ADMM Cybersecurity and
Information Centre of Excellence

Monthly Digest

Issue 01/24 (January)

A monthly round-up of significant news around the world

Maritime Security

The Dark Side of Open-Source Intelligence in Maritime Security

Use of Open-Source Intelligence in Maritime Domain

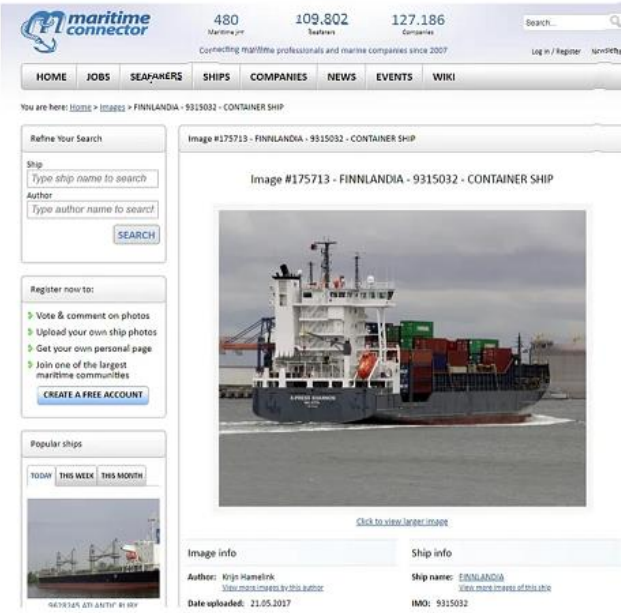
1. *Observer Research Foundation (ORF)*'s report published on 4 October 2023 defines open-source intelligence (OSINT) as available public sources of information for national security purposes, business intelligence, research, maintaining law and order, and media reporting. In the maritime domain, this translates to a diverse range of data taken from publicly available websites containing port schedules, satellite imagery, social media chatter, as well as detailed information about the crew akin to a nautical LinkedIn. Maritime tools such as Automatic Identification System (AIS) can be used to identify vessels in maritime navigation, plan shipping operations, and ensure safety of navigation. According to *Frontiers*, AIS-equipped vessels and shore-based stations exchange identifying information about a vessel's position, course and speed, and at times, this maritime data is collected and sold by global aggregators to maritime operators and industry stakeholders.

Exploiting OSINT for Malignant Purposes

2. According to CREST, open-source marine traffic tools such as 'MarineTraffic.com' and 'VesselFinder.com' use unencrypted AIS transponder messages to create global real-time maps of ship movements. As *Medium* article reported, these tools can also be used to extract information by scrutinising shipping schedules, social media posts by crew members, and satellite imageries to track cargo routes. Consequently, the OSINT tools that facilitate maritime

functions have been misused by malicious actors. Pirates and terrorists have used these tools to gather information about specific vessels or crew members, and to plan their attacks. As these OSINT tools are hosted online, they are also prone to potential cyberattacks.

3. As an example, cyber-attacks on AIS can have significant impact on port operations and maritime safety of vessels. *Science Direct* reported that the types of cyber-attacks on AIS amongst others include spoofing, and arbitrary weather forecasts, and man-in-the middle attacks.[1] When such attacks happen, AIS may be compromised and lead to: (a) fake messages being sent; (b) bogus vessels created with a mimicked trajectory; (c) search and rescue alerts created to lure vessels into certain areas to facilitate attacks by pirates; or (d) AIS information such as speed and voyage information being altered.



You are here: Home > Images > FINNLANDIA - 9315032 - CONTAINER SHIP

Image #175713 - FINNLANDIA - 9315032 - CONTAINER SHIP

- Vote & comment on photos
- Upload your own ship photos
- Get your own personal page
- Join one of the largest maritime communities

Image info

Author: Krijn Hamelink

Date uploaded: 21.05.2017

Ship info

Ship name: FINNLANDIA

IMO: 9315032

Example: Using Maritime Connector to track information about a container ship and its crew

4. For instance, the positions of two NATO warships were falsified in the AIS on 19 June 2021. MarineTraffic.com recorded that the two NATO warships had left Odesa in the middle of the night and sailed towards Crimea, coming within miles of Sevastopol which houses the headquarters of the Russian Black Sea Fleet. This would have been a provocative action if the warships had indeed reached the entrance of the Russian naval base. However, Webcam live feeds broadcasted on YouTube and screenshots of the live feeds showed that the two warships did not leave Odessa. The motives for faking the positions of the

