibr SS-N-27 Missiles, Admiral Grigorovich Class Frigates #ВМФ #ЧФ Admiral Grigorovich &amp; Admiral Essen Transit Bosphorus towards Med Back-to-Back En Route to #Tartus. My Pics v @reuterspictures.” [Twitter]. Accessed May 23, 2019. https://twitter.com/YorukIsik/status/1033263372798701568.

@YorukIsik. 2018d. “Plane of Interest: Syrian Arab Air Force 585th Transport Squadron of the 29th Air Brigade’s Four-Engine Turbofan Strategic Airlifter Ilyushin Il-76T YK-ATD Flew from Tehran Mehrabad to -Likely- Hamah Military Airport through Iraqi Airspace.” [Twitter]. Accessed May 27, 2019. https://twitter.com/YorukIsik/status/990358624856834048.

Amir. 2017. “Iran’s SAM Coverage.” *Iran GeoMil*. Accessed May 16, 2019. https://irangeomil.blogspot.com/2017/08/irans-sam-coverage.html.

Antonyan, Tatev M. 2017. “Russia and Iran in the Syrian Crisis: Similar Aspirations, Different Approaches.” *Israel Journal of Foreign Affairs* 11 (3): 337–48.

Atkins, Maj Sean A. 2018. “Multidomain Observing and Orienting: ISR to Meet the Emerging Battlespace.” *Air and Space Power Journal,* fall vol.*:* 26-43.

Bacchus. 2019. “Google Earth 3D Maps Exposes Taiwan’s Secret Military Bases.” *Digital Trends*. Accessed February 19, 2019.

https://www.digitaltrends.com/computing/google-earth-3d-map-exposes-taiwan-military-bases/.

Barrington Lisa, and Richard Balmforth. 2018. “Syria Says Air Defences Responding to ‘New Israeli Aggression.’” *Reuters*. Accessed March 19, 2019. https://uk.reuters.com/article/uk-mideast-crisis-syria-israel-response-idUKKBN1FU0AO.

Bartlett, Jamie, Carl Miller, and Jeremy Crump. 2013. *Policing in an Information Age*. CASM Policy Paper. London: Demos.

Barzegar, Kayhan. 2008. “Iran and the Shiite Crescent: Myths and Realities.” *Brown Journal of World Affairs* 15 (1): 87-99.

BBC. 2015. “Nato Warns on Russian Role in Syria.” Accessed September 9, 2015. https://www.bbc.com/news/world-europe-34205003.

BCC. 2018. “Russia Sends S-300 Missile System to Syria.” Accessed March 2, 2019. https://www.bbc.com/news/world-middle-east-45723503.

Bellingcat. 2017. “New Satellite Imagery Shows Russian Su-24 Jets at the Hmeimim Air Base.” Accessed January 20, 2019. https://www.bellingcat.com/news/mena/2017/01/20/new-satellite-imagery-shows-russian-su-24-jets-hmeimim-air-base/.

Bellingcat. 2018. “Open Source Survey of Alleged Chemical Attacks in Douma on 7th April 2018.” Accessed April 11, 2019. https://www.bellingcat.com/news/mena/2018/04/11/open-source-survey-alleged-chemical-attacks-douma-7th-april-2018/.

Bosphorus Naval News. 2015a. “Another Southbound Passage Of Nikolay Filchenkov.” Accessed April 12, 2019. https://turkishnavy.net/2015/09/13/another-southbound-passage-of-nikolay-filchenkov/.

Bosphorus Naval News. 2015b. “Foreign Warship On Bosphorus in 2015.” Accessed January 4, 2016. https://turkishnavy.net/foreign-warship-on-bosphorus/foreign-warship-on-bosphorus-in-2015/.

Brabham, Daren. 2013. *Crowdsourcing*. Boston: MIT Press Essential Knowledge.

Bulos, Patrick J. McDonnell, W. J. Hennigan, Nabih. 2015. “Russia Launches Airstrikes in Syria amid U.S. Concern about Targets.” *LA Times*. Accessed May 22, 2019. https://www.latimes.com/world/europe/la-fg-kremlin-oks-troops-20150930-story.html.

Byman, Daniel. 2018. “Confronting Iran.” *Survival* 60 (1): 107–28.

Casagrande, Genevieve. 2016. *Russian Airstrikes in Syria (September 30, 2015 – September 19, 2016)*. Washington DC: Institute for the Study of War.

Cenciotti, David. 2015. “Six Russian Su-34 Fullback Bomber Have Just Arrived in Syria. And This Is the Route They Have Likely Flown to Get There.” *The Aviationist*. Accessed September 28, 2015. https://theaviationist.com/2015/09/29/su-34-have-arrived-in-syria/.

