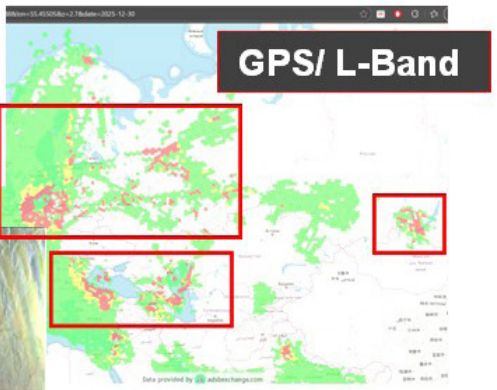
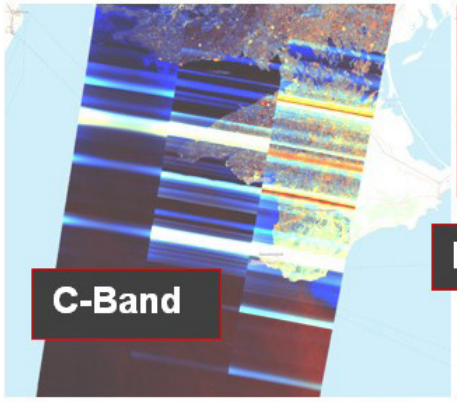
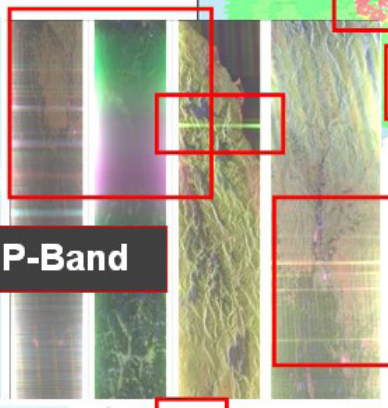
Russian, Chinese and Myanmar’s Junta, war-related electromagnetic emissions observed from space

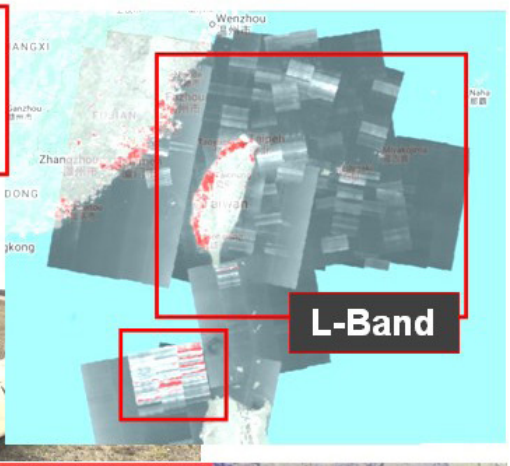
Simon Hagmayer, 04.01.2026

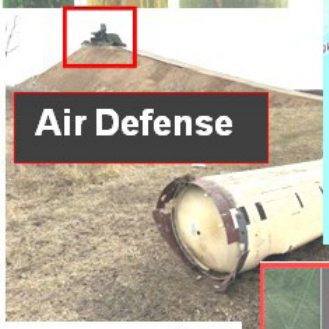
Band	Freq range [GHz]	Satellite used	center Freq of satellite [GHz]
P-band	*0.23-1*	*P-SAR*	*0.435*
L-band	1-2	ALOS PALSAR	1.2575
S-band	*2-4*	-	-
C-Band	4-8	Sentinel-1	5.405
X-Band	8-12	TerraSAR-X/ AMSR	9.650/ 10
Ku-band	*12-18*	*AMSR*	*18*











UNCLASSIFIED

7 June 2023

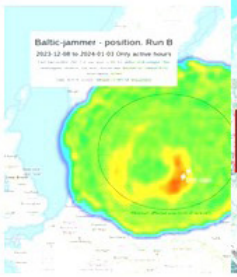
3GIMBALS

TIRADA-2

Name: Tirada-2
Name Russian: Тирада-2
Other names: Tirada-2S
Other names, Russian: Тирада-2С
Purpose/use: Uplink jamming of communications satellites using a narrow beam to target the frequencies of certain satellite communication channels
- Disrupts the operation of satellite communications by determining the parameters of the satellite communications complex and creating interference
- Capable of disrupting the satellite communications of reconnaissance UAVs

Bandwidth/frequencies: 3–14 GHz, centimeter band
Range/antennae ranges: unspecified, several tens of kilometers
Variants: Tirada-1D, Tirada-2S, Tirada-2.2, Tirada-2.3 (also called RB-371A), and Tirada-2.4
Approximate date of adoption to Russian military: 2019
TTPs used to counter system(s): Unknown
Additional information:
- Suspected of being used to disrupt SpaceX's Starlink communications satellites on the southern frontlines in Kherson and Zaporizhzhia oblasts, as well as Kharkiv, Donetsk, and Luhansk oblasts in the east
- Predecessor of Tirada-2 and other variants is the Soviet era Tirada-1D
- Different variations of Tirada-2 may be designed to cover different parts of the

The Tirada complex includes a mobile command center, a hardware machine with means of detecting communications and jamming – mounted on a KamAZ chassis , and an electric generator. Source: © 9 October 2022. For-ua.info



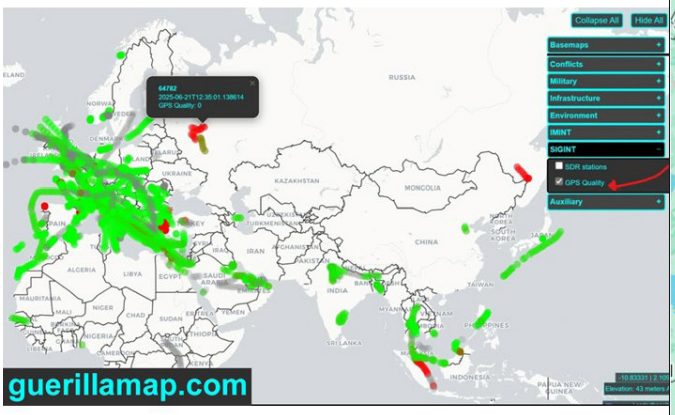
In Summary

What we observe

Since Russia's full-scale invasion of Ukraine, electromagnetic warfare has intensified dramatically, reaching unprecedented levels. Extensive GPS jamming and spoofing, radar interference, counter-drone electronic warfare, and large-scale air-target radar activity now emit signals so powerful they can be detected by space-based sensors not designed for this purpose. While first observed in the Russo-Ukrainian war, similar phenomena are now occurring in regions such as Myanmar, near Taiwan and Lebanon.

These activities cause widespread navigation disruptions, including incorrect ship positions transmitted via AIS and faulty GPS data received by aircraft. Satellite observations across multiple frequency bands (P, L, C, X, and Ku) from instruments such as Sentinel-1, TerraSAR-X, AMSR, ALOS PALSAR, and ESA's Biomass P-SAR reveal strong interference signals linked to electronic warfare.

Overall, the study demonstrates that modern electronic warfare now operates at a scale and intensity detectable globally from space, marking a significant escalation in electromagnetic

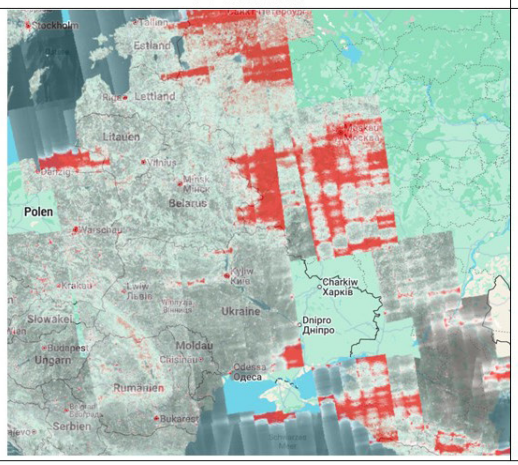
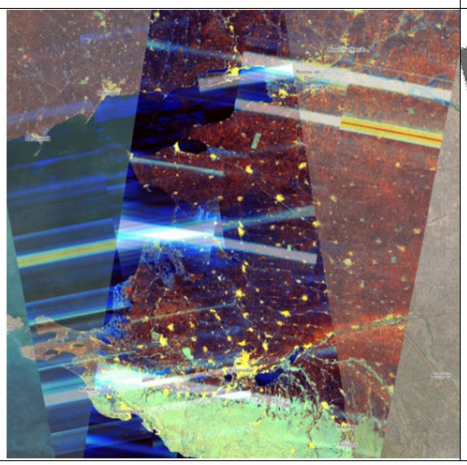
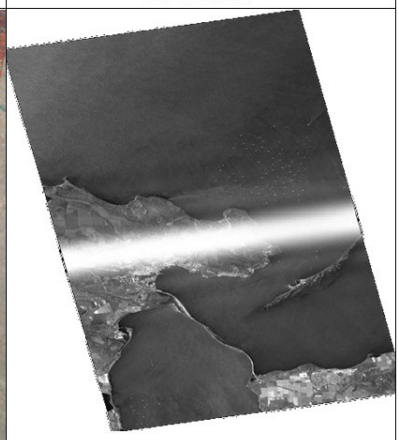
GPS interference via ADS-B	C-band jamming, seen on Sentinel-1
	

What we conclude

Now, after we have seen these signals there are **three main questions**:

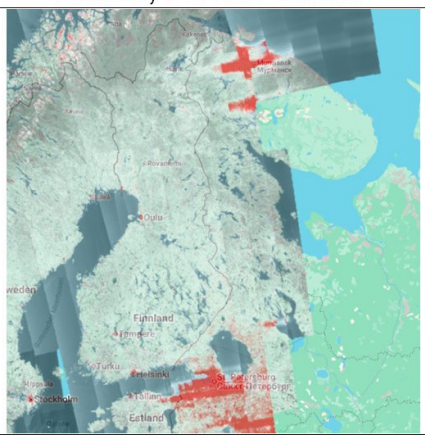
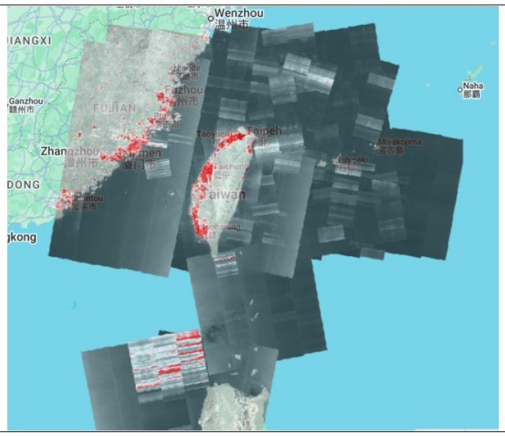
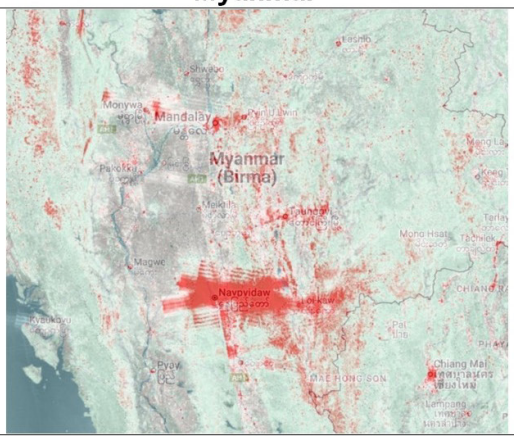
What frequencies and areas are affected?

Definitely L, C and X-band and to some degree maybe also P-band. It's highly likely that S-band is also affected. Above 10 GHz we were not able to detect something, but that does not mean that there is nothing.

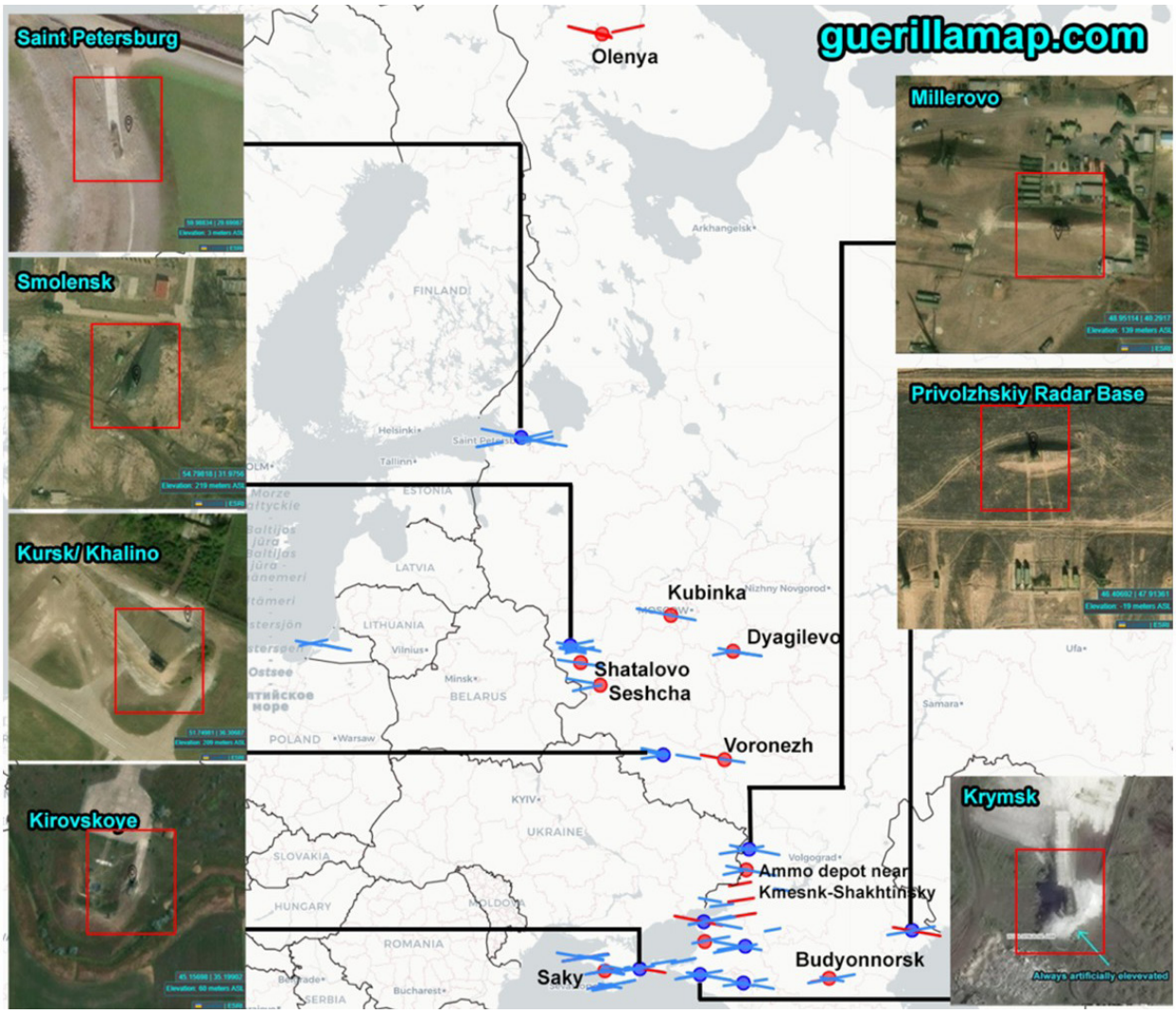
L-band	C-band	X-band
		

We see the strongest emissions along the Russo-Ukrainian border, Kaliningrad, St. Petersburg and Murmansk, all near high value targets, like air bases.