[1] Man-in-the-middle attack is a cyberattack where the attacker secretly relays and possibly alters the communication between two parties who believe that they are only communicating with each other, without realising that the attacker has inserted himself within their conversation.

warships in the AIS remain unclear, but it calls into questions the efficacy of OSINT data like the AIS. Such disinformation is aligned with the trend observed against the backdrop of a complex historical relationship between NATO and Russia, often characterised by political tension.

Navigating the Dark Side of OSINT in Maritime Safety

5. Open-source tracking websites have made it easier for malicious actors to submit unverified data reports that could harm maritime safety. *Authentic8* reported on 5 June 2023 that useful measures to safeguard maritime security include proactively investing in cyber intelligence expertise to monitor online chatter, analysing satellite imagery for suspicious activities, and implementing stricter data security protocols for maritime companies. For example, when authorities can detect that a vessel's AIS is turned off, this could be a sign that the vessel is involved in illegal activities such as unlawful fishing or smuggling, and wants to prevent being tracked. In addition, the International Maritime Organisation (IMO) – a specialised agency of the United Nations – requires all ships to include cyber risk management in their safety management systems in accordance with the international safety management (ISM) code. Such a measure further encourages flag administrations to ensure that ship owners and managers are properly addressing cyber risks in maritime safety.

6. Fostering international cooperation and information sharing among maritime authorities creates a formidable front against threats to maritime safety and maritime security. For example, *Xinde Marine News* reported on 4 August 2023 that the Regional Cooperation Agreement on Combatting Piracy and Armed Robbery against Ships in Asia (ReCAAP)[2] Information Sharing Centre (ISC) held a dialogue with the shipping industry to strengthen cooperation in fighting sea robbery in the Straits of Malacca and Singapore. The ReCAAP ISC provides a useful platform for regional countries and their partners to exchange information and enhance situational awareness in addressing maritime issues. Singapore's Information Fusion Centre (IFC), set up in 2009, also provides a platform for multinational information-sharing and collaboration with regional and extra-regional partners through its IFC Real-time Information-sharing System (IRIS), and conducts capacity-building activities like the Maritime Information Sharing Exercise to facilitate operational cooperation.

7. By taking these proactive measures, we can better ensure that the vast oceans remain a safe and prosperous highway for global trade and cooperation.

[2] ReCAAP is regional agreement established in 2006 which involves 14 Asian countries and their 7 partners – Australia, Bangladesh, Brunei, Cambodia, China, India, Indonesia, Japan, Laos, Malaysia, Myanmar, the Netherlands, Norway, the Philippines, Singapore, South Korea, Sri Lanka, Thailand, Timor-Leste, the United Kingdom and Vietnam, aimed at promoting and enhancing cooperation against piracy in the waters of Asia.

Terrorism

Terrorist Attack in Marawi, Philippines

1. On 3 December 2023, a bombing occurred during a Catholic Mass at the gymnasium of the Mindanao State University in Marawi, killing four people and injuring 50 others. This was the first large-scale terrorist attack since the August 2020 twin bombings in Jolo, Sulu[3].

2. Subsequently on 7 December 2023, ISIS official weekly newsletter *Al-Naba* published an editorial stating that ISIS had claimed responsibility for the bombing in Marawi. This was the first time the southern Philippines was featured in an *Al-Naba* editorial.

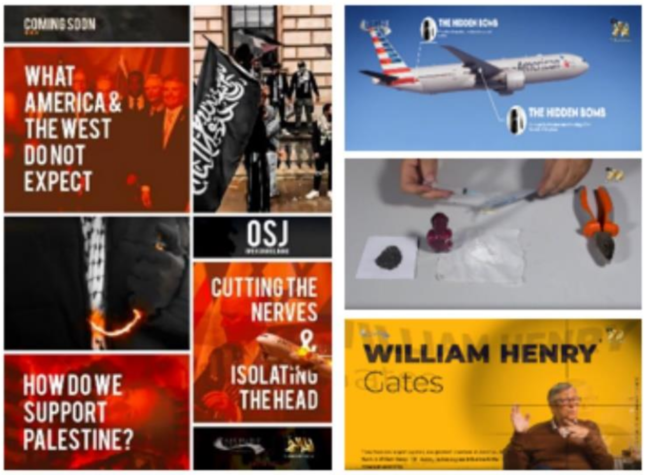
Release of 'New' Edition of Al Qaeda in the Arabian Peninsula's Flagship Magazine, *Inspire*

