SECURITY & DEFENCE QUARTERLY
https://securityandefence.pl/

Fitness OSINT: Identifying and tracking military and security personnel with fitness applications for intelligence gathering purposes

Cyprian Aleksander Kozera

kozeracyprian@gmail.com

https://orcid.org/0000-0001-8620-9849

Institute of Strategic Studies, Faculty of National Security, War Studies University, gen. Chruściela "Montera" 103, 00-910 Warsaw, Poland

Abstract

The objective of this paper is to demonstrate the possibility of tracking and identifying military and other security personnel, operating in secretive or restricted areas. Such exposure might have dire consequences from the perspective of counterintelligence or physical security. Open Source Intelligence (OSINT) and Social Media Intelligence methods and techniques were employed to gather and analyse information on security and military personnel and expose their activities on-line. The case studies presented in the article exemplify utilisation of the new "Suunto" fitness application for open-source-based intelligence research. Despite general Operational Security rules that require all personal data such as names, pictures and habits to be kept discreet, open-source based research with one of the most popular fitness applications allowed the identification of military personnel and government agents operating in Afghanistan, Mali, Syria or working at national military facilities. In a single case, it took the author less than thirty minutes to identify personal details of a US Army soldier in Afghanistan and a Special Forces officer in one of the European countries and obtain their home addresses and pictures of them and their families. The results of the research show how OSINT techniques concerning fitness applications are useful both for intelligence and counterintelligence, specifically for malicious and terrorist purposes, and how necessary it is to make fitness and other, supposedly personal, activity private, especially for those who carry out sensitive missions and work in a restricted or secretive environment.

Keywords:

intelligence, OSINT, open source, fitness application, Suunto

Article info
Received: 29 September 2020
Revised: 17 December 2020
Accepted: 17 December 2020
Available online: 30 December 2020
DOI: http://doi.org/10.35467/sdq/131759

Introduction

By employing Open Source Intelligence techniques (OSINT) and without resorting to any sophisticated tools and programmes, it is still possible to track and identify military and other security personnel operating in secretive or restricted areas. Despite the general Operational Security (OPSEC) rules that require all personal data such as names, pictures, and habits to be kept discreet, a quick glance at the most popular fitness applications allows military personnel and government agents operating in Afghanistan, Mali, Syria or working at national military facilities to be identified. In a single case, it took the author less than thirty minutes to identify personal details of a US Army soldier in Afghanistan or a Special Forces (SF) officer in one of the European countries and obtain their home addresses and pictures of them and their families. OSINT and Social Media Intelligence (SOCMINT) methods and techniques were employed to gather and analyse open-source information on security and military personnel and expose their activities on-line.

The results of the research show how OSINT techniques concerning fitness applications are useful both for intelligence and counterintelligence, specifically for malicious and terrorist purposes, and how necessary it is to make fitness and other, supposedly personal, activity private, especially for those who carry out sensitive missions and work in a restricted or secretive environment. Furthermore, it places OSINT techniques and tools among the most useful and effective research methods in the domain of Military and Security Studies for the purpose of verification of actual events (though one of the least discussed).

In order to conduct this analysis, the author pursued the following research questions:

1. What is OSINT and how does it work?

2. How does one use fitness applications for OSINT purposes?

3. What kind of results does it produce and how can it be exploited?

A methodological approach is based on an analysis of the data publicly available and openly accessible with the newest Suunto fitness application. The method included verification of all publicly visible profiles and their activities in selected conflict theatres (Afghanistan, Mali, and Syria) and some publicly known locations of Special Forces units. The identified cases were then inspected thoroughly with regard to their activity and additional data and information uploaded. The obtained information was cross-checked with other openly available sources (such as internet websites and social media).

The most obvious drawback of this method is its *ex definitione* dependence on data made public by users, and thus it is solely the tip of the iceberg of all data concerning the on-line activity of soldiers and security personnel. No disinformation attempts were identified during the study and, in this context, it would not be cost-effective. Despite the limited amount of obtained data, it was possible to identify specific individuals, making the data worth investigating.

Results of the conducted examination appear on the next few pages. They include case studies of soldiers and security agents exposing information about themselves that may be considered sensitive, at odds with basic personal security rules, and, consequently, could be abused by illicit actors or exploited by foreign intelligence services.