Some quite similar signals **(both, L- and C-band)** were present in China near Taiwan, in the sea around Taiwan and in the Junta controlled areas in Myanmar.

Russia, Ukraine border	Russia, Finland border
	
China - Taiwan	**Myanmar**
	

Sentinel-1 derived locations of transmitters:



What is the purpose of this electromagnetic emission?

Most likely a combination of different purposes: Detection, Jamming/Spoofing, Communication.
In general: Protecting high value targets, this is given due to the geographical locations the signals occur.

Jamming and spoofing can be subdivided further into different categories:

- Blind Ukrainian effectors (missiles, drones, …) : Jam their GPS, blind missile radar heads to prevent target finding.
- Blind ISR (Intelligence, Surveillance, Reconnaissance) : Blind radar satellite and aerial reconnaissance.
- Disrupt communication: Jam satellite or drone data links, ground based communication, etc.

What systems/emitters could be responsible?

A whole bunch of different systems probably, some are specific EW systems for GPS jamming and spoofing, like Tobol, or, Pole-21, some for radar jamming, like Repellent-1 or Tirada-2. Others are probably air defense radars sending at maximum power, like associated radars of Pantsir or S-400 SAM systems.

When we talk about the strong C-band signals in the Sentinel-1 images, then Repellent-1 (anti-UAV) or Tirada-2 (anti Satcom, like Starlink) systems are highly likely, in combination with maybe S-400 radar systems.

Of course in the Chinese/ Myanmar case there will be similar systems.

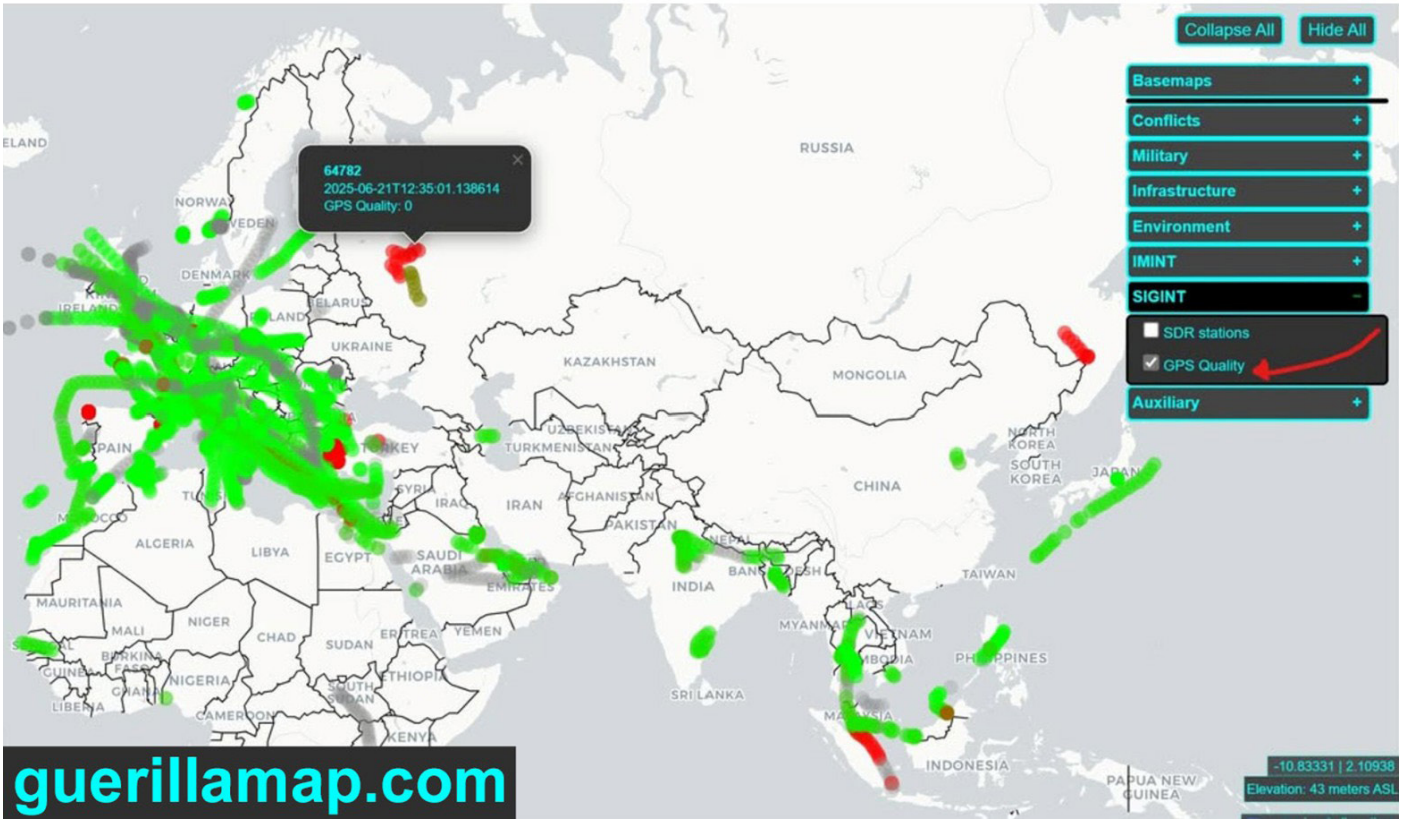
Notably the Russians have a huge arsenal of different, domestically produced EW systems. Russia is using everything it has in respect to EW in this conflict. We also have to consider radar detection and communication systems and not just EW. So when we think of the full scale war we have to imagine all these systems being in service in an integrated electromagnetic defense web, each with their respective advantages and functions.

1.What we observe

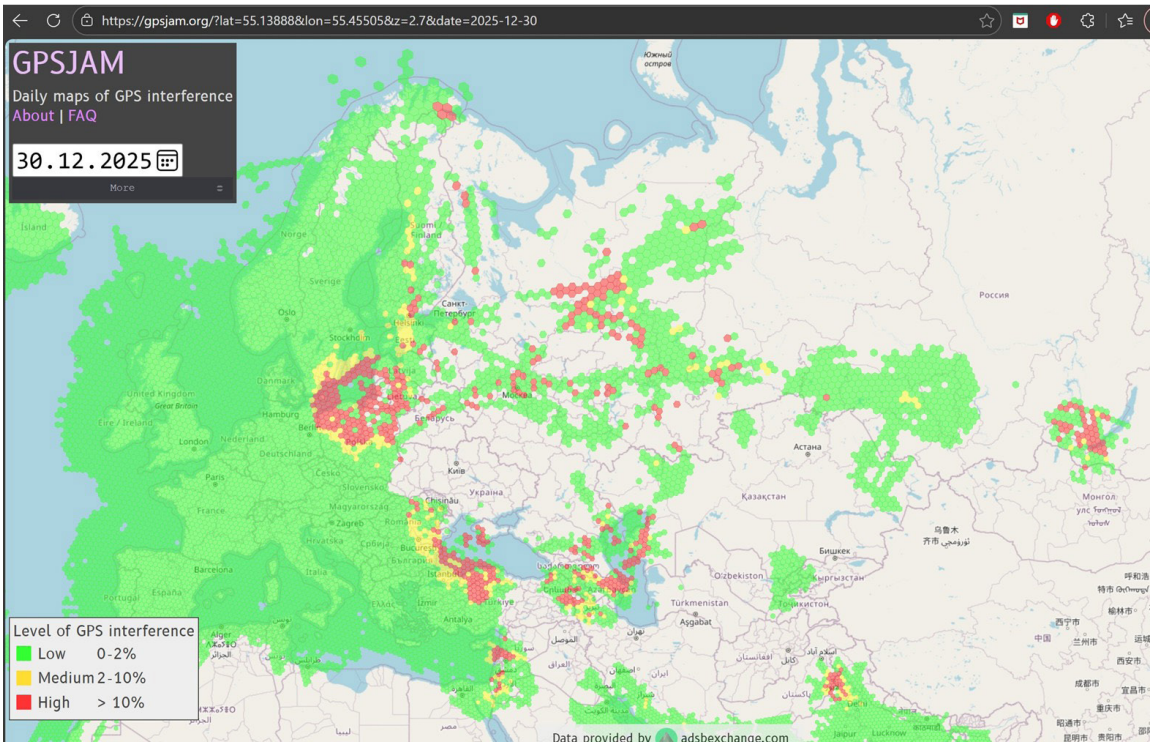
Since Russia's full scale invasion of Ukraine, the electromagnetic warfare was pushed to a whole new level. GPS jamming and spoofing, radar jamming, counter drone EW (Electronic Warfare) or the scale and amplitude of radar air target identification reached levels never seen before. The signals emitted in this war are sometimes strong enough to be seen from space sensors that were never intended to monitor such signals and could not be seen before, or at least not at such a scale. The emitted power is probably strong enough to grill a chicken in front of theses radar dishes. The phenomenon is now no longer limited to the Russo-Ukraine war, but we now see it in Myanmar, Lebanon and near Taiwan too.

We see wrong positions of ships sent via their AIS. We see bad GPS positions picked up by airplanes near and in Russia. We see massive L, C and X-band signals on different imaging satellites, such as Sentinel-1, AMSR, TerraSAR-X, or Biomass P-SAR.

Here is an example of the detected GPS-jamming. Airplanes can transmit a so-called ADS-B signal, sending information like position, altitude, speed, aircraft identification and so on. One of the parameters transmitted is a GPS quality indicator and we can map this information, where



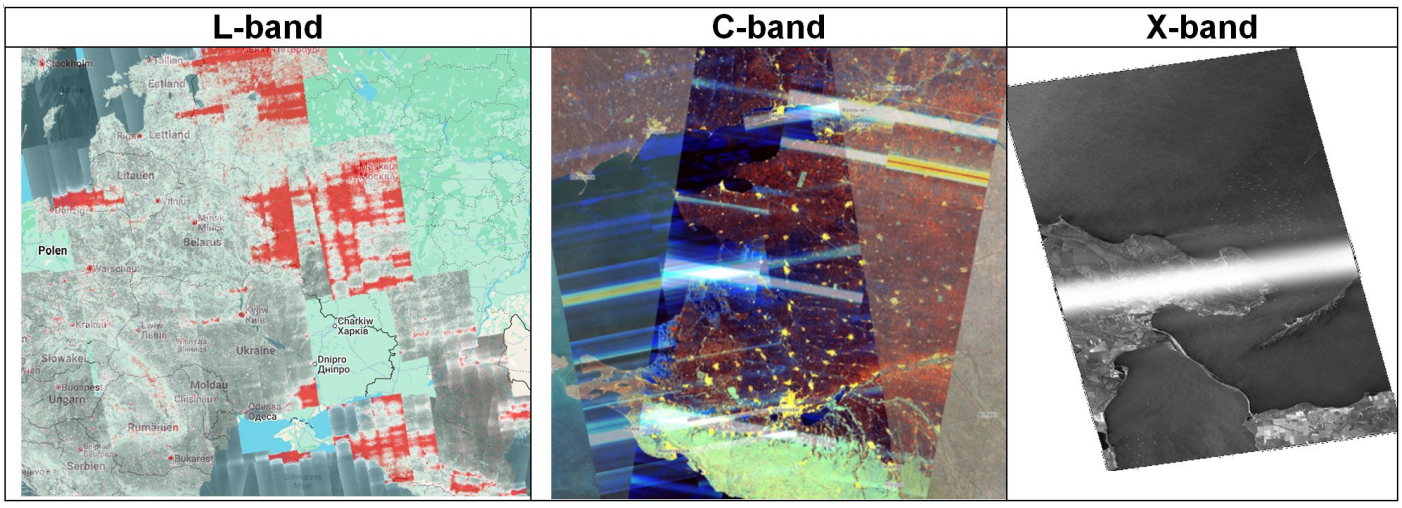
We can clearly identify areas with bad GPS, mostly in Russia and on this specific day also in the Aegean Sea, or Malaysia. Gpsjam.org takes it one step further and also includes civil aircraft; this gives us a more complete picture:



In the radar domain, there are 4 different satellite instruments we used in this study. For P-band we used a new instrument called P-SAR onboard the Biomass satellite from ESA with a center frequency of 435 MHz. In L-Band we used the Japanese (JAXA) ALOS PALSAR satellite with a 1257.5 MHz center frequency.

In C-band ESA's Sentinel-1 with 5.4 GHz and in X-band the German TerraSAR-X with roughly 9.6 GHz and AMSR, a Japanese passive radar with a 10 GHz band and we used the same sensor also for Ku-band, where it can observe 18 GHz signals.