3. On 29 December 2023, Al Qaeda in Arabian Peninsula (AQAP)'s official media outlet *Al-Malahem Media Foundation* released the 18th edition of the group's flagship magazine, *Inspire*, after a six-year hiatus. This edition urged readers to participate in *jihad* and/or *hijrah* (migration) in response to the "religious war" in the Israel-Hamas conflict, and suggested creating a potassium chlorate-black seeds bomb for use against the US, UK and French commercial airlines, as well as high-profile American business leaders and economists including Bill Gates, Elon Musk, and Ben Bernanke.

4. *Inspire* is significant for motivating at least one terror attack, namely the 2013 Boston Marathon attack, where the *Open Source Jihad* (OSJ) segment of the magazine featured step-by-step instructions detailing methodologies of potential attacks. Examples of past OSJ editions included how to construct various bombs, assemble and use firearms, plan vehicle ramming attacks, and attempt train derailment operations.

5. At least one pro-AQ media group was known to have disseminated *Inspire #18*. Past editions of *Inspire* were known to be circulated within the regional pro-ISIS community.

[3] Twin blasts including a suicide bombing killed at least 15 people and wounded 75 others in Jolo, Sulu on 24 August 2020.


COMING SOON
WHAT AMERICA & THE WEST DO NOT EXPECT
OSJ
CUTTING THE NERVES & ISOLATING THE HEAD
HOW DO WE SUPPORT PALESTINE?
THE HIDDEN BOMB
THE HIDDEN BOMB
WILLIAM HENRY Gates

Screengrabs of AQAP's Inspire #18

ISIS Spokesperson's Audio Statement "And Kill Them Wherever You Find Them"

6. On 4 January 2024, an official ISIS media entity *Al-Furqan Media Foundation* released an audio statement by ISIS spokesperson Abu Hudhayfa al-Ansari, titled "And Kill Them Wherever You Find Them". Abu Hudhayfa also announced the launch of a military campaign in his statement. ISIS had only launched three global military campaigns in the past, with the last one dated April 2022. These campaigns are typically designed to boost activity, morale and propaganda of its various affiliates around the world.

7. Notably, this was the first time the ISIS spokesperson addressed the Israel-Hamas conflict. The spokesperson also incited attacks against "Shi'ites, Jews, Christians and their allies" with a focus on religious and civilian targets.

8. Since the start of the campaign, ISIS has claimed responsibility for numerous attacks stretching from Iraq and Syria, to Nigeria and Mozambique. Notable attacks included a twin suicide attack in Iran that targeted a memorial service for deceased Islamic Revolutionary Guard Corps' commander Qassem Soleimani, and an ambush in the southern Philippines that killed two personnel from the Philippine Armed Forces. This was Iran's deadliest terror attack since 1979, which killed at least 84 and wounded 284.

وَاقْتُلُوهُمْ حَيْثُ ثَقِفْتُمُوهُمْ
كلمة صوتية للمتحدث الرسمي للدولة الإسلامية
الشيخ المجاهد أبي حذيفة الأنصاري (حفظه الله تعالى)

Promotional Banner for "And Kill Them Wherever You Find Them"