Intelligence, Intelligence Studies and Open Source Intelligence

The intelligence could be simply defined as 'a kind of knowledge' – as Sherman Kent put it in 1949 – or 'the type of organisation which produces the knowledge', or 'the activity pursued by the intelligence organisation' (Herman, 1996, pp. 1–2). The Intelligence is often called the second oldest profession and, as such, a professional activity, it covers the three main missions: collection-and-analysis, covert action, and counterintelligence (Johnson, 2007, pp. 3–4). The intelligence cycle (or process) is inherent in all these three tasks and, according to David Omand, the classic intelligence process consists of: (1) directing setting requirements, (2) collecting, (3) analysing and assessing, (4) disseminating, and (5) reader feedback (Omand, 2010, pp. 117–118). Similarly, the US Joint Staff divides the cycle into: (1) planning and direction, (2) collection, (3) processing and exploitation, (4) analysis and production, and (5) dissemination and integration (Joint Intelligence, 2013, pp. I–6; Minkina, 2014, p. 170). These stages can be simplified into: guidance regarding what is needed, collecting data, processing information, analysing intelligence, disseminating it, and receiving the feedback and providing any necessary adjustments. It therefore shows how the collected data is refined at each of the aforementioned stages and, consequently, becomes the information and, after, a proper analytical process – a piece of intelligence ready to be used by decision- or policymakers. However, not only do states use intelligence but also non-state armed groups and terrorist organisations carry out intelligence missions for their own purposes too (Minkina, 2014, p. 24; Wirtz, 2009, pp. 73–86). Here, OSINT is specifically helpful, as the state actors have mastered other, more sophisticated techniques and use them primarily.

The information is therefore the most crucial component of the whole intelligence process and, as a result, of all missions of the Intelligence profession. In this context, the information itself is often understood as intelligence and is equal to *"a tangible product collected and analysed (assessed or interpreted) in the hopes of achieving a deeper comprehension"* on requested security matter – as Loch K. Johnson (2007, p. 1) explains. Most commonly, however, intelligence differs from information on the basis of the former possessing some secret component. Although, as we are about to learn, not all intelligence is secret (i.e. based on secret data). Yet, as Abram N. Shulsky (2002, p. 172) claims: *"intelligence seeks access to information some other party is trying to deny"*. We shall therefore differentiate the intelligence from information in another way. For the purpose of the OSINT analysis and this article, we shall understand intelligence to be processed information which some other party is trying (or would have tried) to conceal from us (if they know we possess it) and that may be operational (i.e. useful in a security-related context or achieving a strategic interest).

The information can be obtained through various methods, and the Intelligence, as a craft, invented numerous (and seemingly endless) abbreviations, always at hand when it comes to obscuring these methods or disciplines of intelligence collection. These are: HUMINT (Human Intelligence), SIGINT (Signal Intelligence), IMINT (Imagery Intelligence), MASINT (Measurement and Signature Intelligence), FININT (Financial Intelligence), PROTINT (Protected Information), etc. (Johnson, 2007, pp. 5–6; Omand, 2010, pp. 32–33). However, the most accessible in terms of methodology, and the one that is the subject of this analysis, is OSINT – Open Source Intelligence, i.e. the intelligence that can be obtained from publicly available sources or, as Robert David Steele put it in more professional language: "unclassified information that has been deliberately discovered, discriminated, distilled and disseminated to a select audience in order to address a specific question" (Steele, 2007, p. 129). OSINT is, therefore, specific information refined from data accessible to everyone, public and legal. It is intelligence that is virtually lying on the street – all you need is to collect it. It is the press, books, TV, public governmental reports and your friend's picture from the school yearbook, their comments on news websites or public posts on social media. For the latter, there is even another specialised sub-domain of Intelligence, called SOCMINT (Social Media Intelligence) (Omand *et al.,* 2012). It is worth noting, though, that SOCMINT is not always open-source based as it can also work with private (not publicly available) data through various tools and techniques (contrary to open-source investigations that are often dubiously ethical).

In general, compared to some sciences (e.g. Quantitative Sociology), Intelligence is not about gathering a huge amount of data, yet rather a low quantity of specific data confirmed by various sources (cf. Minkina, 2014, pp. 77, 165). In terms of OSINT concerning individuals, however, the amount of data tends to matter. Every piece of open source information in a specific case is a jigsaw puzzle that often adds to the picture. Furthermore, what is specifically crucial in the case of OSINT is that a single piece of information can be worthless, yet when properly set with another, like puzzles, could reveal a broader picture. For instance, somebody's activity on a professional portal (e.g. LinkedIn) does not necessarily reveal much, yet if we add to that his Facebook posts, tweets, Instagram pictures, WhatsApp stories, comments on a news website, exchanges on hobby forums, a dating application profile, stuff being sold on E-bay, articles written for the high-school newspaper and his fitness activities – we can gather a lot of knowledge about a single individual, even enough to tentatively profile them psychologically, learn their home address and obtain pictures of their close relatives. As we have previously stated, intelligence refers to processed and operational information which some other party would have tried to conceal from us, had they known we possessed it. Elementarily, most of us would not care about a single piece of information such as one of the above going public (because it is precisely us who make it public), yet when we realise what can be found out about ourselves when collecting and analysing it as a whole, we might like to have it hidden from the public view. To simplify, in such a case, we can state that one piece of information is nothing, two starts to paint a picture, while three reveals sensitive knowledge. Consequently, the power of OSINT lies in the ability to collect as much publicly available data as possible on a specific case, and properly assess it.