Cenciotti, David. 2018. “Analysis: Tracking All The U.S. Intelligence Gathering Missions Over the Black Sea After The Kerch Strait Incident.” *The Aviationist* (blog). Accessed December 11, 2018. https://theaviationist.com/2018/12/11/analysis-tracking-all-the-u-s-intelligence-gathering-missions-over-the-black-sea-after-the-kerch-strait-incident/.

CIA. 1953. “Nuclear Weapons in Soviet Propaganda.” *Radio Propaganda Report*. Reston: Foreign Broadcast Information Service.

CIA. 1970. “Foreign Radio and Press Reaction to President Nixon’s Report on U.S. Foreign Policy for the 1970s.” *FBIS Reaction Report*. Reston: Foreign Broadcast Information Service.

CIA. 1985. “News from the Bureaus.” *Newsletter Edition 85-5*. Reston: Foreign Broadcast Information Service.

Clausewitz, Carl. 1976. *On War*. Princeton: Princeton University Press.

Colasanti, Nathalie, Rocco Frondizi, Joyce Liddle, and Marco Meneguzzo. 2018. “Grassroots Democracy and Local Government in Northern Syria: The Case of Democratic Confederalism.” *Local Government Studies* 44 (6): 807–25.

Cooper, Tom. 2018. *Moscow’s Game of Poker: Russian Military Intervention in Syria, 2015-2017*. Warwick: Helion and Company.

CSIS. 2017. “MIM-104 Patriot Launcher - 3D Model.” Accessed May 16, 2019. https://sketchfab.com/models/68f874853be6481db434ea4bf71bb5fa/embed?autostart=1.

Dakhli, Leyla. 2013. “Tunisia and Syria: Comparing Two Years of Revolution.” *Middle East Critique* 22 (3): 293–301.

Dan, Harel. 2018. “X Marks The Spot: Identifying MIM-104 Patriot Batteries From Sentinel-1 SAR Multi-Temporal Imagery.” *Medium* (blog). Accessed October 22, 2018. https://medium.com/@HarelDan/x-marks-the-spot-579cdb1f534b.

Datz, I. M. 2008. *Military Operations under Special Conditions of Terrain and Weather*. New Delhi: Lancer.

Dedijer, Stevan. 2005. ‘‘Obvescevalna knjiznica v obvescevalnem zivcnem sistemu Slovenije?’’ *Organizacija znanja* 10 (3): 124–129.

Defense Blog. 2016. “Russia Fires Bastion-P Anti-Ship Missile against Ground Targets in Syria.” 2016. Accessed November 15, 2018. https://defence-blog.com/news/russia-fires-bastion-p-anti-ship-missile-against-ground-targets-in-syria.html.

Dixon, Paul. 2017. “‘Endless Wars of Altruism’? Human Rights, Humanitarianism and the Syrian War.” *The International Journal of Human Rights*: 1–24.

Doucet, Lyse. 2018. “Syria & the CNN Effect: What Role Does the Media Play in Policy-Making?” *Daedalus* 147 (1): 141–57.

Draeger, Walter R. 2009. “Take Advantage of OSINT.” *Military Intelligence* 35 (5): 39-44.

ecoross1. 2018. “Российский Зенитный Ракетный Комплекс ‘Тор-М2’ На Авиабазе Хмеймим.” *Bmpd* (blog). Accessed April 26, 2019. https://bmpd.livejournal.com/3173438.html.

Engels, Donald W. 1978. *Alexander the Great and the Logistics of the Macedonian Army*. Berkeley: University of California Press.

Erbel, Mark, and Christopher Kinsey. 2018. “Think Again – Supplying War: Reappraising Military Logistics and Its Centrality to Strategy and War.” *Journal of Strategic Studies* 41 (4): 519–44.

Estelles-Arolas, Enrique, and Fernando Gonzalez L. Guevara. 2012. ‘‘Towards an Integrated Crowdsourcing Definition,’’ *Journal of Information Science*, 38 (2): 9–10.

Frantzman, Seth J. 2018. “Analysis: The New War against Iran in Syria Is Psychological - Middle East - Jerusalem Post.” *Jerusalem Post.* Accessed May 27, 2019. https://www.jpost.com/Middle-East/Analysis-The-new-war-against-Iran-in-Syria-is-psychological-556545.

Gibbons-Neff, Thomas. 2016. “Satellite Images Highlight Potential Problems with Russia’s Lone Aircraft Carrier.” *Washington Post*. Accessed November 30, 2018.