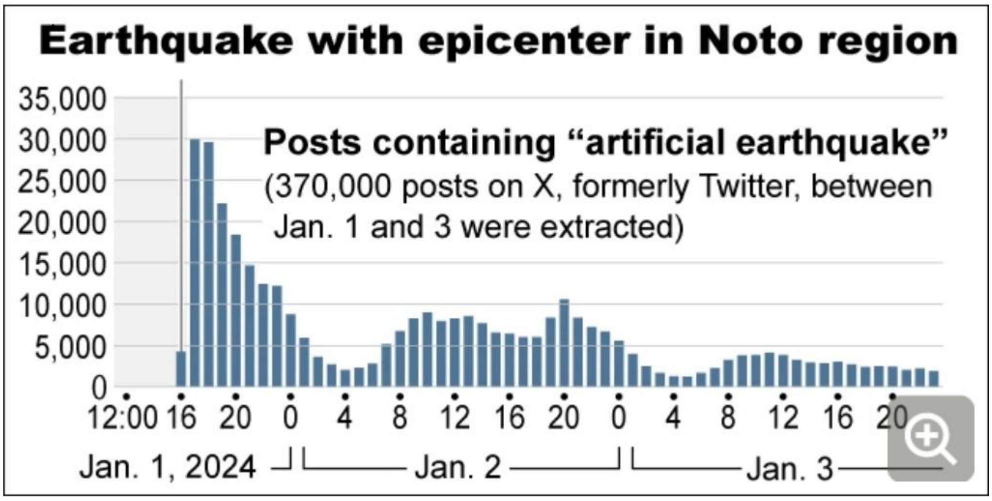
Humanitarian Assistance and Disaster Relief

Misinformation in Japan Quake on New Year's Day

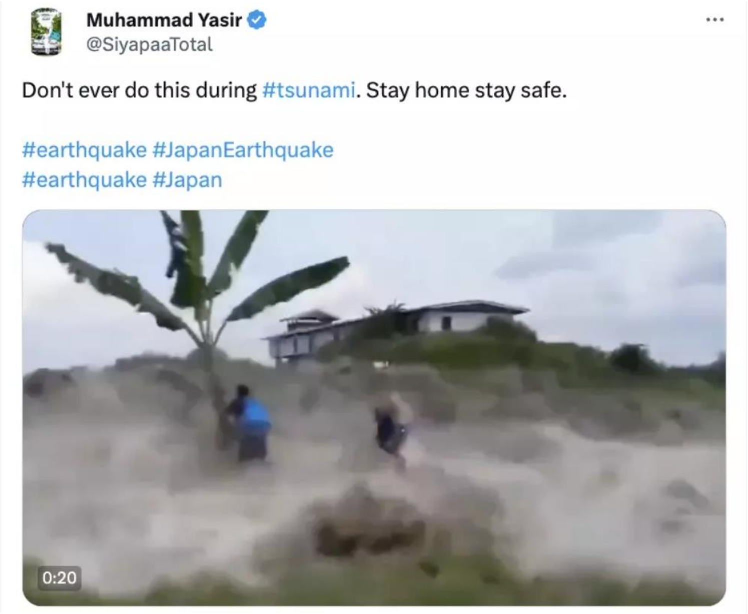
Misinformation spread following Japan Quake

1. **A land-based earthquake of magnitude 7.6 hit central Japan on New Year's Day 2024,** spreading out from Ishikawa Prefecture across the country. This earthquake triggered landslides, building and infrastructure damage, as well as high waves across Japan's western coastline, according to a report by *blackdot* on 4 January 2024.

2. *The Asahi Shimbun* reported on 5 January 2024 that **hundreds of thousands of social media posts spread quickly following the disaster, claiming that the earthquake was artificially created**. A study using Brandwatch, a social media analytics tool, found that these posts were mainly disseminated through X (formerly Twitter). Different types of social media posts were circulated. One social media post featured a link to a website claiming that an international treaty prohibits the military use of artificially-created earthquakes and tsunamis, potentially insinuating that the earthquake was manmade. In another example, a report by *Boom* on 2 January 2024 discovered a viral video of a couple being swept away by a tidal wave during the earthquake, which turned out to be an old video filmed in Indonesia of a tidal bore that occurred in December 2021.



A study by Brandwatch, a social media analytics tool (Source: The Asashi Shibum)


Muhammad Yasir
@SiyapaaTotal

Don't ever do this during #tsunami. Stay home stay safe.