Here, however, come some open source disadvantages. For even if OSINT is easy to obtain, riskless, usually current (up-to-date), rich in sources etc. – from these very qualities arise OSINT-related challenges: of digging through endless data, avoiding information noise or obfuscation (too much information sometimes created on purpose to mislead), assessing what is truly important, dealing with the general character of the information (often OSINT lacks essential details), etc. (Hulnick, 2010, pp. 235–236; Minkina, 2014, p. 193). Moreover, open sources can be non-existent on topics related to the most sensitive and urgent issues or places like North Korea or its recent nuclear programme advancements (Johnson, 2007, p. 2; Hulnick 2010, p. 231). No method is perfect and there is no crystal ball in the Intelligence. OSINT usually serves as a good starting point for further investigation and can therefore limit the use of "real spying" methods. *"It provides a very robust foundation for other intelligence disciplines"* – as Steele noted (Steele, 2007, p. 129). The optimal state of the intelligence collecting stage is, thus, crowned with "jointness", i.e. synergic fusion of all sources and methods (Johnson, 2007, p. 10; cf. Hulnick, 2010, p. 240). Furthermore, OSINT is extremely "shareable" – it can be exchanged with partners without risk of endangering (public) sources (contrary to e.g. HUMINT; Steele, 2007, p. 129). OSINT, however, is much more prone to be used by illicit actors than intelligence services – while states can gain access to the information through other means and methods, terrorist organisations, for instance, may need to limit their reconnaissance to OSINT generally, or social media particularly, and thus *"the adversary utilisation of SOCMINT is considerable and outweighs the advantages of this technology"* for Intelligence services (Dover, 2019, p. 216).

In the US in the middle of the 1990s, in some intelligence domains, such aseconomic analysis, as many as 95% of the intelligence reports were composed of open-source information. In general, one can approximate that 80% of the material available for intelligence analysis is OSINT (Hulnick, 2010, p. 230). Furthermore, open-source based information sometimes provides even more details than other sources. However, it took more time to produce open-source based reports and it did not cover all the requested subjects on its own (Aspin-Brown, 1996, p. 88). Also, as discussed previously, OSINT may be hard to verify, contradictory, or even purposefully deceiving. With the technological breakthroughs of the 21st century, some of the OSINT disadvantages may be significantly reduced, though one should bear in mind that key intelligence (e.g. the missing, yet crucial, 5-20% of the content) may still not be gathered from open sources (Minkina, 2014, pp. 192–193). Nonetheless, it shows how substantial OSINT is in the intelligence process.

While the Internet has been under the scrutiny of OSINT analysts since it was made globally available (cf. JMITC, 1996, pp. 49–66), with the emergence of the global web, both the existence and availability of open sources skyrocketed (Hulnick, 2010, p. 230). Let us only note, for instance, that access to satellite imagery was previously limited to several governments equipped with cutting-edge technology; presently, anyone can have a look at the Earth's most remote places via Bing Maps, Google Earth Pro or through products of enterprises offering more up-to-date data for commercial purposes (the first was a US company, Space Imaging in 1999; Johnson, 2007, p. 6). Even the list of blurred places (accessible through public domain such as Google or Bing Maps yet blurred) diminish regularly, as governments understand that is harder and harder to hide information from the public eye (especially democracies governed by the rule of transparency). In the US, post 9/11 intelligence reform contributed to the increasing consideration of OSINT as well (Hulnick, 2010, p. 229).

Open Source Intelligence therefore gained new attention in the Intelligence Studies, though with constant developments of new internet-based tools, OSINT studies require constant updates in terms of tools and techniques. The Bellingcat Community, a group of open-source journalists and researchers, plays a significant role in revealing and analysing tools, techniques and cases of OSINT being employed – ranging from documenting flight MH-17 being shot down by a Russian BUK missile (Higgins, 2014), to identifying GRU agents involved in the Salisbury poisoning incident (Bellingcat Investigation Team, 2018), to environmental damage related to disappearing date palms in Yemen (Zwijnenburg, 2020). Due to massive developments in the OSINT domain, the literature is not capable of keeping pace with the tools and even techniques of OSINT. Sometimes, every update of an application or a change in its interface even requires an update in related OSINT techniques. For instance, in the previous Facebook layout, in order to find out somebody's constant ID (names can be changed over time, but ID remains the same), it was necessary to access the website code and then look for "entity ID", but after the recent update, it is necessary to search for "userID" (this technique is called de-anonymisation or re-identification).