Gibson, Stevyn. 2004. “Open Source Intelligence: An Intelligence Lifeline.” *The RUSI Journal* 149 (1): 16–22.

Golaya, Arun Pratap, and Nithiyanandam Yogeswaran. 2018. “‘AIS 2.0’: Technological Changes, Implications and Policy Recommendations.” *Maritime Affairs: Journal of the National Maritime Foundation of India* 14 (2): 63–74.

Gordon, Michael R., and Eric Schmitt. 2018. “Russian Moves in Syria Pose Concerns for U.S.” *The New York Times*. Accessed January 19, 2018. https://www.nytimes.com/2015/09/05/world/middleeast/russian-moves-in-syria-pose-concerns-for-us.html.

GovTribe. 2018. “YEMEN CASEVAC & MEDEVAC AIRLIFT RW&FW HTC711-18-R-R008.” Accessed May 16, 2019. https://govtribe.com/opportunity/federal-contract-opportunity/yemen-casevac-medevac-airlift-rwfw-htc71118rr008.

Gross, Judah Ari. 2018. “IDF Pictures Show Targeted Iranian Intel Sites in Syria.” *Times of Israel.* Accessed May 27, 2019. https://www.timesofisrael.com/idf-pictures-show-targeted-iranian-intel-sites-in-syria/.

Gross, Judah Ari. 2018. “IDF Says It Has Bombed over 200 Iranian Targets in Syria since 2017.” 2018. Accessed April 19, 2019 https://www.timesofisrael.com/idf-says-it-has-carried-out-over-200-strikes-in-syria-since-2017/.

Gruters, Peter C., and Katherine T. Gruters. 2018. “Publicly Available Information: Modernizing Defense Open Source Intelligence.” *Special Operations Journal* 4 (1): 97–102.

Gupta, Ranjit. 2016. “Understanding the War in Syria and the Roles of External Players: Way Out of the Quagmire?” *The Round Table* 105 (1): 29–41.

Haaretz. 2018. “NATO Confirms Russian Naval Buildup Off Syria, Calls for Restraint,” Accessed August 29, 2018. https://www.haaretz.com/middle-east-news/syria/nato-confirms-russian-naval-build-up-off-syria-as-tensions-rise-1.6429071?utm_source=dlvr.it&utm_medium=twitter.

Haddad, Fanar. 2011. *Sectarianism in Iraq: Antagonistic Visions of Unity*. New York: Columbia University Press.

HARM. 2018a. “Hunting AQAP in Yemen: Joint UAE-US Special Operations Base in Mukalla (IMINT).” Accessed May 16, 2019. https://t-intell.com/2018/09/09/hunting-aqap-in-yemen-joint-uae-us-special-operations-base-in-mukalla-imint/.

HARM. 2018b. “The Ayatollah’s Shield: SAM Deployments and Capabilities of the Iranian Air Defenses IMINT”. *T-Intelligence*. Accessed March 1, 2019. https://t-intell.com/2018/12/05/the-ayatollahs-shield-sam-deployments-and-capabilities-of-the-iranian-air-defenses-imint/

HARM. 2018c. “The Syria Strikes: Forecast Reflection and Damage Report of the Joint Air and Naval Operations.” *T-Intelligence.* Accessed May 2, 2019. https://t-intell.com/2018/04/18/the-syria-strikes-forecast-reflection-and-damage-report-of-the-joint-air-and-naval-operations/.

HARM. 2018d. “Israel Shadow-Raids Syria: Preempting Iranian Retaliation (an OSINT P-BDA).” *T-Intelligence.* Accessed May 27, 2019b. https://t-intell.com/2018/05/01/israel-shadow-raids-syria-preempting-iranian-retaliation-an-osint-p-bda/.

HARM. 2019. “Israeli/ U.S. Airborne SIGINT on Station for High-Value TEHRAN Flight.” Accessed May 7, 2019. https://t-intell.com/2019/02/04/israeli-u-s-airborne-sigint-on-station-for-high-value-tehran-flight/.

HARM. 2019b. “Forensic Video Analysis: Syrian Air Defense Unit Abandoned Pantsir S-1 under Israeli IAI Harop Fire.” *T-Intelligence.* Accessed May 28, 2019a. https://t-intell.com/2019/01/29/forensic-video-analysis-syrian-air-defense-unit-abandoned-pantsir-s-1-under-israeli-iai-harop-fire/.

Harp, Seth. 2018. “A Year After the End of ISIS Control in Raqqa, a Ruined City Looks to Rebuild.” *The New Yorker*. Accessed May 5, 2019 https://www.newyorker.com/news/dispatch/a-year-after-the-end-of-isis-control-in-raqqa-a-ruined-city-looks-to-rebuild.