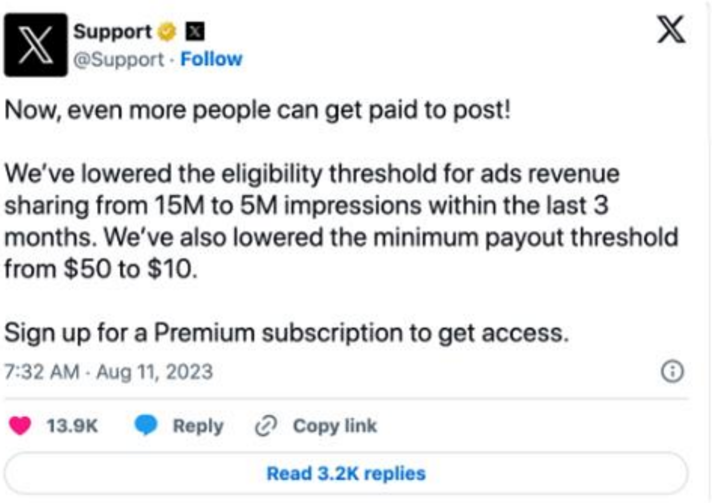
#earthquake #JapanEarthquake
#earthquake #Japan

A X post of a couple apparently being swept away during the Japan earthquake, which was found to be an image in Indonesia in 2021 (Source: Boom)

3. The wide spread of social media posts on the Japan earthquake is consistent with the pattern we have observed following the onset of incidents that have substantial public interest. These posts may contain accurate information, or they could be manipulated to contain doctored images and false information. In the absence of complete or timely information, there is a high risk that social media users may share information quickly without first verifying their accuracy, leading to misinformation going viral.

4. Misinformation and disinformation during natural disasters can negatively impact rescue efforts, incite fear and anxieties in the people, and erode confidence in the decision-making and actions taken by government authorities. For instance, the Japanese people were distrustful of telecommunications vehicles sent to repair mobile phone base stations wrecked by the earthquake as there were fake news that these vehicles would rob homes of residents who had evacuated after the quake. *Kyodo News* reported on 9 January 2024 that Japan Prime Minister Fumio Kishida had implored the Japanese people to “strictly refrain” from spreading malicious and fake news that would hinder relief efforts during times of crisis and human suffering.

Financial incentive potentially triggering misinformation



Support
@Support · Follow

Now, even more people can get paid to post!

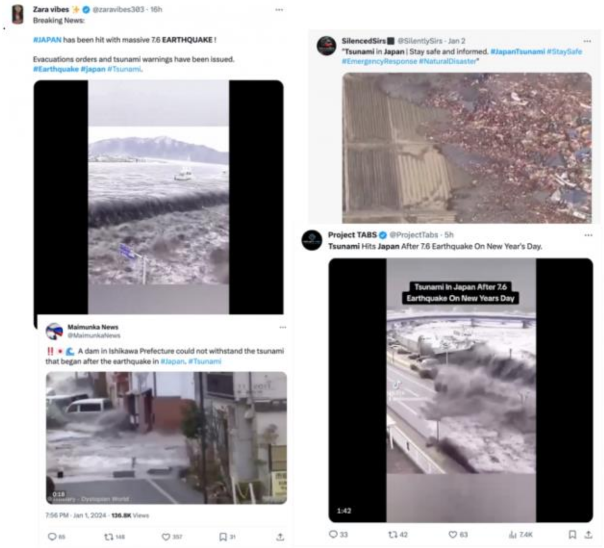
We've lowered the eligibility threshold for ads revenue sharing from 15M to 5M impressions within the last 3 months. We've also lowered the minimum payout threshold from $50 to $10.

Sign up for a Premium subscription to get access.

7:32 AM · Aug 11, 2023

Blue checkmark system on X
(Source: blackdot)

5. *The Asahi Shimbun* analysed that financial greed may be behind the rising trend of misinformation. For example, subscribers of X now have the option to boost visibility and garner high interactions on their posts through the blue checkmark by way of a paid subscription. The higher viewership then results in more monetary gains for the subscribers who posted on X. Shinichi Yamasuchi, an associate professor at the Center for Global Communications of the International University of Japan, specialising in disinformation and defamation issues, explained that X had been allocating revenue based on the number of times a post is viewed since the second half of 2023.



Zara vibes @zaravibes303 · 16h
Breaking News:

#JAPAN has been hit with massive 7.6 EARTHQUAKE !

Evacuations orders and tsunami warnings have been issued. #Earthquake #japan #Tsunami.