The fundamental intelligence studies, however, remain valid despite technical changes occurring in the OSINT environment. The so called 'laws of intelligence' remain the same, and, thus, associated methods, even if tools and techniques are susceptible to frequent changes. Here, we should recognise, for the purpose of this study, that as a method, the author understands general, rather unsusceptible to change, ways of obtaining information, while a technique would be a specific application of this method that is susceptible to changes over time (cf. the example discussed above).

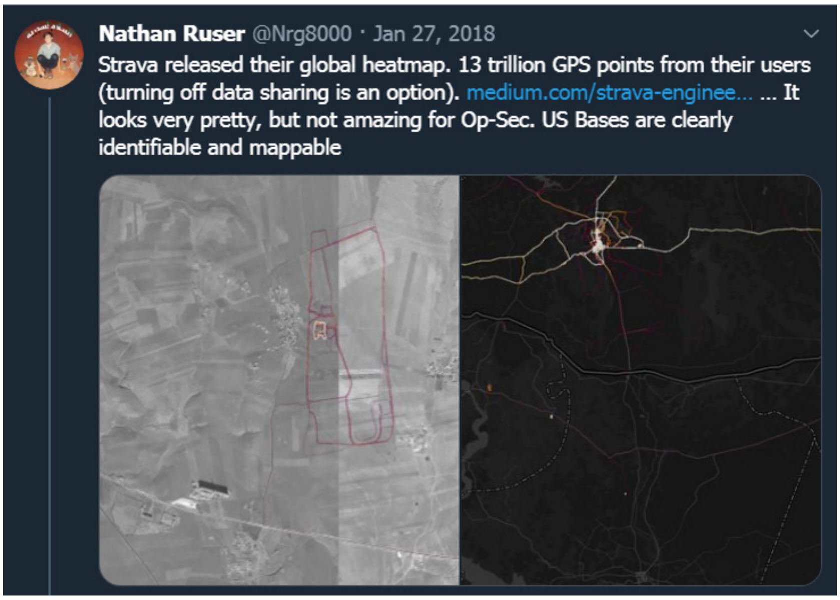
As Michael Warner (2007, p. 17) duly stated: *"Intelligence thus by definition resists scholarship"*, with the 'democratisation' of OSINT studies; however, handbooks, guidebooks and manuals have been appearing increasingly in recent years. Most Intelligence study 'bibles' like theses edited by Loch K. Johnson: Handbook of Intelligence Studies (2007) and Oxford Handbook of National Security Intelligence (2010) do possess a chapter devoted to OSINT ("Open Source Intelligence" by Robert D. Steele 2007, pp. 129–147; and "The Dilemma of Open Sources Intelligence: is OSINT Really Intelligence?" by Arthur S. Hulnick 2010, pp. 229–241 – respectively). Other studies are specifically devoted to practical aspects of OSINT, specifically on the Web, like: Open Source Intelligence Techniques. Resources for Sharing and Analysing Online Information by Michael Bazzell (2018) or Open Source Intelligence Methods and Tools: A Practical Guide to Online Intelligence by Nihad A. Hassan and Rami Hijazi (2018). The latter two manuals, as they discuss specific techniques, require constant and frequent updating, as exemplified by the yearly editorial effort of Michael Bazzell.

This analysis is a modest attempt to update the domain of Security Studies and Intelligence Studies with one specific technique and tool that allows the identities of law enforcement and military personnel to be revealed – identities that should otherwise remain confidential yet were publicly exposed by the aforementioned personnel themselves (often unwarily). The results presented on the following pages therefore do not reveal any restricted information as all the data is open source. Furthermore, all information that could allow exact individuals to be identified has been obscured to respect their privacy.

Fitness applications as OSINT tools

Fitness mobile applications (Strava, Polar, Suunto, etc.), despite their primary and obvious use as tools that allow one to track one's fitness and health, with time became a sport community platform or a social media of sorts, where one can share the training details with other users (including type of training, running routes, heart rates, pauses, etc.), short descriptions, comments, and even photographs. For military and security personnel, especially those in need of being in the best shape and those deployed, fitness applications are a place to exchange their training achievements, share training ideas or just get together. For the OSINT researcher, it has become a tool for gathering information on these very professionals.

Fitness apps have been under the scrutiny of the OSINT community for some time already. In November 2017, the Strava application and website revealed its whole database of the "heat maps", i.e. users' exact training routes (Robb, 2017). Some of these routes, located in remote inaccessible locations in conflict theatres or secretive locations, accumulated in a specific way that pointed to a surprising recurrence in taking the same jogging route of an unnatural shape in remote and hazardous areas. These, especially in Afghanistan or Syria, were easily associated with military facilities (forward operational bases, airfields, etc.), some of them secretive – at least up to that moment (Ruser, 2018). The next year, a similar trait was detected in the Polar fitness application by Foeke Postma – it could even allow specific routes to be associated with particular users (Postma, 2018). As this study is building upon the foundation of the studies conducted by the aforementioned, this technique will be discussed later in this article following the author's own investigation with a different application.