Some impressions from the different radar bands and interferences observed:



Now, after we have seen these signals there are three main questions:

- **What frequencies are affected?**
- **What is the purpose of this electromagnetic emission?**
- **What systems/emitters could be responsible?**

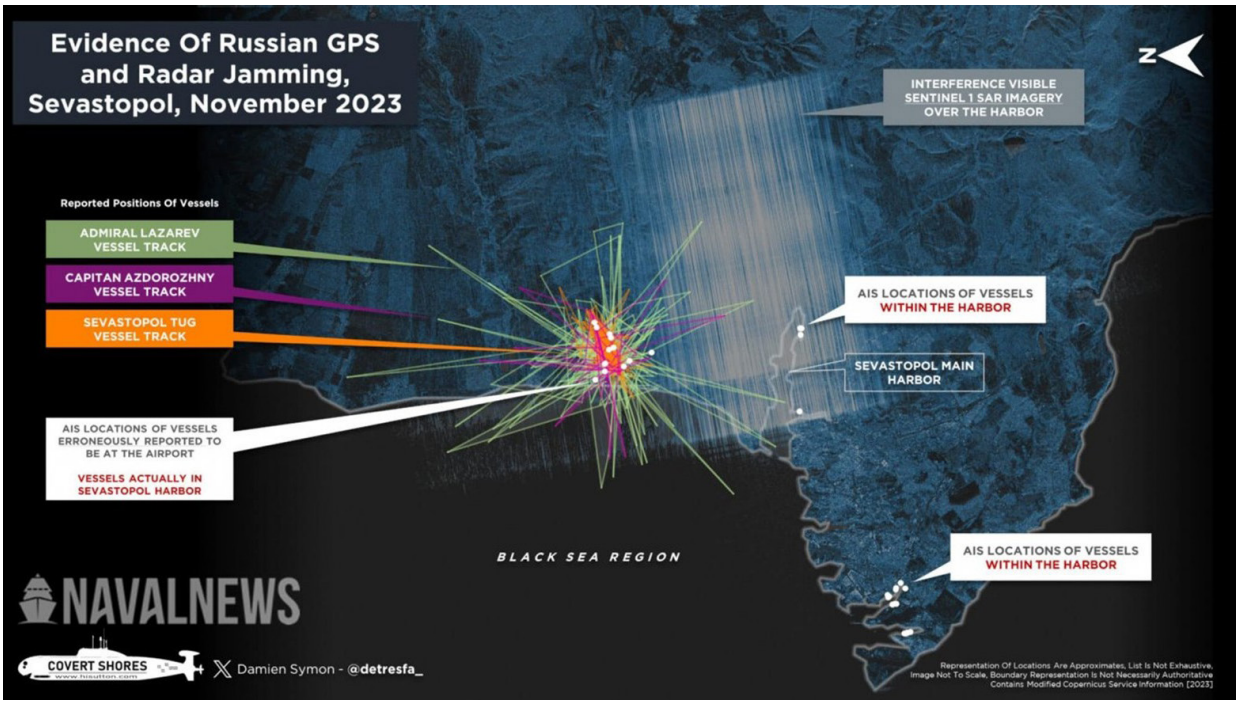
1.1.Literature

A quick search for the occurrence of these signals did not bring up much. Most articles are focused on GPS jamming, especially for some special single cases with prominent figures on a plane (von der Leyen) or air traffic navigation difficulties in countries bordering Russia. However, much less information can be gathered on higher frequencies, like C or X-band.

An article in navalnews started when the first signals were visible on Sentinel-1 satellites in Sevastopol in 2023: *https://www.navalnews.com/naval-news/2023/11/russias-powerful-invisible-defenses-around-sevastopol-rendered-visible/.*

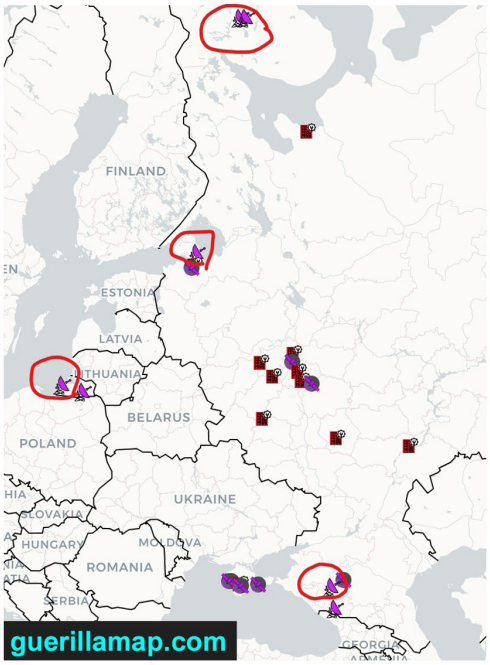
The article suggested the interference is an EW protection for countering UAV's by satellite navigation spoofing, therefore GPS/GNSS spoofing. The spoofing could be seen on ship AIS signals, where several ships near Crimea reported an obvious wrong position. It is interesting that the vessels' false positions were clustered around the international airport. This may indicate that the source of the jamming is there. The article concluded that the C-band signals visible in the Sentinel-1 images were specifically emitted to blind these satellite images and that it just appeared on C-band.

Recent images from TerraSAR-X however also confirm such signals in X-band and we do not think that the emissions are specifically sent to blind satellite imagery, at least not as their primary goal,



Another article from bulgarianmilitary discussed possible emitters after the occurrence in Sevastopol in 2023: https://bulgarianmilitary.com/2023/11/27/unknown-russian-complex-near-sevastopol-creates-strong-interference/.

Their theory was that it was either Voronezh early warning systems or Nebo-M. I think the Voronezh theory can be rejected quite easily given the fact that these systems are stationary and not necessarily near the emitter positions we can observe, at least not at all sites. So maybe they are part of the game, but definitely not entirely:



Mapped locations of Voronezh early warning sensors

An article by Wes O'Donnell (https://wesodonnell.medium.com/a-peek-inside-russias-gps-jamming-playbook-7c02da481009) shows Russia's different EW systems specialized in GPS jamming and spoofing:

Pole-21

21Rather than relying on a single massive transmitter, Pole-21 disperses dozens of small jamming nodes across civilian cell towers or utility masts.
Each node emits noise centered on GPS and other GNSS frequencies.

By linking them together, Russia creates an RF “sprinkler system” that covers entire regions. Kaliningrad bristles with these nodes, and Crimea has hosted clusters as well. A Pole-21 cluster, with dozens of nodes high on towers, can black out areas tens of km wide.

R-330Zh “Zhitel”

For tactical bubbles. This truck-mounted jammer can detect and jam a wide swath of spectrum, from satellite phones to GSM to GPS. Its purpose is to create localized denial zones for advancing units or to protect command posts from drone swarms.

With a range of tens of kilometers, it’s mobile enough to “jam and scoot,” complicating counter-battery or airstrike attempts.

Krasukha-4

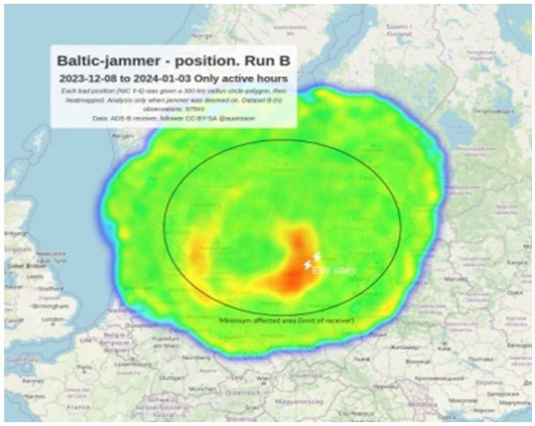
The big iron of Russia's EW forces. Mounted on an 8×8 chassis, it's designed to blind airborne radars like NATO AWACS or US JSTARS. Its primary targets are surveillance aircraft, but the sheer amount of RF power it pours into the ether creates collateral GPS disruption in nearby bands. If you're flying near a Krasukha emission lobe, your satellite navigation is going to have a bad day.

A Krasukha with high-gain panels can project disruption hundreds of kilometers in the right geometry. The former version Krasukha-2 was also widely used to jam radar signals in S band (2.3 GHz–3.7 GHz), the version 4 on the other hand can jam X-band radar.

Tobol (14Ts227)

Strategic level. This isn't a truck at all but a network of fixed satellite monitoring and interference sites across Russia.
Analysts believe at least one Tobol node operates out of Kaliningrad. Unlike Pole-21's brute force or Zhitel's mobility, Tobol provides selective, time-bound interference aimed at adversary satellite links.

In practice, that means Russia can create carefully shaped GPS denial zones without spraying the entire spectrum.



1.2.Frequencies

We can definitely see strong signals in the 3 highlighted bands, and since S-band is right in bet-

Band	Freq range [GHz]	Satellite used	center Freq of satellite [GHz]
P-band	*0.23-1*	*P-SAR*	*0.435*
L-band	1-2	ALOS PALSAR	1.2575
S-band	*2-4*	-	-
C-Band	4-8	Sentinel-1	5.405
X-Band	8-12	TerraSAR-X/ AMSR	9.650/ 10
Ku-band	*12-18*	*AMSR*	*18*

The P-band also shows some artifacts and noise, but it cannot be stated for sure that massive emissions are present like in the other bands. Higher frequencies than X-band do not show any disturbances, at least not at an 18 GHz observation.

What purpose do these frequencies usually have?

L-band
- ADS-B
- GNSS. At around 1.2 GHz sits the GPS frequency, with other providers like the European Galileo in similar frequencies.
- Mobile service and telecommunication

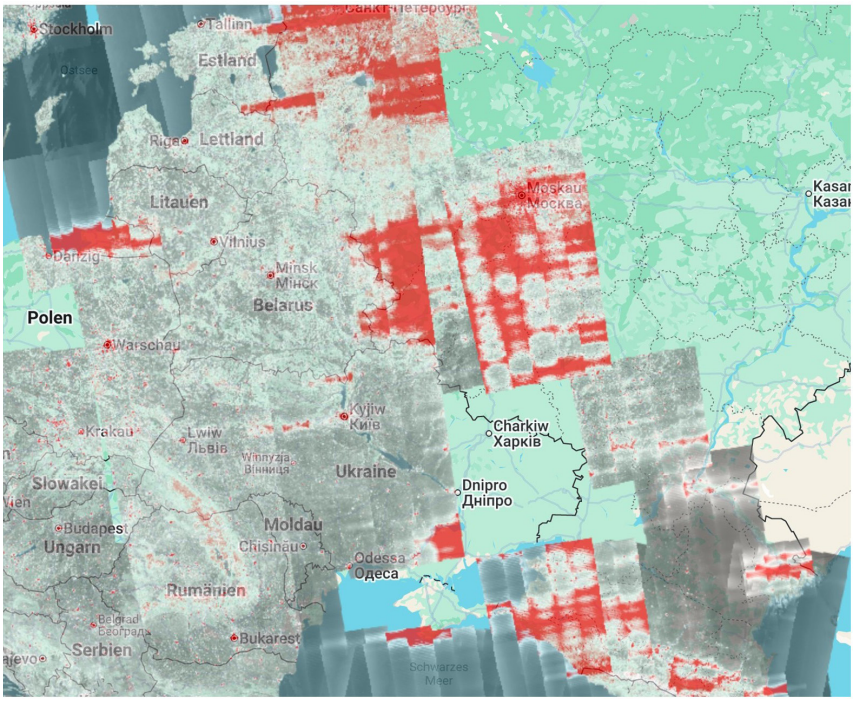
S-band
- Wi-Fi & Bluetooth(2.3 GHz to 2.6 GHz)
- Satellite communications
- Radar Systems
- Satellite imagery, e.g. ALOS PALSAR

C-band
While C-band is used for radar imaging, like the Sentinel-1 satellite, there are other applications working in the same frequencies:

- Radar Systems, e.g. air traffic control radar
- Fixed Wireless Broadband
- Microwave Links
- Wi-Fi or 5G signals, can work in this frequency band
- Satellite communication often works in part of the broader C-band (4.0–8.0 GHz), which is particularly suitable for long-distance communication because it can penetrate the atmosphere and is less affected by weather conditions like rain.

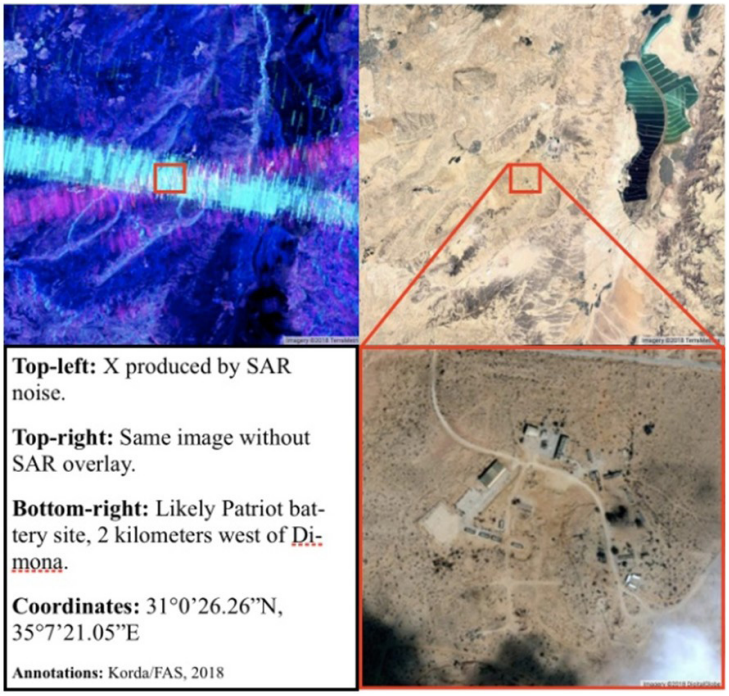
X-band
- Radar Systems, e.g. air traffic control radar or maritime vessel traffic control
- Terrestrial communications and networking
- Space communications, like data downloads and uplinks

L-band and GNSS



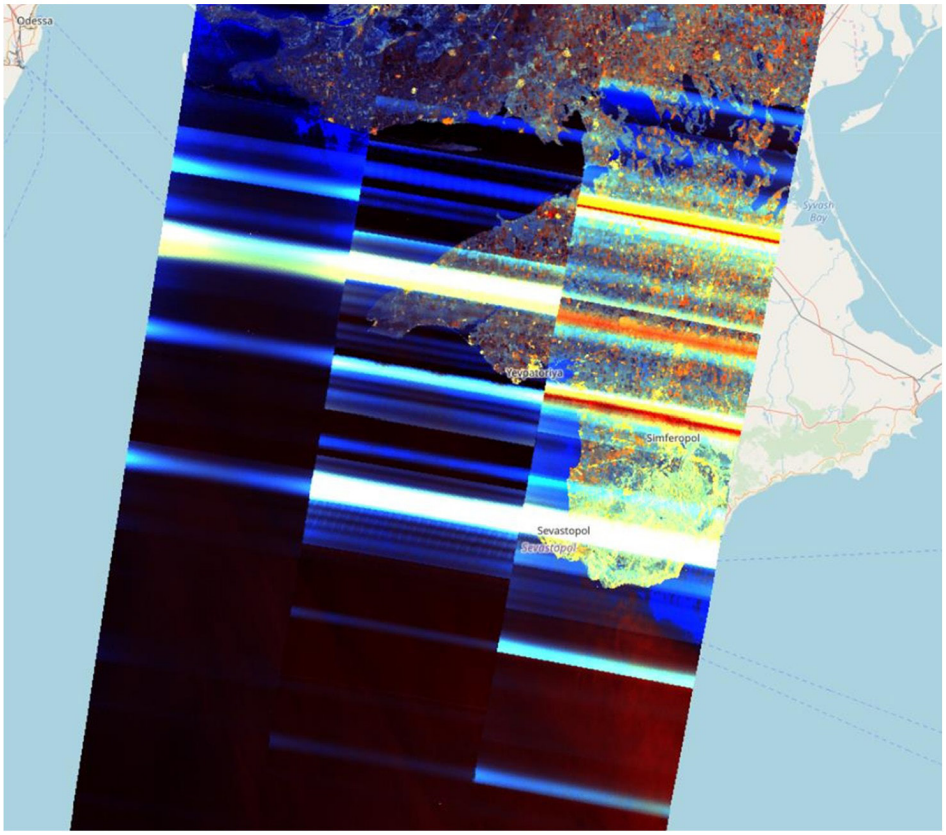
We can observe massive interference in the L-band using the ALOS sensor. Massive, not just in signal strength, but also in area coverage. Basically, the whole Russo-Ukrainian border and Russo-NATO border is covered in L-band interferences. Furthermore, as stated earlier, we can back that claim by GPS interferences measured in these areas, because GPS works in L-band too.