Hassan, Nihad A, and Rami Hijazi. 2018. *Open Source Intelligence Methods and Tools: A Practical Guide to Online Intelligence*. New York: Apress.

Henderson, James H. 2008. *Military Logistics Made Easy: Concept, Theory, and Execution*. Bloomington: AuthorHouse.

Heneghan, Tom, and Tom Perry. 2015. “Russian Air Strikes Hit CIA-Trained Rebels, Commander Says.” *Reuters*. Accesed October 1, 2015. https://www.reuters.com/article/us-mideast-crisis-syria-camp-idUSKCN0RV4KM20151001.

Heuer, Richards J. 1999. *Psychology of Intelligence Analysis*. Washington, D.C.: Center for the Study of Intelligence, Central Intelligence Agency.

Hinnebusch, Raymond. 2018. “From Westphalian Failure to Heterarchic Governance in MENA: The Case of Syria.” *Small Wars & Insurgencies* 29 (3): 391–413.

Howe, Jeff. 2006. “The Rise of Crowdsourcing” *WIRED*. Accessed May 8, 2019. https://www.wired.com/2006/06/crowds/.

Hribar, Gašper, Iztok Podbregar, and Teodora Ivanuša. 2014. “OSINT: A ‘Grey Zone’?” *International Journal of Intelligence and CounterIntelligence* 27 (3): 529–49.

https://www.washingtonpost.com/news/checkpoint/wp/2016/11/30/satellite-images-highlight-potential-problems-with-russias-lone-aircraft-carrier/.

Hubbard, Ben. 2018. "Dozens Suffocate in Syria as Government Is Accused of Chemical Attack." *The New York Times*. Accessed October 10, 2018. https://www.nytimes.com/2018/04/08/world/middleeast/syria-chemical-attack-ghouta.html.

Hughes, Geraint Alun. 2014. "Syria and the Perils of Proxy Warfare." *Small Wars & Insurgencies* 25 (3): 522–38.

Hulnick, Arthur S. 2002. "The Downside of Open Source Intelligence." *International Journal of Intelligence and CounterIntelligence* 15 (4): 565–79.

ImageSatIntl. 2017. "ISI Reveals Russian Iskander Missiles Deployment in Syria. "Accessed May 23, 2019. https://www.imagesatintl.com/insights-iskandar/.

Internet World Stats. 2019. "World Internet Users Statistics and 2019 World Population Stats." Accessed April 25, 2019. https://www.internetworldstats.com/stats.htm.

Issacharoff, Avi. 2015. "Israel Raises Hezbollah Rocket Estimate to 150,000." *Times of Israel*. Accessed May 27, 2019. http://www.timesofisrael.com/israel-raises-hezbollah-rocket-estimate-to-150000/.

ISW. 2019. "Syria Situation Report." *Institute for the Study of War*. Accessed May 21, 2019. http://www.understandingwar.org/backgrounder/syria-situation-report.

Jomini, Antoine. 1971. *The Art of War*. New York: Greenwood Press.

Juneau, Thomas. 2018. "Iran's Costly Intervention in Syria: A Pyrrhic Victory." *Mediterranean Politics*, May, 1–19.

Kerr, Michael, and Craig Larkin, eds. 2015. *The Alawis of Syria: War, Faith and Politics in the Levant*. Oxford: Oxford University Press.

Kuenssberg, Laura. 2018. "Cabinet Agrees 'need for Action' in Syria." *BBC*. Accessed April 13, 2019. https://www.bbc.com/news/uk-43733861.

Lahad, Carmel, Carmel Stern, and Yael Fuchs. 2018. "The Israeli Air Force : Inside Operation 'House of Cards." *IAF website*. Accessed May 27, 2019. http://www.iaf.org.il/4477-50446-en/IAF.aspx.

Lavrov, Anton. 2018. "The Russian Air Campaign in Syria," Moscow: Center for Analysis of Strategies and Technologies.

Leighton, Richard M., and Robert W. Coakley. 1995. *Global Logistics and Strategy, 1940-1943*. Washington DC: Center of Military History United States Army.

Leviev, Ruslan. 2015. “Bellingcat - Are There Russian Troops Fighting in Syria? - Bellingcat.” *Bellingcat*. 2015. https://www.bellingcat.com/news/mena/2015/09/07/are-there-russian-troops-fighting-in-syria/.

Lewis, Jeffrey. 2015. “This Satellite Image Leaves No Doubt That Russia Is Throwing Troops and Aircraft Into Syria.” *Foreign Policy*. Accessed May 22, 2019. https://foreignpolicy.com/2015/09/14/this-satellite-image-leaves-no-doubt-that-russia-is-throwing-troops-and-aircraft-into-syria-latakia-airport-construction/.