Nathan Ruser @Nrg8000 · Jan 27, 2018
Strava released their global heatmap. 13 trillion GPS points from their users (turning off data sharing is an option). medium.com/strava-enginee... ... It looks very pretty, but not amazing for Op-Sec. US Bases are clearly identifiable and mappable

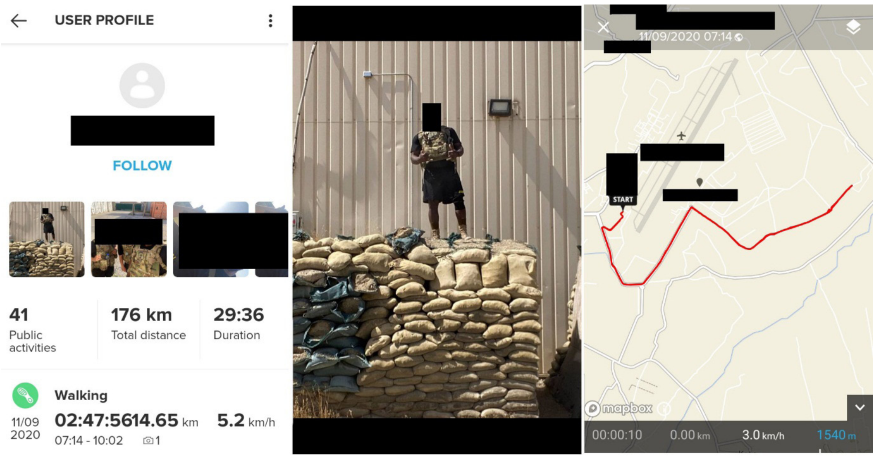
Figure 1. A screenshot of a Twitter thread by Nathan Ruser, who discovered that Starva Heat Map is revealing secretive military locations. The training routes (note unnatural pattern) are visible over satellite photographs that expose no facility at the time the photo was taken. Note: the author of the post states that the number of GPS points is wrongly 13 trillion points, while it was in fact 3 (US) billion GPS points (the number corrected in later posts) (Ruser, 2018).

After the Strava incident, the company decided to censure their most sensitive "heat maps" and military personnel were reminded not to share their activities when on duty, and especially during the deployment. It remains, however, an OPSEC issue, as many military and security personnel worldwide are still unaware of the threats to which they are exposing themselves and their institutions when sharing their data or just using their tracking devices.

Exploring the new Suunto fitness application, the author of this article discovered that many military and security personnel still expose their data, often to an astonishing extent. Some broader research allowed more details on them to be established, in some cases including name, surname, exact place of work, home address and pictures of the individual and his closest relatives. It took less than 30 minutes of OSINT research, without employing any sophisticated tools. It should be noted that contrary to the Strava issue, this study does not use PROTINT (data-protected personal information as defined by Omand, 2010, pp. 32–33) and solely focuses on the data willingly revealed by fitness trackers users.

The fitness application "Suunto" developed by Amer Sports Digital and associated with Suunto tracking devices (e.g. sport watches, very common among Western military personnel due to their robust construction and long-lasting battery) possesses a "Community" mode that allows one to explore others' training routes (hiking, cycling, running, swimming, etc.). In the form of dots of various colours, the map presents users' activities that are made public. Ideally, it helps to design one's own training route, using others' experiences. For the OSINT research purpose, it can be employed to gather information on military and security personnel, especially their home location, activity patterns, surrounding details, aliases, etc.

During one research session, the author scanned Afghanistan territory looking for publicly exposed training sessions. These were several. Among them, one was specifically interesting as the athlete's training was located within one of the airbases. The profile has no profile picture but was signed with a full name. Closer examination showed that pictures from within the base were exposed together with photos of other soldiers (with the rank and name tag) and associated with their common activities in a military base. In the background, some facilities were visible. Older training showed that this User, identified as a US Army senior non-commissioned officer (NCO) previously to being deployed to Afghanistan, had undergone short military training in a military facility in Texas (August 2020). The application also shows that the Army NCO has been training in a specific location in Maryland for the last couple of years. Detailed examination allowed his most common starting point (probably the permanent home address) to be pinpointed to a relatively precise location on a specific road in a town east of Washington DC. Also, using his profile name from the Suunto account, one can find his Facebook account where his pictures in uniform and with his closest family members are made public. Within about fifteen minutes, one could gather this soldier's name, surname, rank, probable unit, deployment, previous training sites (e.g. a military facility in Virginia, 2019), type and intensity of preferred sport activity, home address, family pictures, his wife and army friends' details. This army NCO would rather not be a target of foreign service agents, yet with all these details exposed, he made himself and his family a susceptible target of e.g. a terrorist attack. This case does not seem to provide any sensitive material for foreign intelligence, yet rather exemplifies a significant lack of one user's personal security awareness.