C-band



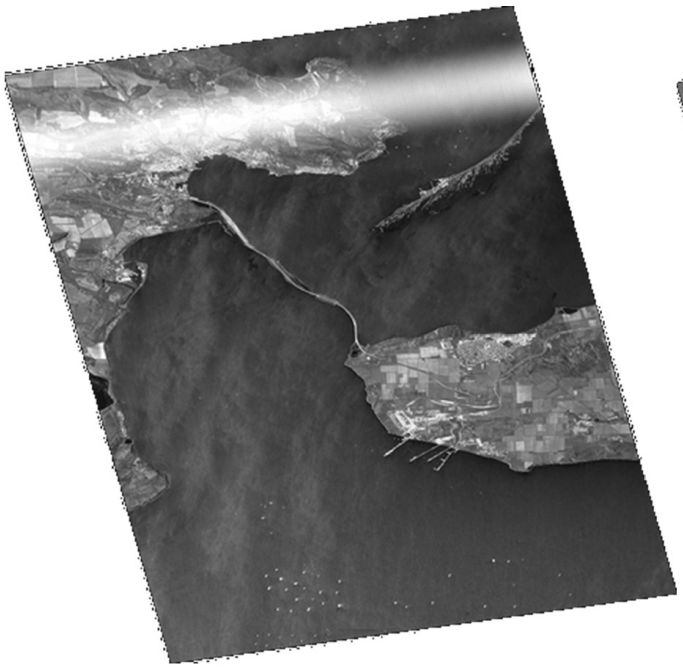
Sentinel-1 beautifully shows the massive signal interference, e.g. on Crimea. This amplitude is something completely new, there were some analyses earlier, pre Ukraine war. For example a Patriot air defense system could be detected in Israel using Sentinel-1 images, but the signals detected there were much weaker.

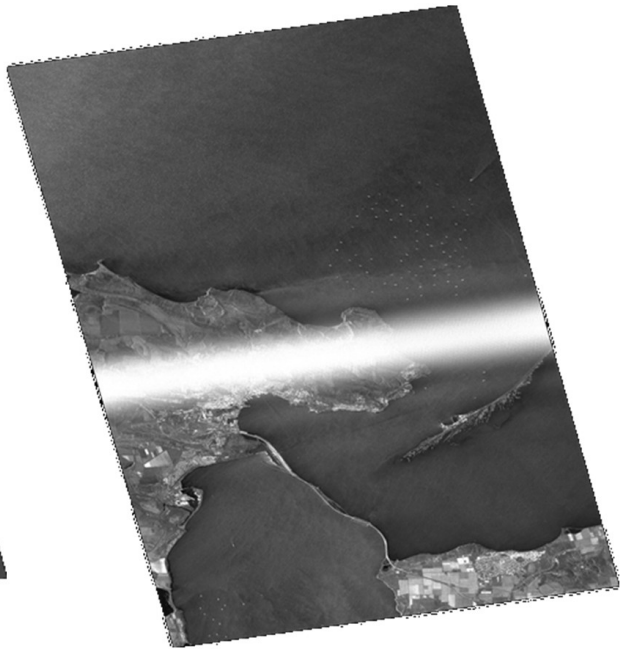
The signals on Crimea are magnitudes stronger:



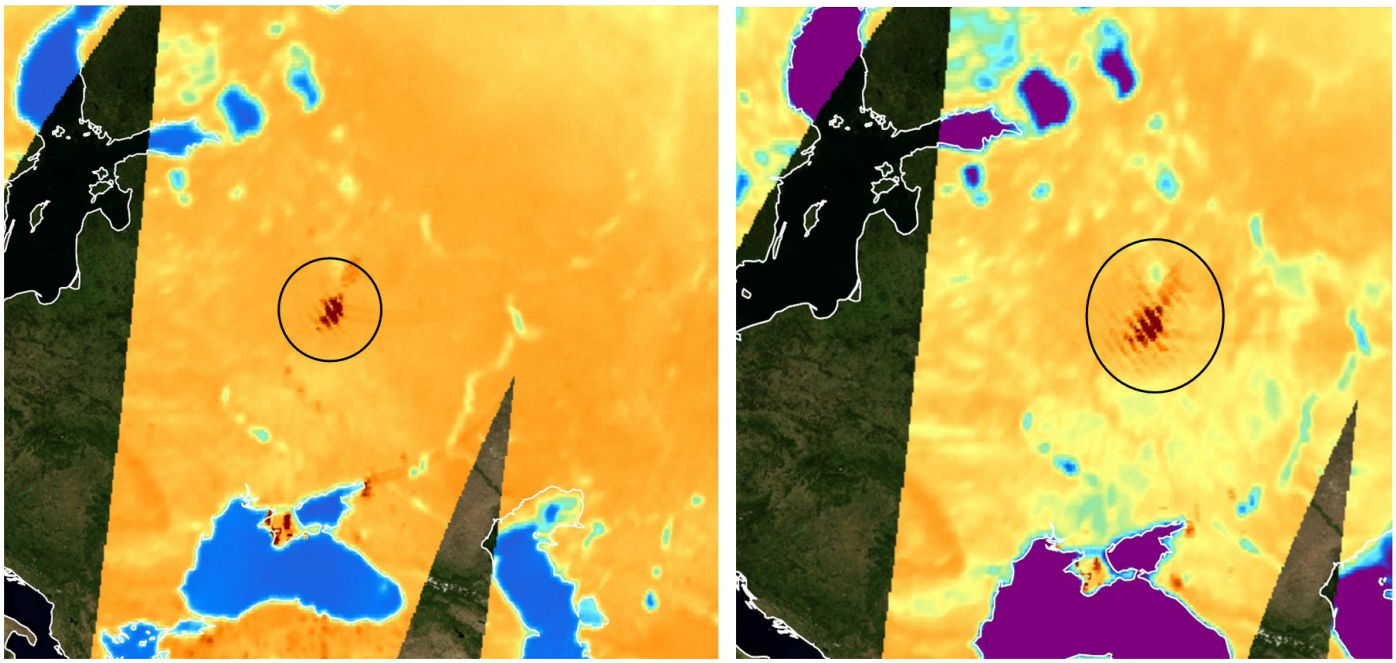
X-band

TerraSAR-X imagery shows more or less the same interferences we see in C-band, here an example from the Kerch Strait.



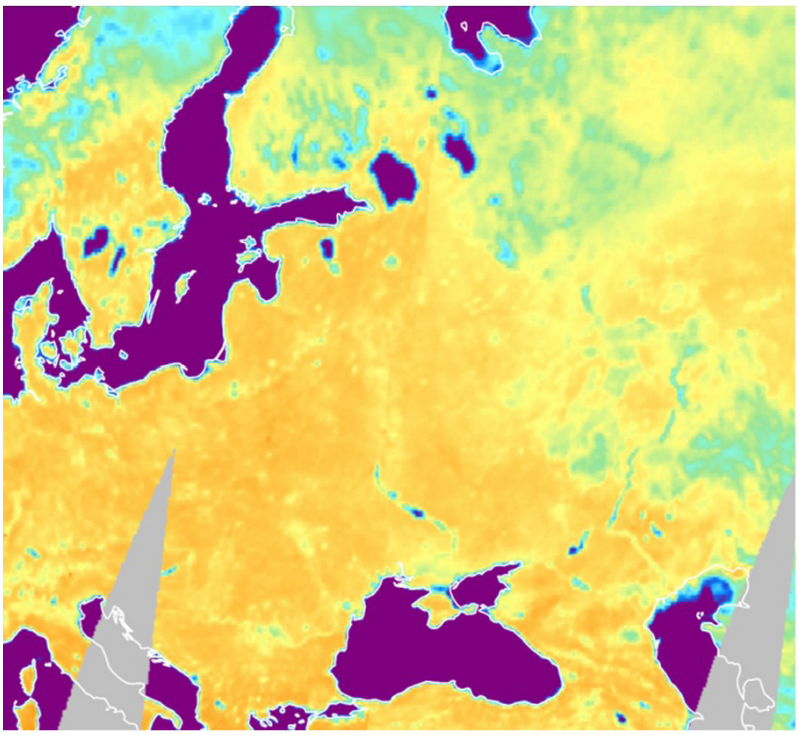


The Japanese AMSR is passive radar satellite with a very coarse spatial resolution, nevertheless, the disturbances are so strong, they are visible even then, here in 10GHz in the Tula region, south of Moscow:



Higher than 10 GHz?

The same sensor (AMSR) also has bands with higher frequencies, here an example with 18 GHz:



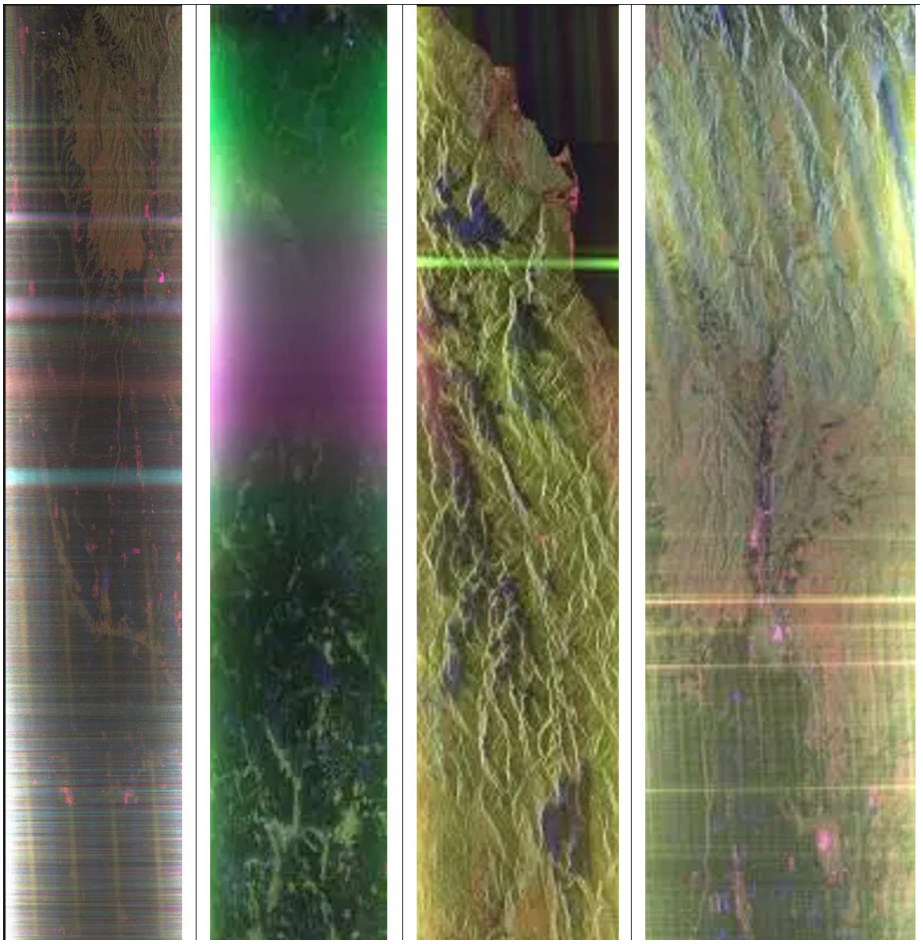
Nothing is visible on the AMSR images over 10GHz, giving us an upper boundary for EW activity in X-band. However it is hard to say with such a coarse resolution, pretty sure there is some interference, maybe just some very local ones, in higher frequencies too.

Lower than L-band?

There is a new ESA P-band sensor onboard the “Biomass” satellite since 2025, and there are some images near the typical jamming areas in Russia. These P-band images show some noise, but we are not sure if it’s really EW related.