Lewis, Oris, Mark Heinrich, and William Maclean. 2018. “Israel Has Struck in Syria since Russia Plane Downed: Israeli Official.” *Reuters*. Accessed October 29, 2018. https://www.reuters.com/article/us-israel-syria-idUSKCN1N325F.

Lister, Charles. 2014. “Assessing Syria’s Jihad.” *Survival* 56 (6): 87–112.

Lombardi, Marco, Todd Rosenblum, and Alessandro Burato. 2015. *From SOCMINT to Digital Humint: Re-Frame the Use of Social Media Within the Intelligence Cylce*. Accessed April 2, 2019. http://www.fondazionedegasperi.org/wp-content/uploads/2016/04/SocmInt-HumInt.pdf

Low, Tammy. 2018. *Exploitation of Big Data for Special Operations Forces.* Occasional Paper. MacDill Air Force Base: JSOU Press.

Lowenthal, Mark M. 2001. “OSINT: The State of the Art, The Artless State,” *Studies in Intelligence*, Vol. 45, No. 3.

Luttwak, Edward. 1993. *The Endangered American Dream*. New York: Simon & Schuster.

Mandel, D. R., and A. Barnes. 2014. “Accuracy of Forecasts in Strategic Intelligence.” *Proceedings of the National Academy of Sciences* 111 (30): 10984–89.

Mansharof, Yossi. 2019. “Iran Strengthens Its Land Route to Damascus.” *JISS*. 2019. Accessed June 20, 2019 https://jiss.org.il/en/mansharof-iran-strengthens-its-land-route-to-damascus/.

Marcus, Jonathan. 2015. “Russia’s S-400 Syria Missiles Send Robust Signal,” *BBC*. Accessed February 28, 2019. https://www.bbc.com/news/world-europe-34976537.

Martin, Russel. 2018. *Russia in the Middle East. From Sidelines to Centre Stage*. Brussels: European Parliamentary Research Service.

Matthew Uttley and Christopher Kinsey. 2012. “The Role of Logistics in War.” In: *The Oxford Handbook of War*, edited by Julian Lindley-French and Yves Boyer. Oxford: Oxford University Press, 401-16.

McKeever, Alexander. 2019. “Wrath of the Olives: Tracking the Afrin Insurgency Through Social Media.” *Bellingcat*. Accessed March 1, 2019. https://www.bellingcat.com/news/mena/2019/03/01/wrath-of-the-olives-tracking-the-afrin-insurgency-through-social-media/.

Mercado, Stephen C. 2004. “Sailing the Sea of OSINT in the Information Age.” *CIA*. Accessed June 2, 2019. https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/vol48no3/article05.html.

Miller, Bowman H. 2018. “Open Source Intelligence (OSINT): An Oxymoron?” *International Journal of Intelligence and CounterIntelligence* 31 (4): 702–19.

Morris, Loveday. 2018. “Iranian Forces Fire Rockets at Israeli Military in First Direct Attack Ever, Israel’s Army Says.” *Washington Post*. Accessed May 9, 2018. https://www.washingtonpost.com/world/iranian-forces-fire-rockets-at-israeli-military-in-first-direct-attack-ever-israeli-army-says/2018/05/09/62e3a526-52f7-11e8-a6d4-ca1d035642ce_story.html.

NATO. 2018. “NATO Standard AJP-4, Allied Joint Doctrine for Logistics (Edition B Version 1)” *Allied Joint Publication.* Brussels: NATO Standardization Office.

Niu, Song, and Aml Ali. 2018. “‘Islamic State’ and the Great Powers’ Game in Syria.” *Asian Journal of Middle Eastern and Islamic Studies* 12 (2): 240–56.

O’Connor, Sean, and Jeremy Binnie. 2017. “Second Russian S-400 in Syria Confirmed.” *Jane’s by IHS Markit*. 2017. Accessed January 28, 2019. https://www.janes.com/article/74500/second-russian-s-400-in-syria-confirmed.

O’Connor, Sean. 2007a. “IMINT & Analysis: The S-200 SAM System: A Site Analysis.” *IMINT & Analysis* (blog). July 22, 2007. http://geimint.blogspot.com/2007/07/s-200-sam-system-site-analysis.html.

O’Connor, Sean. 2007b. “IMINT & Analysis: The S-300P SAM System: A Site Analysis.” *IMINT & Analysis* (blog). August 1, 2007. http://geimint.blogspot.com/2007/08/s-300p-sam-system-site-analysis.html.