Maimunka News
@MaimunkaNews

‼️ 🇯🇵 🌊 A dam in Ishikawa Prefecture could not withstand the tsunami that began after the earthquake in #Japan. #Tsunami

7:56 PM · Jan 1, 2024 · 136.8K Views

SilencedSirs @SilentlySirs · Jan 2
"Tsunami in Japan | Stay safe and informed. #JapanTsunami #StaySafe #EmergencyResponse #NaturalDisaster"

Project TABS @ProjectTabs · 5h
Tsunami Hits Japan After 7.6 Earthquake On New Year's Day.

A X post of tsunami apparently following the Japan quake, which were images from a tsunami in Japan in 2011
(Source: blackdot)

6. In the case of the Japan earthquake, it was observed that there was a sudden rush of X accounts with blue checkmarks posting videos of large waves sweeping across Japan and causing damage to building and roads. These images were later found through reverse image searches to depict the 2011 tsunami in Japan. One should therefore exercise caution and verify the facts rather than share information callously. The perils of misinformation going viral and causing mass confusion during the peak of crises can result in heavy costs for the nation, and hamper efforts to restore peace and stability swiftly for the people.

CONTACT DETAILS

All reports can be retrieved from our website at www.acice-asean.org/resource/.

For any queries and/or clarifications, please contact ACICE at ACICE@defence.gov.sg.

Prepared by:
ADMM Cybersecurity and Information Centre of Excellence

REFERENCES

Maritime Security

1. Open-Source Intelligence Has Arrived
https://www.orfonline.org/research/open-source-intelligence-has-arrived

2. Shining A Light on AIS Blackouts With Maritime OSINT
https://www.frontiersin.org/ariticles/10.3389/fcomp.2023.1185760/full

3. OSINT Vs Disinformation: The Information Threats ‘Arms Race’
https://www.crestresearch.ac.uk/comment/osint-vs-disinformation-the-information-threats-arms-race/

4. Practical Maritime OSINT
https://www.cybersecurity.att.com/blogs/security-essentials/practical-maritime-osint

5. OSINT on the Ocean: Maritime Intelligence Gathering Techniques
https://www.wondersmithrae.medium.com/osint-on-the-ocean-maritime-intelligence-gathering-techniques

6. OSINT Tips for Investigating Maritime Vessels
https://www.authentic8.com/blog/maritime-osint-rae-baker

7. ReCAAP ISC Holds Dialogue with Shipping Industry to Strengthen Cooperation to Fight Sea Robbery in the Straits of Malacca and Singapore
https://www.xindemarinenews.com/m/view.php?aid=49379

8. About ReCAAP Information Sharing Centre
https://www.recaap.org/about_ReCAAP-ISC

9. Risk sensitivity of AIS cyber security through maritime cyber regulatory frameworks
https://www.sciencedirect.com/science/article/pii/S0141118723003966

Terrorism

1. Bombing attack on Catholic mass in Philippines kills four
https://www.aljazeera.com/news/2023/12/3/explosion-hits-university-in-philippines-three-reported-killed

2. Boston Marathon bombing of 2013
https://www.britannica.com/sports/Boston-Marathon

3. Philippine military: IS-linked militants kill 2 army intelligence operatives
https://www.benarnews.org/english/news/philippine/troops-killed-01042024130253.html

4. Exploring the Role of Instructional Material in AQAP's *Inspire* and ISIS' *Rumiyah*
https://nsc.crawford.anu.edu.au/publication/10583/exploring-role-instructional-material-aqaps-inspire-and-isis-rumiyah

Humanitarian Assistance and Disaster Relief

1. Old Video from Indonesia falsely linked to Japan earthquake
https://www.boomlive.in/fact-check/indonesia-people-being-swept-away-tsunami-japan-earthquake-fact-check-24004

2. Fact-checking the Japan earthquake: Has a tsunami hit? Is a nuclear plant compromised?
https://blackdotresearch.sg/japan-earthquake-factcheck/

3. Misinformation proving challenge to relief efforts after Japan quake
https://english.kyodonews.net/news/2024/01/ecfb28d4bf14-misinformation-proving-challenge-to-relief-efforts-after-japan-quake.html

4. Scourge of 'fake news' spreads after killer quake in Ishikawa
https://english.kyodonews.net/news/2024/01/ecfb28d4bf14-misinformation-proving-challenge-to-relief-efforts-after-japan-quake.html