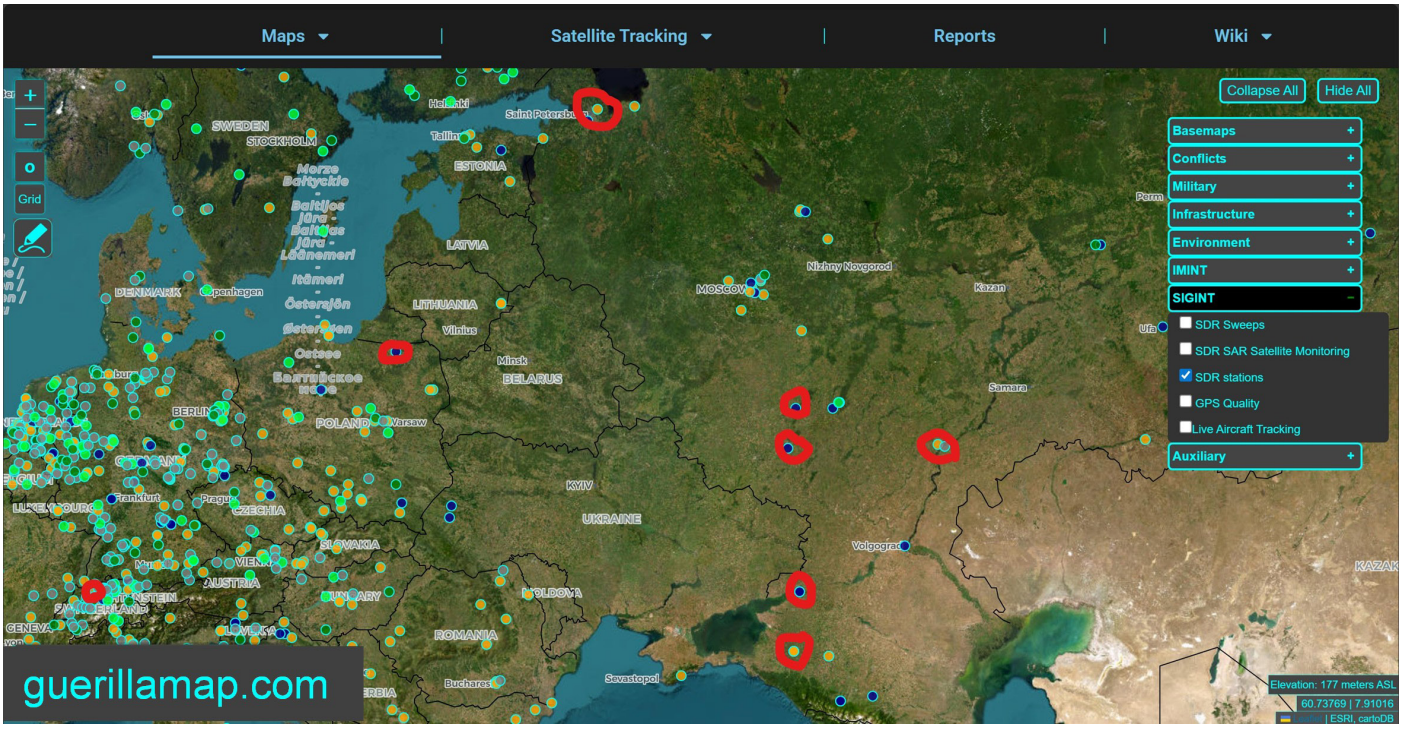
At least some reference images over South America did not show such artifacts and therefore it might really be related to EW, but we can also say IF there is some jamming/ spoofing in P-band, then it must be much weaker than in C or L band and is then probably related to drone control and data transmission jamming, since that typically happens in the 433 MHz, 915 MHz or bluetooth/ wifi range.

Here some examples from the P-SAR sensor in Russia near the Ukrainian border:

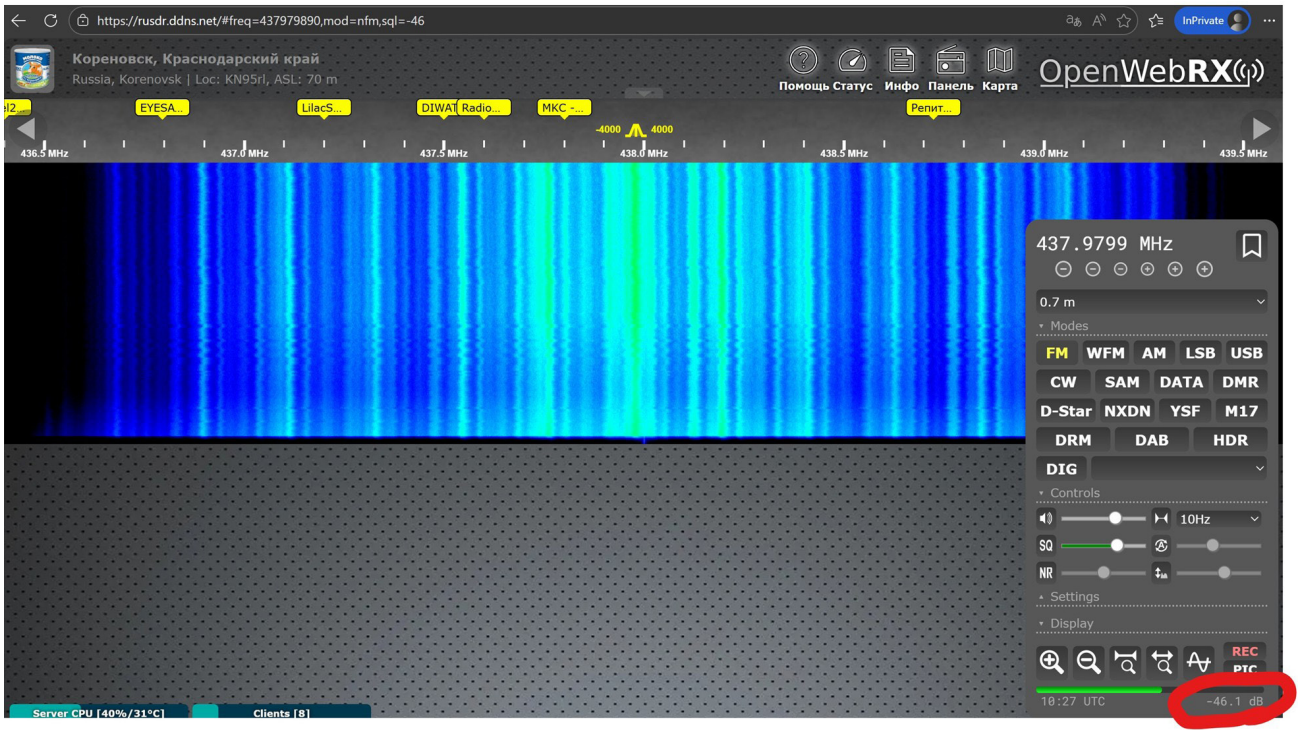


We also started to listen to several SDR (Software Defined Radio) stations inside these jamming areas and it did not show much interference in the P-band either. If at all, we can maybe see some noise in the GPS L5 area near St. Petersburg (but that is again L-band) and maybe, just maybe in the 433 MHz area in Korenovsk:

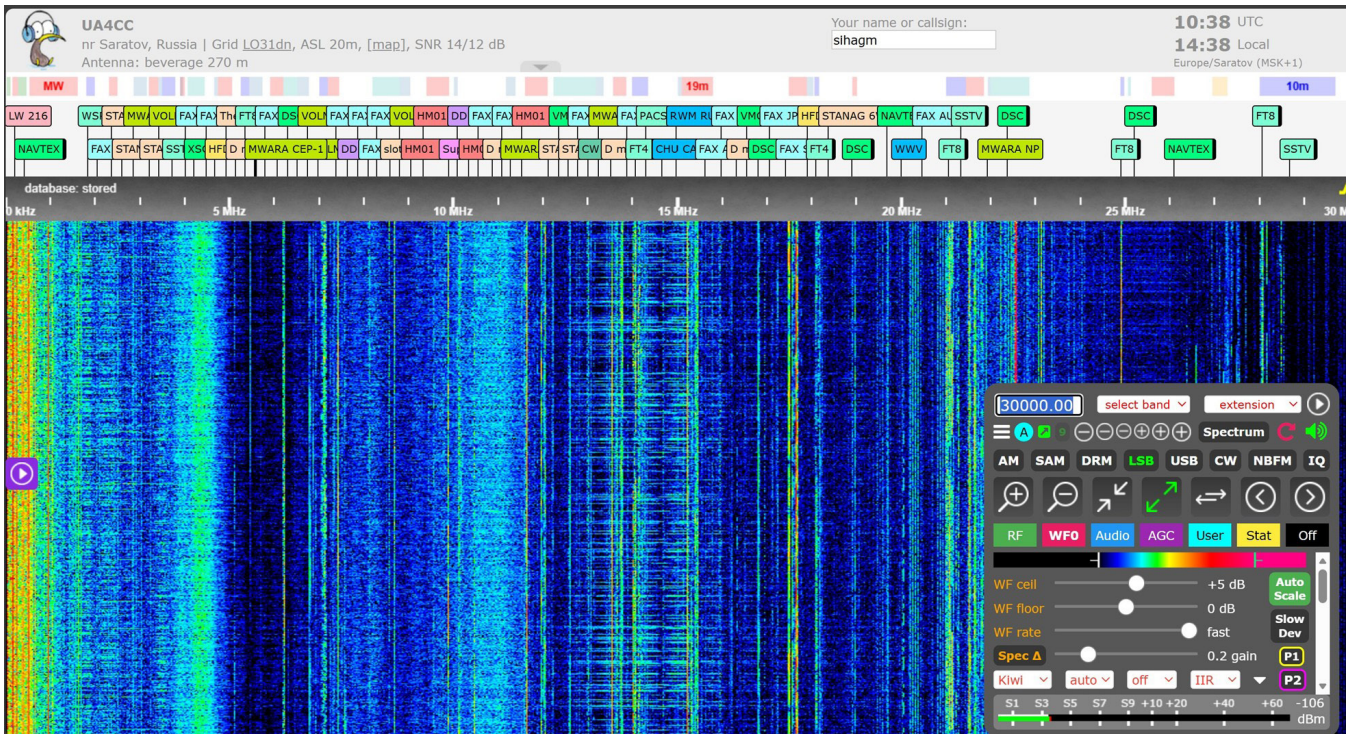
SDR stations investigated:



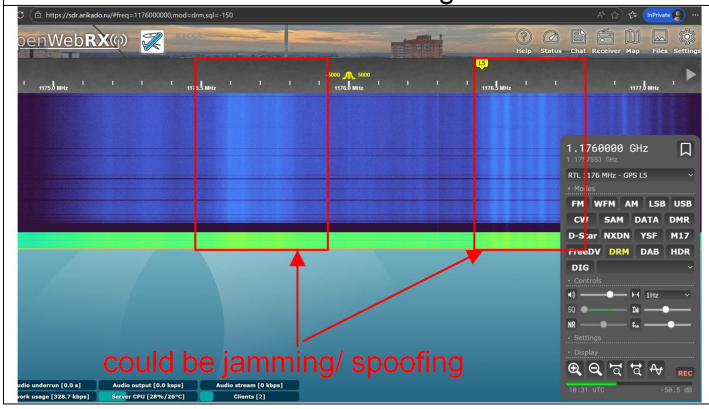
Korenovsk, 433MHz, looks indeed like a jamming signal, but the amplitude is low (-46 dB):



No jamming in Saratov, low frequency, even below P-band:

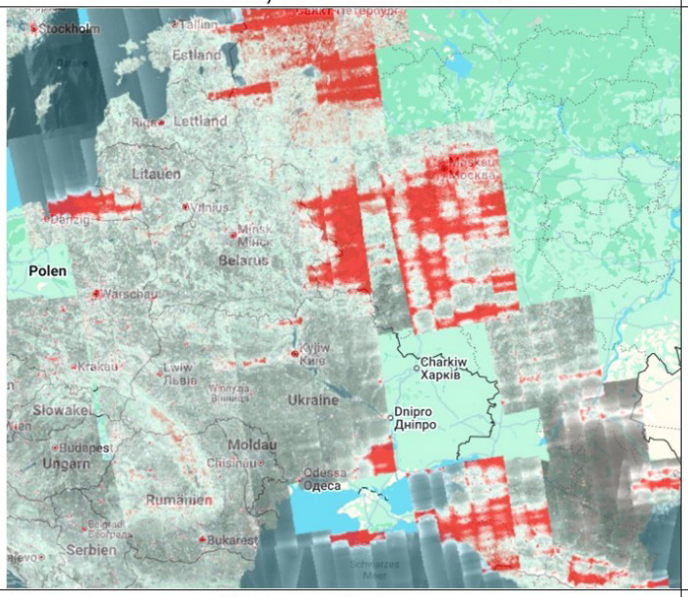
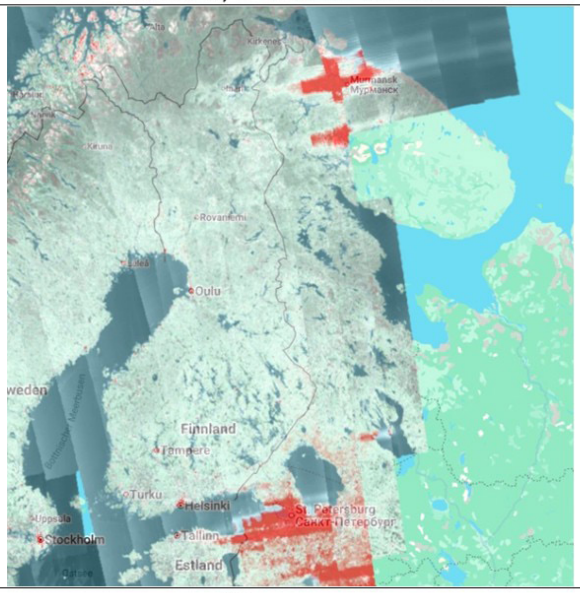
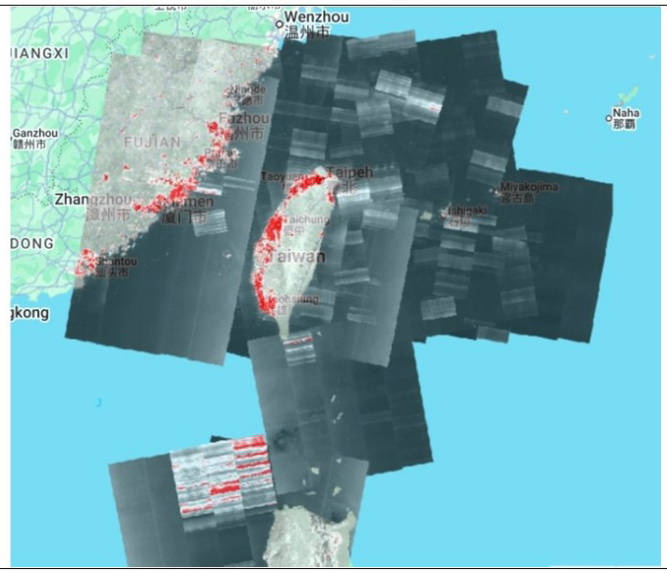
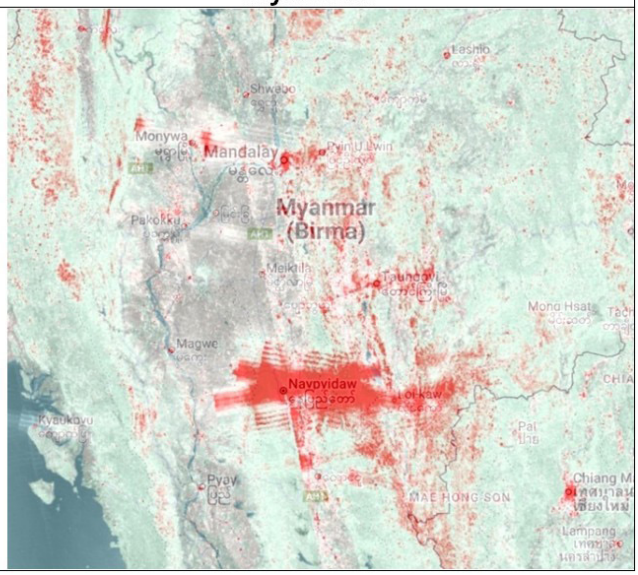