O’Connor, Sean. 2010a. “IMINT & Analysis: Syrian Strategic SAM Deployment.” *IMINT & Analysis* (blog). January 7, 2010. http://geimint.blogspot.com/2007/09/syrian-sam-network.html.

O’Connor, Sean. 2010b. “Strategic SAM Deployment in Iran.” APA-TR-2010-0102. Air Power Australia. http://www.ausairpower.net/APA-Iran-SAM-Deployment.html.

O'Leary, Carole A, and Nicholas A Heras. 2019. *Political Strategy in Unconventional Warfare: Opportunities Lost in Eastern Syria and Preparing for the Future*. JSOU Report 19-1. MacDill Air Force Base: JSOU Press.

Omand, David, Jamie Bartlett, and Carl Miller. 2012. "Introducing Social Media Intelligence (SOCMINT)." *Intelligence and National Security* 27 (6): 801–23.

OPCW. 2019. "OPCW Issues Fact-Finding Mission Report on Chemical Weapons Use Allegation in Douma, Syria, in 2018." Accessed May 24, 2019. https://www.opcw.org/media-centre/news/2019/03/opcw-issues-fact-finding-mission-report-chemical-weapons-use-allegation.

Oryx. 2014. "Captured Russian Spy Facility Reveals the Extent of Russian Aid to the Assad Regime." Bellingcat. Accesed October 6, 2014. https://www.bellingcat.com/news/mena/2014/10/06/captured-russian-spy-facility-reveals-the-extent-of-russian-aid-to-the-assad-regime-2/.

Phillips, Christopher. 2015. "Sectarianism and Conflict in Syria." *Third World Quarterly* 36 (2): 357–76.

Politi, Alessandro. 2003. "The Citizen as 'Intelligence Minuteman.'" *International Journal of Intelligence and CounterIntelligence* 16 (1): 34–38.

Prebilic, Vladimir. 2006. "Theoretical Aspects of Military Logistics." *Defense & Security Analysis* 22 (2): 159–77.

Reuters. 2018. "Syria Repositions Air Assets as Trump Hints at War," April 11, 2018. https://www.reuters.com/article/us-mideast-crisis-syria-usa-intelligence-idUSKBN1HI2PN.

Ripley, Tim. *Operation Aleppo: Russia's War in Syria*. [s.l.]: Telic-Herrick Publications.

Roblin, Sebastien. 2019. "Israel Secret Kamikaze Drones Are Killing Syria's Air Defenses." *The National Interest*. Accessed May 19, 2019. https://nationalinterest.org/blog/buzz/israel-secret-kamikaze-drones-are-killing-syria%E2%80%99s-air-defenses-58397.

Rogers, Clifford. 1995. *The Military Revolution Debate – Readings on the Military Transformation of Early Modern Europe.* Colorado: Westview Press.

Rogoway, Tyler. 2018. "This Awesome Chart Shows All The Assets Used In The Trilateral Missile Strikes On Syria." *The Drive*. Accessed May 24, 2019. https://www.thedrive.com/the-war-zone/20509/this-awesome-chart-shows-all-the-assets-used-in-the-trilateral-missile-strikes-on-syria.

Roth, Jonathan P. 1999. *The Logistics of the Roman Army at War (264 B.C.-A.D. 235)*. Columbia Studies in the Classical Tradition, Leiden/Boston: Brill.

Rovner, Joshua. 2013. “Intelligence in the Twitter Age.” *International Journal of Intelligence and CounterIntelligence* 26 (2): 260–71.

Russian Ministry of Defence. 2017. “Operational Formation of the Russian Navy in the Mediterranean Sea Will Receive the Smetlivy Guard Ship of the Black Sea Fleet.” Accessed May 23, 2019. http://eng.mil.ru/en/news_page/country/more.htm?id=12124338@egNews.

Sanderson, Thomas M. 2017. *Russian-Speaking Foreign Fighters in Iraq and Syria.* Washington DC: CSIS.

Scott, Beth, James Rainey, and Andrew Hunt. 2000. *The Logistics of War*. Maxwell Air Force Base: Air Force Logistics Management Agency.

Scott, Len, and Peter Jackson. 2004. “The Study of Intelligence in Theory and Practice.” *Intelligence and National Security* 19 (2): 139–69.

Sharkov, Damien. 2016. “One Man Has Been Tracking Russia’s Transit through the Bosphorus.” *Newsweek*. Accessed April 23, 2016. https://www.newsweek.com/man-who-stares-boats-449088.

Shurkin, Michael. 2017. *The Abilities of the British, French, and German Armies to Generate and Sustain Armored Brigades in the Baltics*. Santa Monica: RAND Corporation.