USER PROFILE

[redacted]

FOLLOW

[redacted]

41 Public activities | 176 km Total distance | 29:36 Duration

Walking
11/09 2020 02:47:5614.65 km 5.2 km/h
07:14 - 10:02 1

[redacted]

[redacted]
11/09/2020 07:14
[redacted]

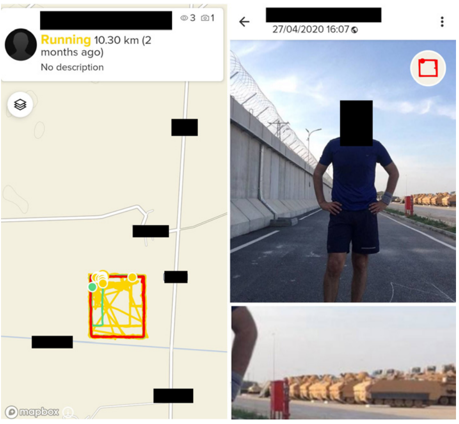
[redacted]
START
[redacted]
[redacted]

mapbox

00:00:10 0.00 km 3.0 km/h 1540 m

Figure 2a, 2b, 2c. A profile of a US Army Senior NCO training at an airbase in Afghanistan. Details provided on his Suunto and Facebook profiles allowed his home address and personal and family details to be discovered (identities and location names obscured; source: Suunto, author's investigation, 2020).

A second investigation case presented is of a Turkish military. The profile signed with name and surname, belongs to a soldier who used to train while being deployed to a military base in south-eastern Turkey, a dozen kilometres from Syrian border, in the spring of 2020. Later, though, around September 2020, he found himself in a Turkish military outpost near a town in northern Syria where he had been continuing his running routine depicted by post-workout pictures. Meanwhile, he had spent some time on Cyprus (July 2020) and in his wife's hometown (according to her Facebook account) in August 2020. His spring training posts from the southern Turkey base were accompanied by pictures. In some of them, one can spot military vehicles or the base facilities in the background, especially on a picture of 27th April 2020, around a dozen M113 Armoured Personnel Carriers in two rows can be identified. The User also has a Facebook profile that reveals his wife's identity and his political opinions. Such cases might be useful when gathering intelligence on Turkish army readiness and equipment at a time of Turkish intervention in Syria.



[redacted] 3 1
Running 10.30 km (2 months ago)
No description

[redacted]
[redacted]
[redacted]
[redacted]
[redacted]

mapbox

[redacted]
27/04/2020 16:07

[redacted]

Figure 3. Screenshots of a Suunto User's training at a Turkish military base near the Syrian border. A close-up of a photo associated with his late April 2020 training allows the identification of M113 Armoured Personnel Carriers in the background (identity and location names obscured; source: Suunto, author's investigation, 2020).

In a similar case, the author found a named embassy security employee who was running in small circles, or "hunting" and "hiking" on the premises of an embassy in Afghanistan (strange depictions of his trainings might be due to automatic recognition of the activity by his sport-watch). One month later (June 2020), the user can be found training on the outskirts of a town in northern Syria; most recently he appeared in south-eastern Turkey at an airport next to the Syrian border (September 2020). His Facebook profile reveals more of his personal details. In parallel, in northern Mali, where armed attacks on the UN peacekeeping forces are frequent, a Romanian soldier revealed a picture of a military base, where he trained. A newly arrived Swedish military man from the same facility shows a picture of his face with his name and surname on his profile, as well as his previous training grounds in a small town in Sweden.

Yet the most striking example of a lack of OPSEC that could be maliciously exploited was perhaps that of a Special Forces officer. Within half an hour, the author identified all the most important information about the SF officer. This Suunto User, whose profile was registered under an initial of a name and full surname, cycles between work and his home on a bike. He starts and ends his routes within a special forces unit and his home in a different town, the exact street visible on the map. Other social media and website accounts registered under the same alias allowed more data to be obtained and confirmed that gathered from the Suunto App, including first name and surname, age, precise home address, telephone number, and pictures of himself and his family members. Contacted by the author in a telephone conversation (the private phone number obtained through open-sources), the Officer claimed that he was not aware of the public visibility of his activities. Due to his position within SF, such an individual could become a target for foreign intelligence services or terrorists. He was not the only member of SF whose Suunto App allowed him to be tracked back home.