Noisier GPS (L-band) in St. Petersburg compared to Switzerland. Note that in Switzerland we see a clear signal (brighter line) for the GPS frequency, whereas in St. Petersburgthis signals disappear inside these signal blocks with a wider bandwidth:

St. Petersburg	Switzerland (for comparison)
	

1.3.Spatial distribution

L-band disruptions were visible in Russia, China (specifically surrounding Taiwan) and Myanmar:

Russia, Ukraine border	Russia, Finland border
	
China - Taiwan	**Myanmar**
	

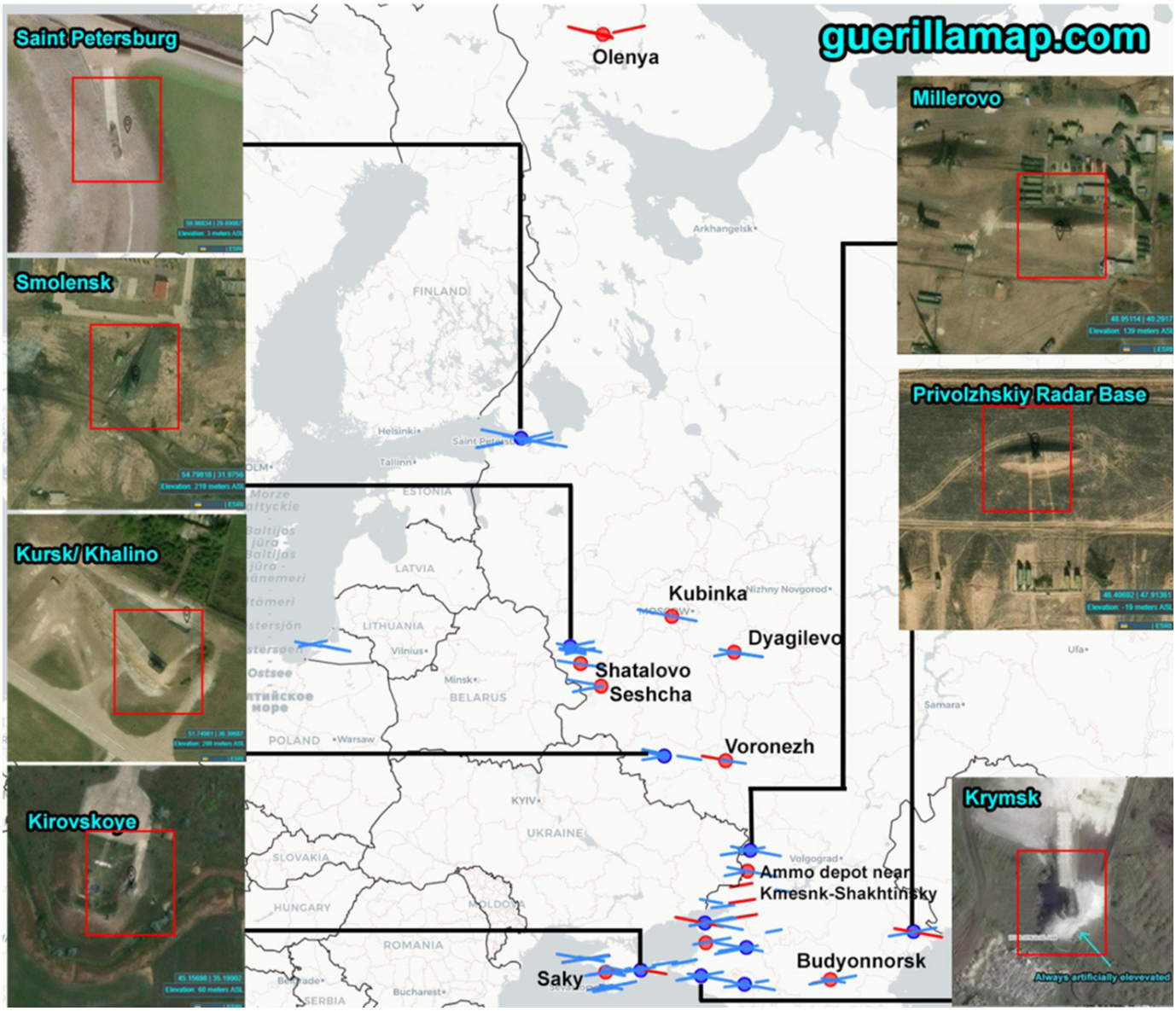
Around Taiwan the signals were mostly, or maybe exclusively sea-based, with some jamming possibly coming from Taiwan itself and not just PLA-sourced (PLA = People's Liberation Army, the Chinese military). The largest and most intense signal block is further south, northwest from the Philippine city Laoag in the contested South China Sea.

In Myanmar the strongest signals are at the city of Naypyitaw, one of the Junta's strongholds. In fact, all the emissions are coming from Junta controlled territory. There is for example some weaker signals observable over the capital of Mandalay.

The C-band, Sentinel-1 analysis shows more or less the same areas, but given the better spatial resolution and higher frequency, we can estimate the approximate emitter location much better.

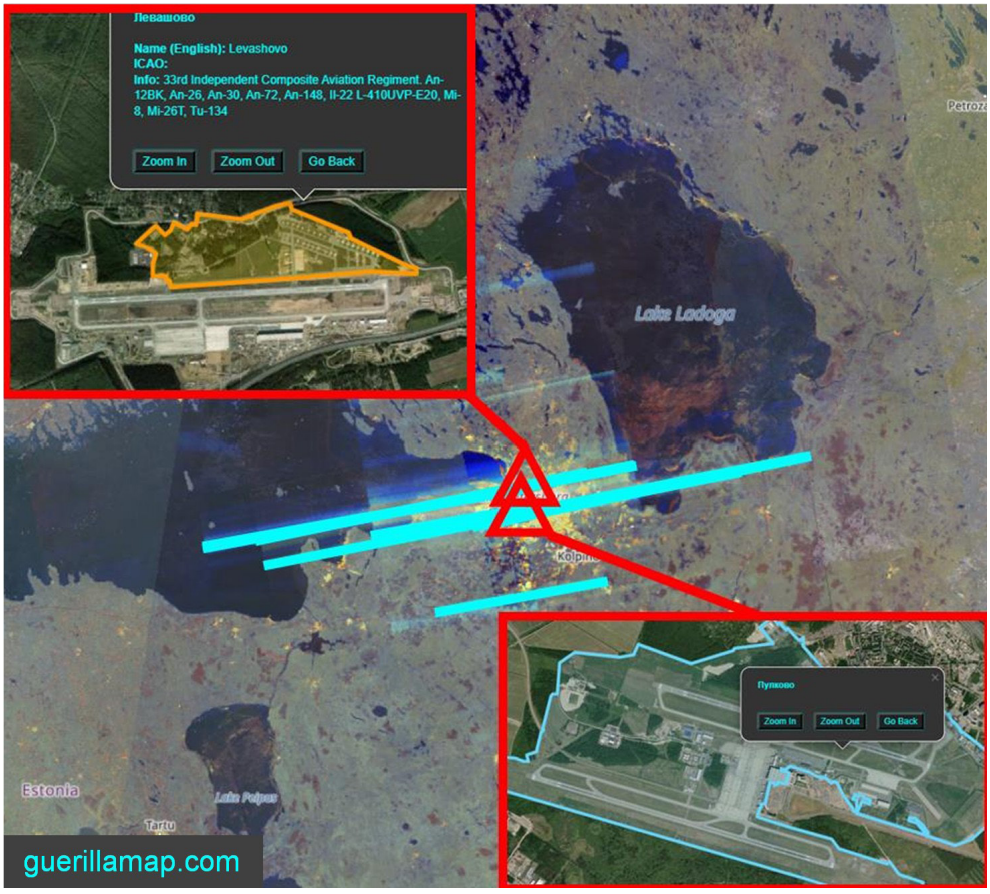
Here an overview of the 2025 emissions:

We can conclude that these C-band EW, or radar systems, must be at the following locations (where the signals intersect). > **Link** < to the map, blue markers are high emission areas and high-resolution-satellite-imagery confirmed locations of Pantsir air defense systems (we will talk about that later), red ones are emitter approximations according to the measured radar signals.

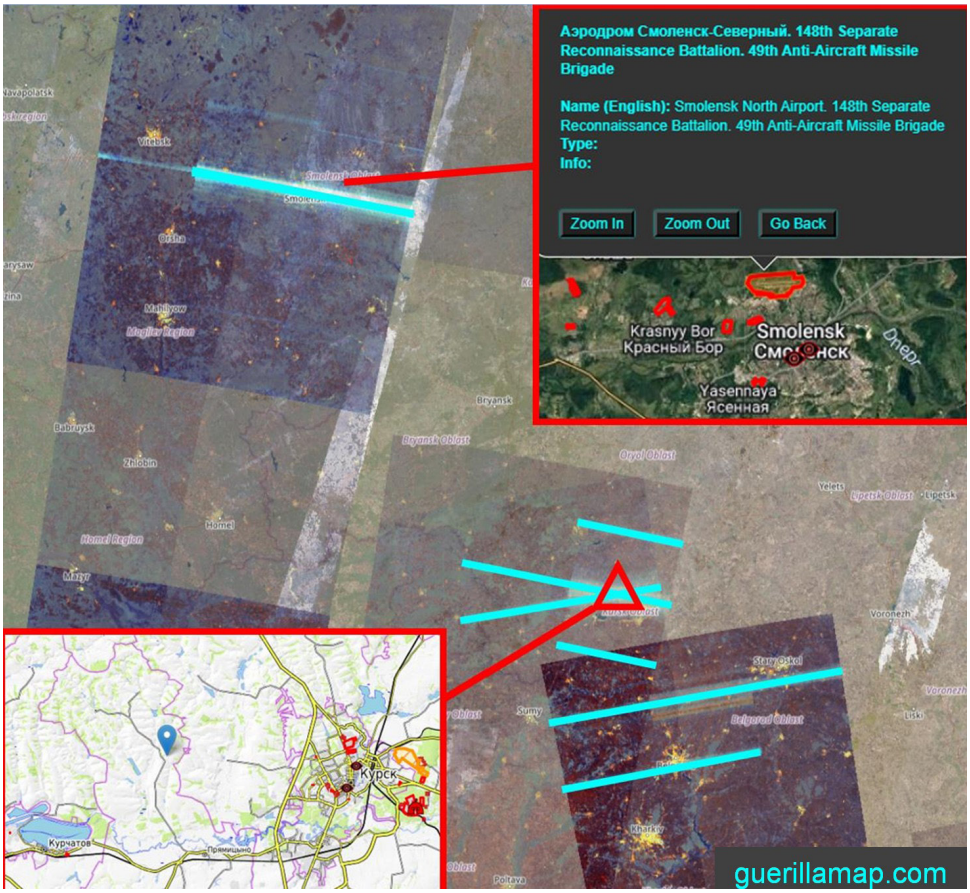


Crimea Saky airbase, Sevastopol (likely 2 systems), the 15th coastal artillery near Cape Fiolent and one near the Kerch Bridge.