Smith, Abbot E. 1984. “Notes on ‘Capabilities’ in National Intelligence — Central Intelligence Agency.” Accessed May 28, 2019. https://www.cia.gov/library/center-for-the-study-of-intelligence/kent-csi/vol1no2/html/v01i2a01p_0001.htm.

Sopko, Maj. Mark G. 1999. “Combat Assessment: Analyzing the Results of an Air Campaign”. Maxwell Airforce Base: USAF Air University.

Starr, Barbara and Levitt, Ross. 2015. “Russian Fighter Jets Enter Syria with Transponders off.” *CNN*. Accessed May 23, 2019. https://www.cnn.com/2015/09/24/politics/syria-russian-fighter-jets/index.html.

Statista. 2019. “Number of Mobile Phone Users Worldwide 2015-2020.” Accessed April 25, 2019. https://www.statista.com/statistics/274774/forecast-of-mobile-phone-users-worldwide/.

Steele, Robert D. 1995. “The Importance of Open Source Intelligence to the Military.” *International Journal of Intelligence and CounterIntelligence* 8 (4): 457–70.

Steele, Robert D. 2004. *Special Operations Forces Open Source Intelligence (OSINT) Handbook (Draft)*. Oakton: OSS International Press.

Stewart, Phil. 2017. “U.S. General Told Syria’s YPG: ‘You Have Got to Change Your Brand.’” *Reuters*. Accessed July 21, 2017. https://www.reuters.com/article/us-mideast-crisis-usa-ypg-idUSKBN1A62SS.

Stottlemyre, Steven A. 2015. “HUMINT, OSINT, or Something New? Defining Crowdsourced Intelligence.” *International Journal of Intelligence and CounterIntelligence* 28 (3): 578–89. https://doi.org/10.1080/08850607.2015.992760.

Stratfor. 2015. “Confirming Russia’s Expanded Presence in Syria.” Accessed May 22, 2019. https://worldview.stratfor.com/article/confirming-russias-expanded-presence-syria.

Stratfor. 2016. “Focal Point.” Accessed May 23, 2019. https://www.stratfor.com/sites/default/files/styles/stratfor_full/public/main/images/focal-point-02-06-2016-3%20(1).jpg.

Strohmeier, Martin, Matthew Smith, Daniel Moser, Matthias Schafer, Vincent Lenders, and Ivan Martinovic. 2018. “Utilizing Air Traffic Communications for OSINT on State and Government Aircraft.” In *2018 10th International Conference on Cyber Conflict (CyCon)*, 299–320. Tallinn: IEEE.

Stubbs, Jack. 2015. “Four-Fifths of Russia’s Syria Strikes Don’t Target Islamic State:...” *Reuters*. Accessed October 21, 2015. https://www.reuters.com/article/us-mideast-crisis-syria-russia-strikes-idUSKCN0SF24L20151021.

Sullivan, Marisa. 2014. *Hezbollah in Syria*. Middle East Security Report 19. Washington DC: Institute for the Study of War.

Tangen, Ole Jr. 2016. “Furry Animals Invade Twitter during Brussels Manhunt.” *DW*. Accessed May 9, 2019. https://www.dw.com/en/furry-animals-invade-twitter-during-brussels-manhunt/a-19120084.

Times of Israel. 2018. “Satellite Photos Indicate Precision of Raid on Iranian Military Base in Syria.” Accessed May 27, 2019. https://www.timesofisrael.com/satellite-photos-indicate-precision-of-raid-on-iranian-military-base-in-syria/.

Times of Israel. 2019. “Syria Says Israeli Jets Carry out Airstrike near Aleppo.” Accessed May 28, 2019. https://www.timesofisrael.com/syria-says-israeli-jets-carry-out-airstrike-near-allepo/.

Tomass, Mark. 2016. *The Religious Roots of the Syrian Conflict The Remaking of the Fertile Crescent*. Basingstoke: Palgrave Macmillan.

Trevithick, Joseph. 2018. “Israel Halts Plans For F-15s To Train In Alaska As Iranian Air Defenses Appear In Syria.” *The Drive*. Accessed May 27, 2019. https://www.thedrive.com/the-war-zone/20225/israel-halts-plans-for-f-15s-to-train-in-alaska-as-iranian-air-defenses-appear-in-syria.

Trevithick, Joseph. 2019. “Russia’s New Surveillance Plane Just Flew Over Two Of America’s Top Nuclear Labs.” *The Drive*. Accessed May 7, 2019. https://www.thedrive.com/the-war-zone/27678/russias-new-surveillance-plane-just-flew-over-two-of-americas-top-nuclear-labs.