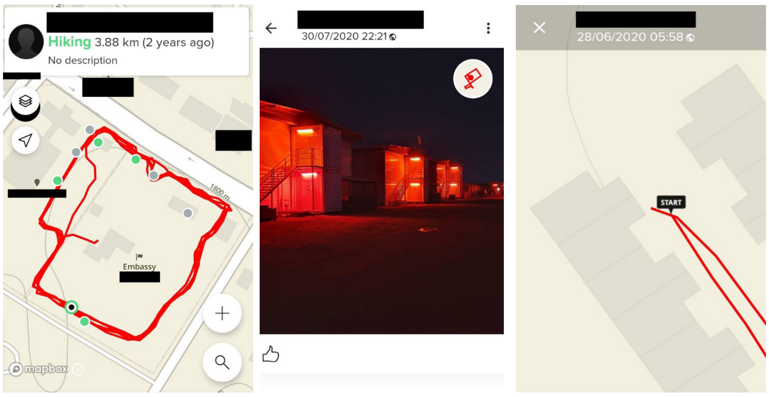


Figure 4a, 4b, 4c. Screenshots of three Suunto Users' accounts providing routes of their training grounds at an embassy in Afghanistan, a picture of a military base in northern Mali, and of the SF Officer's home address. The Users can be related with other locations in their home countries, sometimes even including possible permanent addresses (e.g. fig. 4c). In such cases, numerous training exercises start and end at the same location, a closer examination often allows exact street numbers to be ascertained with convincing precision (identity and location names obscured; source: Suunto, author's investigation, 2020).

Conclusion

The cases discussed cover the use of a fitness application to reveal identities and locations of military and security personnel all over the world – from Afghanistan, to Mali, to Syria, to Europe and the US. The research results concern only one of various existing fitness applications. Therefore, it is a tiny piece of the OSINT domain, yet in certain cases may allow some useful information to be gathered in a short amount of time. Furthermore, cross-checking obtained results with other OSINT tools and techniques that allowed a lot information on a given individual or situation to be obtained. Thus, it does not, and cannot, substitute other methods of the tradecraft (HUMINT, SIGINT, etc.) but can supplement them at very little expense and quickly.

The information above could serve as intelligence to be exploited by a malicious or foreign actor. Intelligence from open-source could allow a target for a terrorist attack on military personnel to be singled out similar to the tragic incident that took place in Woolwich, 2013, when a British soldier was brutally murdered due to him being a member of the armed forces (BBC, 2013), or in 2007 in Basra, when a US base was attacked due to the on-line publication of photos containing GPS coordinates (Rodewig, 2012). Publicly sharing details from military and private life could facilitate identification of soldiers carrying out sensitive tasks in the unit headquarters and then target them with other tools of the intelligence tradecraft. It, therefore, makes one more exposed and vulnerable to other intelligence methods or terrorist attacks.

Some parts of our private life when they become public can endanger ourselves, our families and our organisations. Some of them we make public by agreeing to share small pieces of our lives on the internet, social media or fitness applications. Yet several small pieces add to the virtually full picture. It is, therefore, hard to uphold the boundary between work and private life when our tracking device is constantly on, measuring our bicycle travel from work to home, or a run after a hard day on deployment. It is much easier, though, to set all the settings in the application to manual/private/not visible. This, however, does not always guarantee full privacy. There will always be someone looking for soft spots in the application or devices. The geolocation, for instance, can be tricked and one can sit in an office outside Saint Petersburg and set one's computer geolocation to a military facility in Hereford. Then, suggestions from their fitness app about details of the best athletes nearby to compete with can be received, as Nick Waters from Bellingcat demonstrated with the Strava platform (Nikol, 2020).

Our increasing dependence on electronic and connected gadgets and, consequently, progressing 'encirclement' by the Internet of Things, makes us significantly more exposed and vulnerable. More technology means more untested programmes and applications (and they are only truly tested on its users), more frequent updates, less supervision, more bugs and further opportunities for exploitation by malicious actors. Consequently, such development of fitness and military gadgets (and they become intermingled) opens new possibilities and fuels the need for further studies in this field.

This research proves that we should never entirely trust a device and we ought to not only switch off the app, but also leave smart watches at home, and, especially, not show off when in active service. It is far better to keep one's army stories for a book in retirement, including one's preferred fitness activity.

Funding

This research received no external funding.

Disclosure statement

No potential conflict of interest was reported by the authors.

Bibliography

Aspin-Brown (1996) Aspin-Brown Commission on the Roles and Capabilities of the US Intelligence Community, *Preparing for the 21st Century: An Appraisal of US Intelligence.* Available at: https://www.govinfo.gov/app/details/GPO-INTELLIGENCE (Accessed: 27 September 2020).

Bazzell, M. (2018) *Open Source Intelligence Techniques. Resources for Sharing and Analyzing Online Information.* 6th edn, CreateSpace Independent Publishing Platform.

BBC 2013) 'Woolwich attack: Lee Rigby named as victim', *BBC,* 23 May. Available at: https://www.bbc.com/news/uk-22644857 (Accessed: 27 September 2020).