We can also find these signals along other war-important parts of Russia, namely near St. Petersburg, Smolensk, Kursk and east from the sea of Azov and more precise **Levashovo airbase and St. Petersburg international airport,**



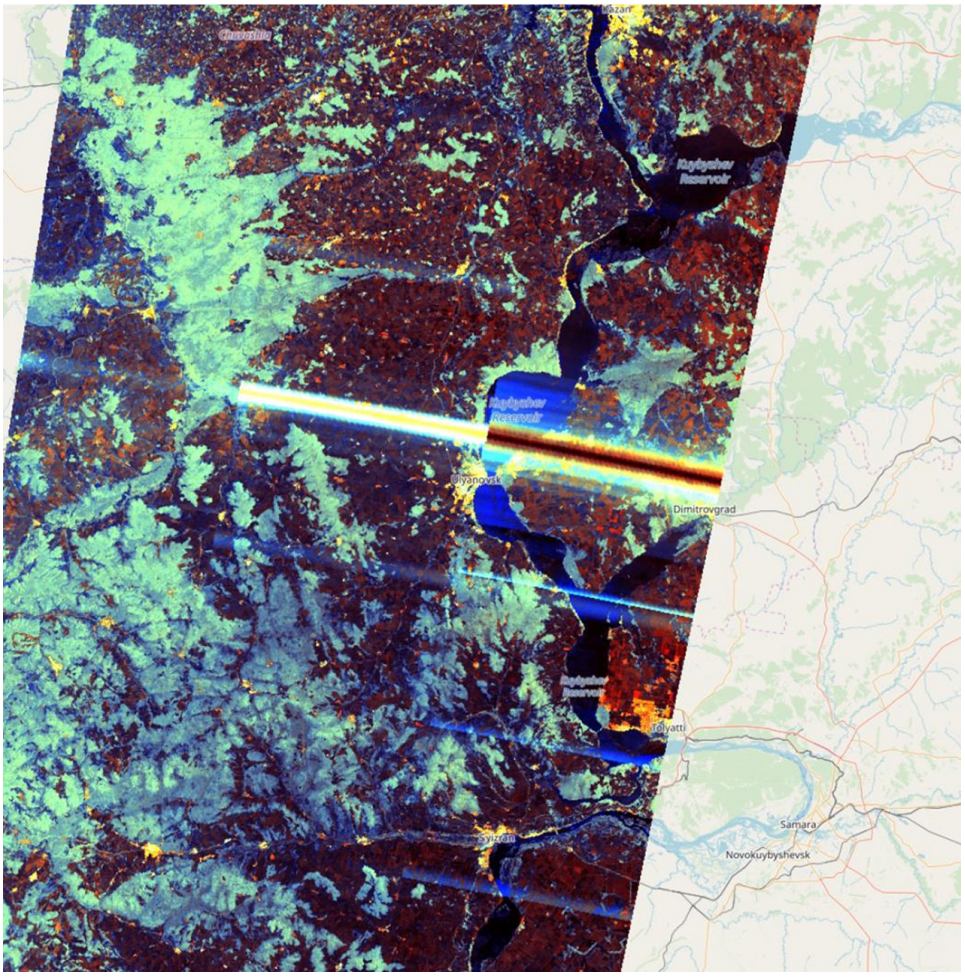
Smolensk north airport, somewhere in the open west of Kursk city,



the separate Electronic Warfare Center No.1270 Rostov, **Primorsko airbase and Krymsk airbase,**

Moscow near Chkalovsky military airbase,

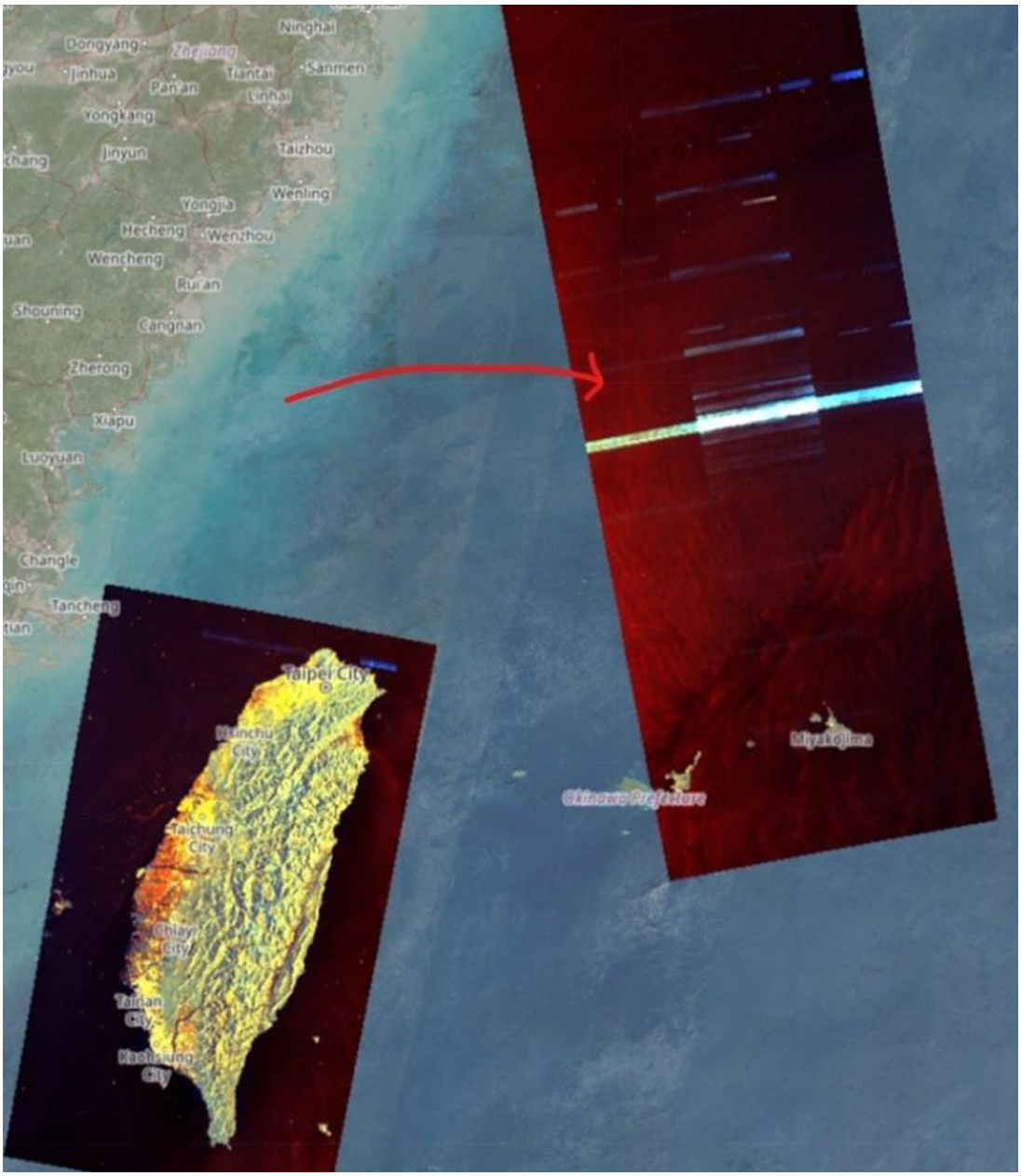
and somewhere near Ulyanovsk, probably at the nearby airbase.



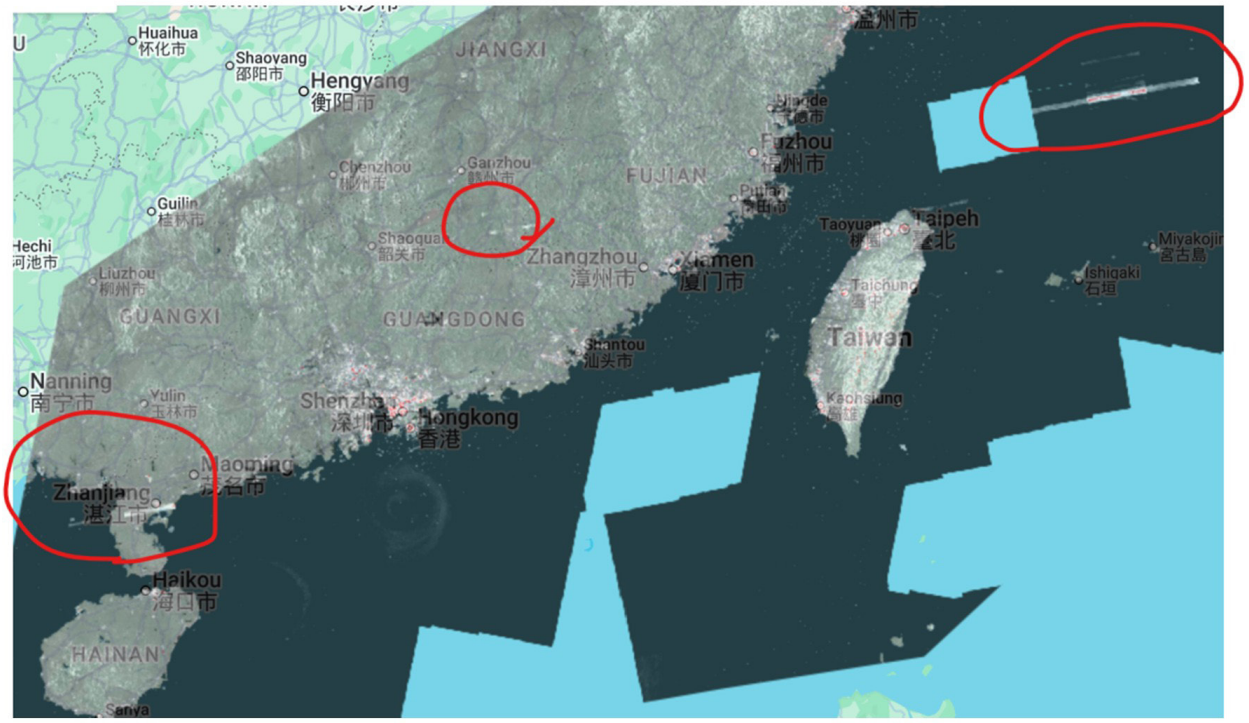
One relatively new occurrence of such signals can be found at the Olenya airbase in the Murmansk Oblast, near the Finnish border. The Olenya air base was one of the 5 air bases, that got struck by Ukrainian FPV drones on the 1st of June 2025. Several strategic bombers were destroyed during the strike.

Taiwan

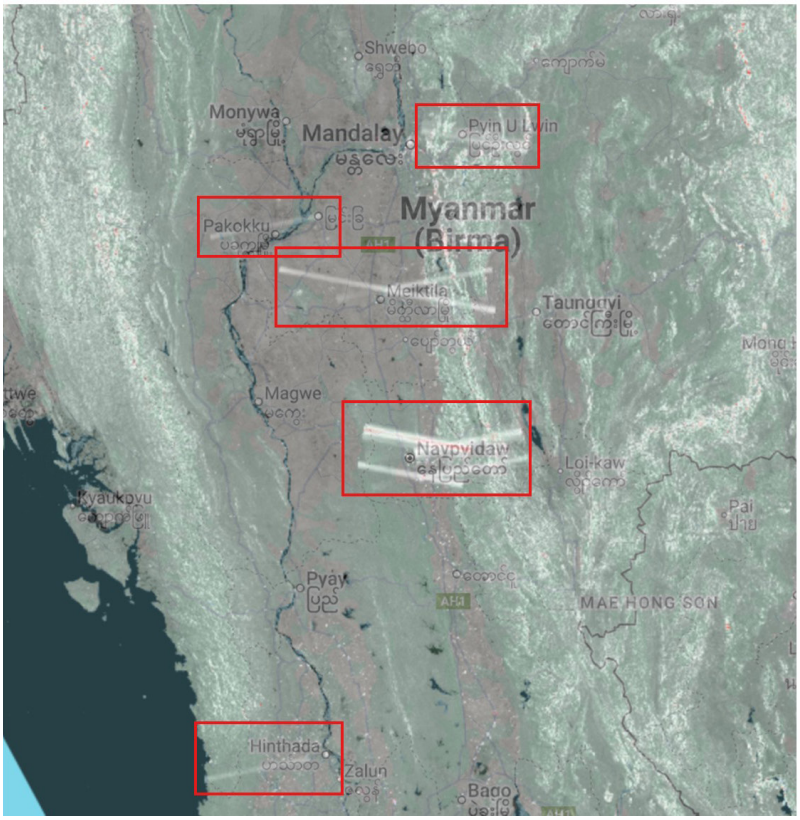
Not just L-band interferences, but also C-band signals can be found in the sea around Taiwan as we did see in Russia. The signal in the following case must have been emitted from a ship given the location. Most probably, it is a Chinese military ship and part of a blockade exercise around Taiwan.

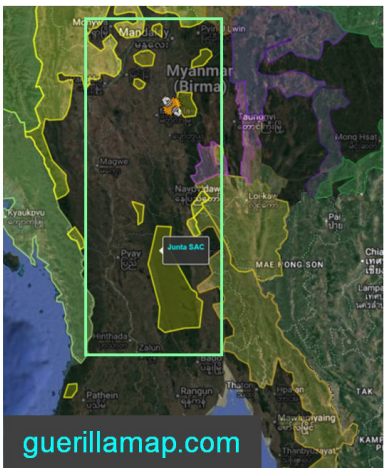


Two other Chinese C-band signals can be detected, one near the Zhanjiang naval base and Suixi airbase, the other near Xunwu.



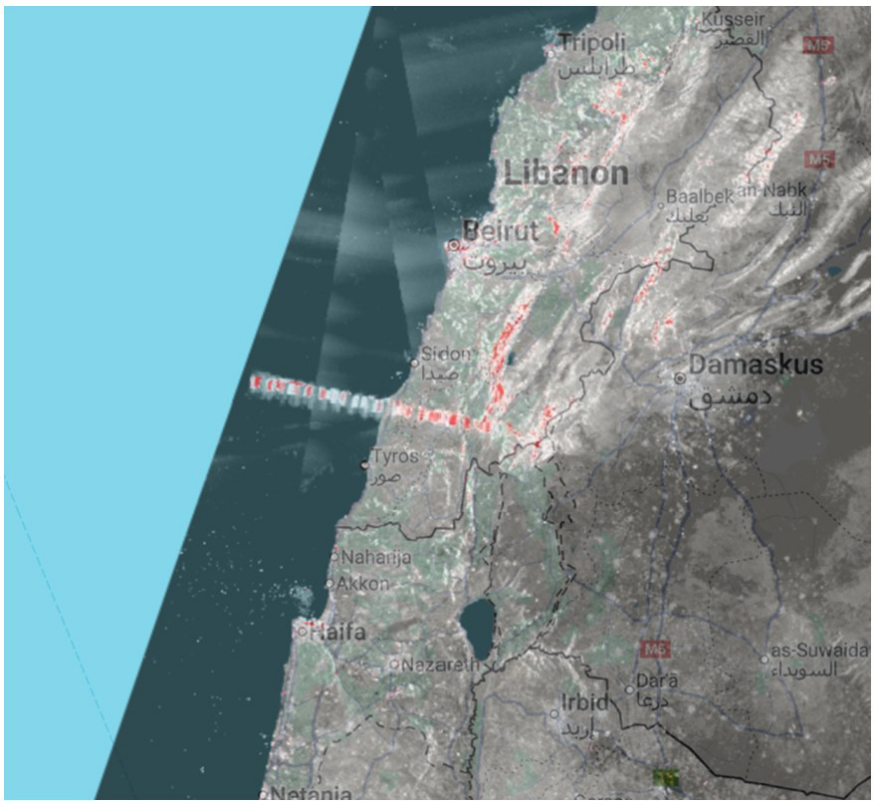
In Myanmar we have a similar picture as for the L-band with a maximum in Naypyitaw and some in Maktila and Hinthada, also here exclusively in Junta controlled areas (shown on the right).