Tzu, Sun. 2006. *The Art of War.* [s.l.]: Filiquarian Publishing.

U.S Department of Defense. 2018b. “Special Report: FY18 Budget.” Accessed May 15, 2019. https://dod.defense.gov/News/Special-Reports/0518_budget/.

U.S. Army. 1993. *Field Manual (FM) 100-5 Operations*. Washington DC: Headquarters Department of the Army.

U.S. Department of Defense. 2018. *Base Structure Report - Fiscal Year Baseline*. Washington DC: Headquarters Department of Defense.

U.S. Department of Defense. 2019. *Dictionary of Military Terms and Associated Terms*. Washington D.C: Praetorian Press.

U.S. Department of State. 2017. “Rewards for Justice - Reward Offer for Information on al-Nusrah Front Leader Muhammad al-Jawlani.” Accessed Dec 2, 2019. 2019https://www.state.gov/r/pa/prs/ps/2017/05/270779.htm

U.S. Department of the Army. 2012. Open Source Intelligence. Washington DC: Department of the Army Headquarters.

U.S. Joint Chiefs of Staff. 2019. “Joint Logistics.” *Joint Publication 4-0*. Washington DC: US Department of Defense.

US Air Force. 2011. “Factsheets: RC-135V/W Rivet Joint.” Accessed February 20, 2019. https://web.archive.org/web/20110320083003/http://www.af.mil/information/factsheets/factsheet.asp?id=121.

Van Creveld, Martin. 1980. *Supplying War: Logistics from Wallenstein to Patton*. 1. paperback ed., Cambridge: Cambridge Univ. Press.

Van Creveld, Martin. 1991. *The Transformation of War*. New York: Free Press.

Van Creveld, Martin. 2000. *The Art of War: War and Military Thought*. London: Cassell.

Webb, Sam. 2015. “Russian Cornwall Bomber Audio: Listen to Radio Broadcast Believed to Be from Military Aircraft Intercepted by RAF Fighters.” *Mirror*. Accessed February 19, 2015. http://www.mirror.co.uk/news/uk-news/russian-cornwall-bomber-audio-listen-5191420.

Wedeman, Ben, and Lauren Said-Moorhouse. 2019. “ISIS Has Lost Its Final Stronghold in Syria, the Syrian Democratic Forces Says.” *CNN*. Accessed June 20, 2019 https://edition.cnn.com/2019/03/23/middleeast/isis-caliphate-end-intl/index.html.

Weinbaum, Cortney, Steven Berner, and Bruce McClintock. 2017. *SIGINT for Anyone: The Growing Availability of Signals Intelligence in the Public Domain*. Santa Monica: RAND Corporation.

WhitehAll Papers. 2000. “The Development of Military Logistics: An Introduction.” *Whitehall Papers* 52 (1): 1–20.

Wigginton, Michael, Robert Burton, Carl Jensen, David McElreath, Stephen Mallory, and Daniel A. Doss. 2015. “Al-Qods Force: Iran’s Weapon of Choice to Export Terrorism.” *Journal of Policing, Intelligence and Counter Terrorism* 10 (2): 153–65.

Williams, Dan. 2018. “Israel Says Struck Iranian Targets in Syria 200 Times in Last Two...,” *Reuters*. Accessed September 4, 2018. https://www.reuters.com/article/us-mideast-crisis-israel-syria-iran-idUSKCN1LK2D7.

Williams, Heather, and Ilana Blum. 2018. *Defining Second Generation Open Source Intelligence (OSINT) for the Defense Enterprise*. Santa Monica: RAND Corporation.

Wright, Donald P., and Timothy R. Reese. 2008. *The United States Army in Operation Iraqi Freedom, May 2003-January 2005*. Fort Leavenworth: Combat Studies Institute Press.

Yesiltas, Murat. 2017. *Operation Euphrates Shield. Implementation and Lessons Learned*. Ankara: Seta.

Zhou, Yimin. 2019. “A Double-Edged Sword: Russia’s Hybrid Warfare in Syria.” *Asian Journal of Middle Eastern and Islamic Studies*, April, 1–16.

Zilber, Neri. 2019. “To Target Israel, Iran’s ‘Suitcase’ GPS Kits Turn Hezbollah Rockets Into Guided Missiles.” *The Daily Beast.* Accessed February 21, 2019. https://www.thedailybeast.com/to-target-israel-irans-suitcase-gps-kits-turn-hezbollah-rockets-into-guided-missiles.

Zisser, Eyal. 2017. “Syria – from the Six Day War to the Syrian Civil War.” *British Journal of Middle Eastern Studies* 44 (4): 545–58.