Bellingcat Investigation Team (2018) 'Full report: Skripal Poisoning Suspect Dr. Alexander Mishkin, Hero of Russia', *The Bellingcat*, 9 October. Available at: https://www.bellingcat.com/news/uk-and-europe/2018/10/09/full-report-skripal-poisoning-suspect-dr-alexander-mishkin-hero-russia/ (Accessed: 27 September 2020).

Dover, R. (2019) 'SOCMINT: a shifting balance of opportunity', *Intelligence and National Security,* 35(2), pp. 216–232. doi: 10.1080/02684527.2019.1694132.

Hassan, N. A. and Hijazi, R. (2018) *Open Source Intelligence Methods and Tools: A Practical Guide to Online Intelligence.* New York – Mississauga: Apress.

Herman, M. (1996) *Intelligence power in peace and war*. Cambridge: Cambridge University Press and the Royal Institute of International Affairs.

Higgins, E. (2014) 'The Buk That Could – An Open Source Odyssey', *The Bellingcat*, 28 July. Available at: https://www.bellingcat.com/news/uk-and-europe/2014/07/28/the-buk-that-could-an-open-source-odyssey/ (Accessed: 27 September 2020).

Hulnick, A. S. (2010) 'The Dilemma of Open Sources Intelligence: Is OSINT Really Intelligence?' in Johnson L.K (ed.) *The Oxford Handbook of National Security Intelligence*. Oxford: Oxford University Press, pp. 229–241.

Joint Intelligence (2013) *Joint Publication 2-0*, 22 October. Available at: https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp2_0.pdf (Accessed: 27 September 2020).

JMITC (1996) *Open Source Intelligence: Professional Handbook*. Joint Military Intelligence Training Center.

Johnson, L. K. (2007) *Handbook of Intelligence Studies*, Abingdon: Routledge

Johnson, L. K. (2010) *The Oxford Handbook of National Security Intelligence*. Oxford: Oxford University Press.

Minkina, M. (2014) *Sztuka wywiadu w państwie współczesnym [The Art of Intelligence in the Modern State]*. Warszawa: Oficyna Wydawnicza RYTM.

Nikol, M. (2020) 'SAS troops have their names and personal details exposed...', *Daily Mail*, 2 February. Available at: https://www.dailymail.co.uk/news/article-7956935/SAS-troops-names-personal-details-exposed.html (Accessed: 27 September 2020).

Omand, D.(2010) *Securing the State.* Oxford: Oxford University Press

Omand, D., Bartlett, J. and Miller, C. (2012) 'Introducing Social Media Intelligence (SOCMINT)', *Intelligence and National Security,* 27(6), pp. 801–823. doi: 10.1080/02684527.2012.716965.

Postma, F. (2018) 'After Strava, Polar is Revealing the Homes of Soldiers and Spies', *The Bellingcat*, 8 July. Available at: https://www.bellingcat.com/resources/articles/2018/07/08/strava-polar-revealing-homes-soldiers-spies/ (Accessed: 27 September 2020).

Robb, D. (2017) 'Building the Global Heatmap', *Strava Medium*, 1 November. Available at: https://medium.com/strava-engineering/the-global-heatmap-now-6x-hotter-23fc01d301de (Accessed: 27 September 2020).

Rodewig, C. (2012) 'Geotagging poses security risks', *The Official Homepage of the U.S. Army* (Archived), 7 March. Available at: https://web.archive.org/web/20120309232923/https://www.army.mil/article/75165/geotagging_poses_security_risks (Accessed: 27 September 2020).

Ruser, N. (2018), 'Strava released their global heatmap...', *Twitter*, Twitter User: Nrg8000, 27 January. Available at: https://twitter.com/Nrg8000/status/957318498102865920 (Accessed: 27 September 2020).

Shulsky, A.N. and Shmitt, G. J. (2002) *Silent Warfare: Understanding the World of Intelligence.* Washington: Potomac Books.

Steele, R. D. (2007) 'Open Source Intelligence', in Johnson L.K (ed.) *Handbook of Intelligence Studies.* Abingdon: Routledge.

Warner, M. (2007) 'Sources and Methods for The Study of Intelligence', in Johnson L.K (ed.) *Handbook of Intelligence Studies*. Abingdon: Routledge.

Wirtz, J. J. (2009) 'Theory of Surprise', in Gill P., Marrin S., Phythian M. (eds.), *Intelligence Theory. Key questions and debates.* Abingdon: Routledge.

Zwijnenburg W. (2020) 'Yemen's Disappearing Date Palms: Applied Environmental OSINT', *The Bellingcat*, 24 July. Available at: https://www.bellingcat.com/news/mena/2020/07/24/yemens-disappearing-date-palms-applied-environmental-osint/ (Accessed: 27 September 2020).