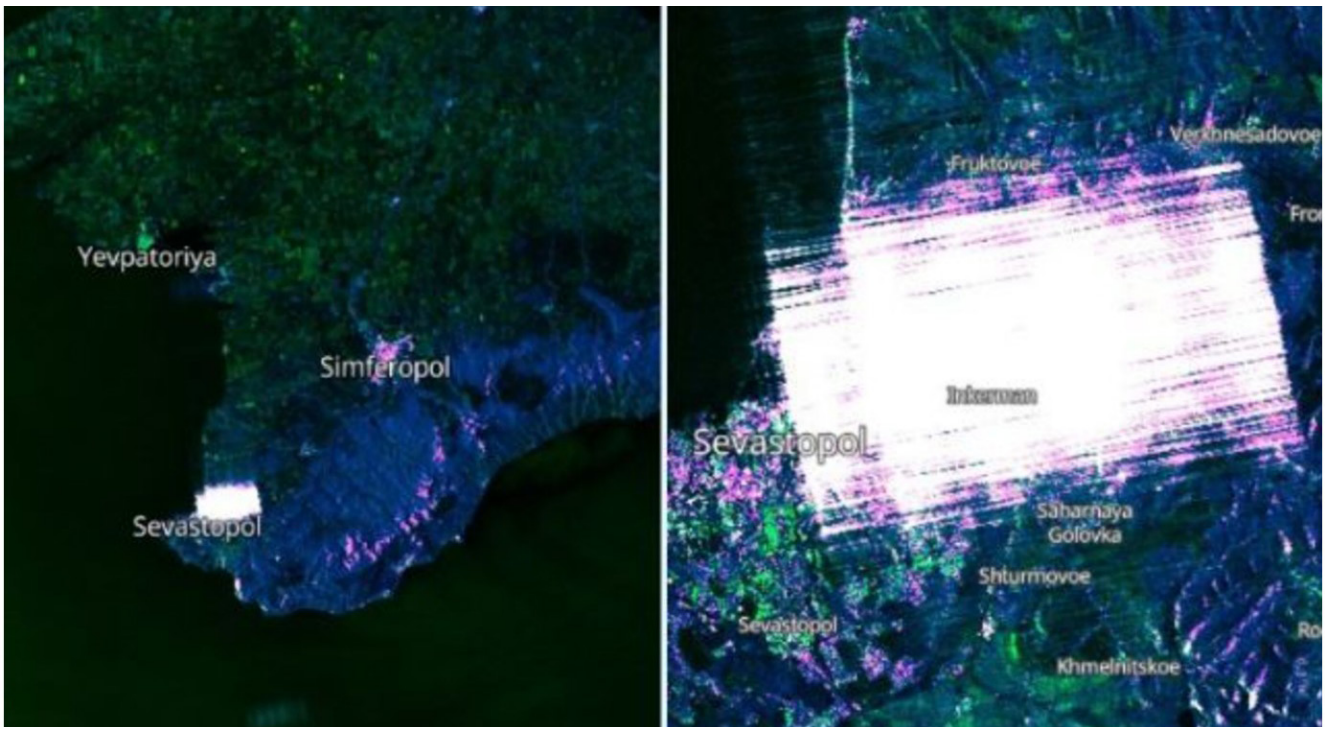
Lebanon

There is one signal burst visible in Lebanon, right between Tyros and Sidon, but that was the only such occurrence.



1.4.Temporal changes

It all started with a single location in Sevastopol in February 2023:

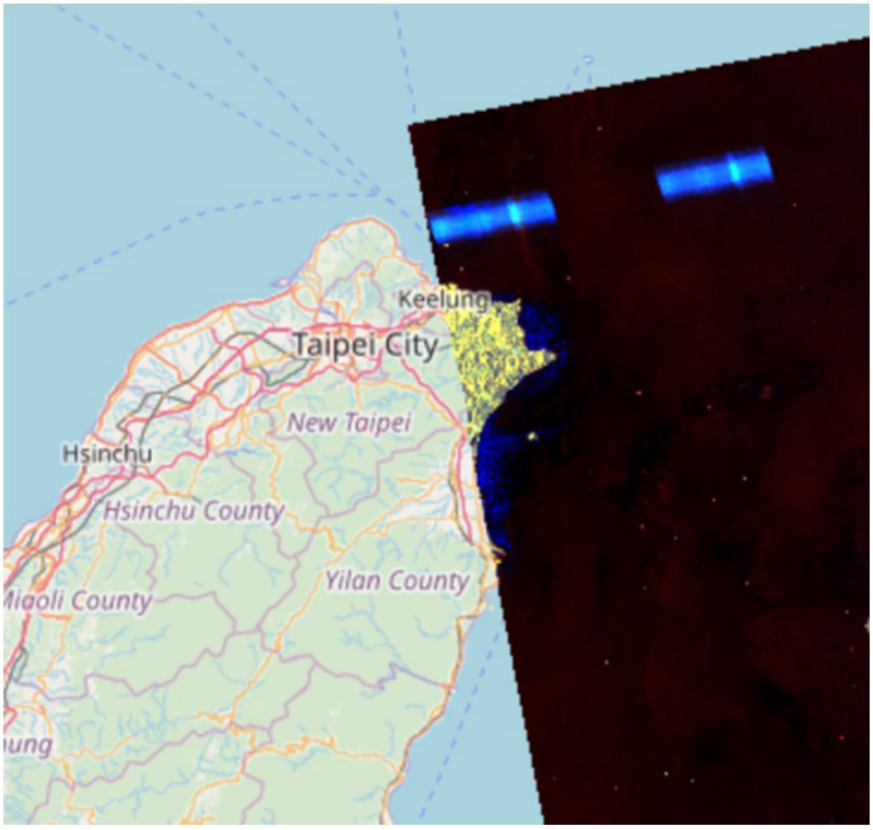


Then these signals in C-band along with more frequent GPS-jamming became more and more frequent and spatially abundant. First, especially the occupied Crimea was affected, then more and more adjacent regions to Ukraine, like Kursk, Belgorod, Voronezh and Rostov too. In the end, there were also signals further away from Ukraine, namely St. Petersburg, Murmansk, or Astrakhan.

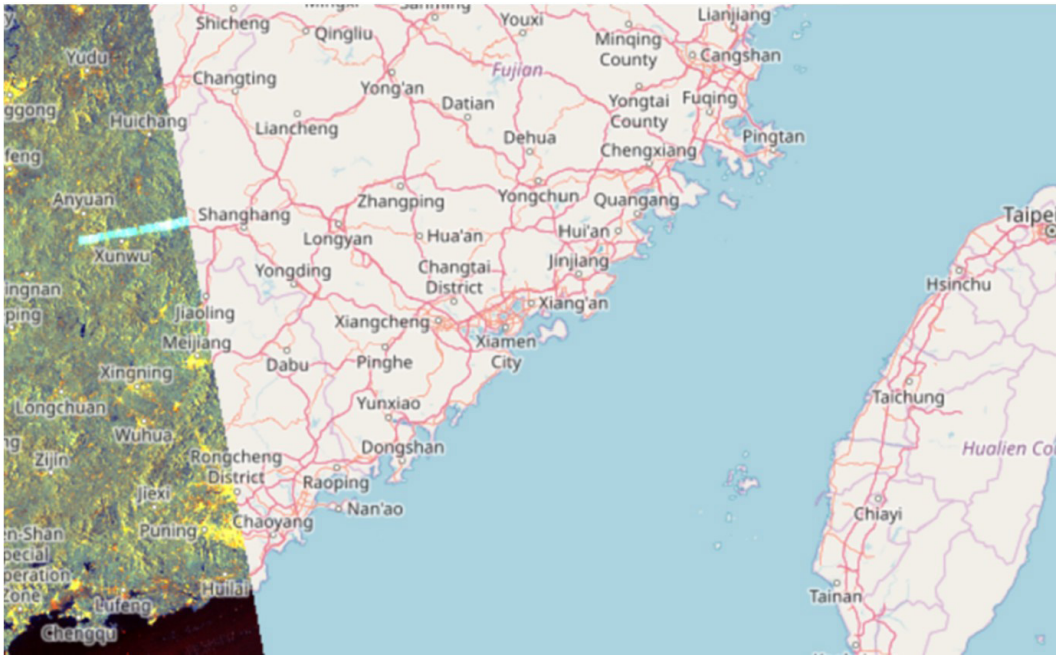
Especially throughout the first half of 2025 we saw a massive increase in such strong signals. But then in the second half of 2025 there were also some significant reductions observable, namely on Crimea, where Ukrainian strikes likely destroyed many radar and EW systems. By now, an overall reduction can be seen, where the peak in emissions was maybe around April 2025.

China – Taiwan

The emissions around Taiwan can be directly linked to PLA exercises in the area, for example here on the 30th of November, during a quite spontaneous PLA exercise when Taiwan's president had a stopover in Hawaii:



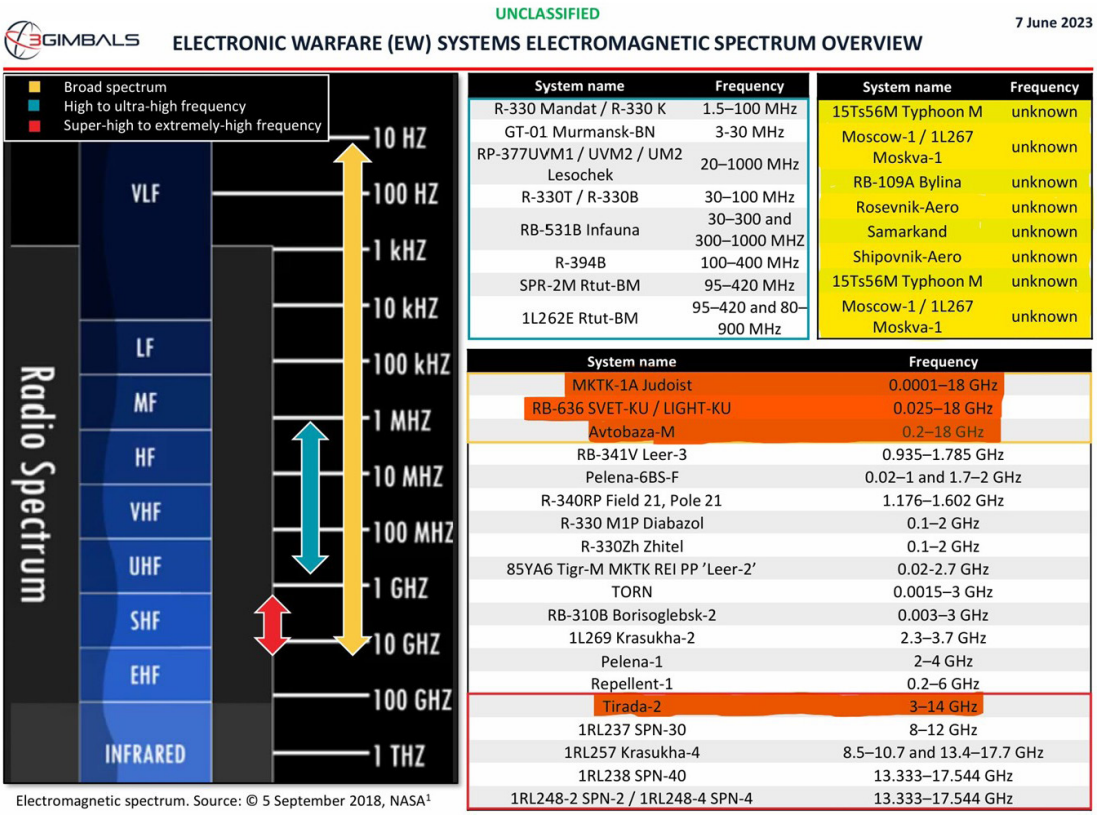
Or here, ahead of the latest “Joint-Sword-2025” exercise from the 26th December 2025:



2.What we hypothesize

2.1.Possible emitters

There is an amazing report from “3Gimbals” listing Russian EW systems from 2023:



System name	Frequency
R-330 Mandat / R-330 K	1.5–100 MHz
GT-01 Murmansk-BN	3-30 MHz
RP-377UVM1 / UVM2 / UM2 Lesochek	20–1000 MHz
R-330T / R-330B	30–100 MHz
RB-531B Infauna	30–300 and 300–1000 MHZ
R-394B	100–400 MHz
SPR-2M Rtut-BM	95–420 MHz
1L262E Rtut-BM	95–420 and 80–900 MHz

System name	Frequency
15Ts56M Typhoon M	unknown
Moscow-1 / 1L267 Moskva-1	unknown
RB-109A Bylina	unknown
Rosevnik-Aero	unknown
Samarkand	unknown
Shipovnik-Aero	unknown
15Ts56M Typhoon M	unknown
Moscow-1 / 1L267 Moskva-1	unknown

System name	Frequency
MKTK-1A Judoist	0.0001–18 GHz
RB-636 SVET-KU / LIGHT-KU	0.025–18 GHz
Avtobaza-M	0.2–18 GHz
RB-341V Leer-3	0.935–1.785 GHz
Pelena-6BS-F	0.02–1 and 1.7–2 GHz
R-340RP Field 21, Pole 21	1.176–1.602 GHz
R-330 M1P Diabazol	0.1–2 GHz
R-330Zh Zhitel	0.1–2 GHz
85YA6 Tigr-M MKTK REI PP ’Leer-2’	0.02-2.7 GHz
TORN	0.0015–3 GHz
RB-310B Borisoglebsk-2	0.003–3 GHz
1L269 Krasukha-2	2.3–3.7 GHz
Pelena-1	2–4 GHz
Repellent-1	0.2–6 GHz
Tirada-2	3–14 GHz
1RL237 SPN-30	8–12 GHz
1RL257 Krasukha-4	8.5–10.7 and 13.4–17.7 GHz
1RL238 SPN-40	13.333–17.544 GHz
1RL248-2 SPN-2 / 1RL248-4 SPN-4	13.333–17.544 GHz

Notably the Russians have a huge arsenal of different, domestically produced EW systems.

If we think of a single transmitter being responsible for all these emissions (which we don't), then there are just a few systems capable of emitting in such a large frequency range. We have marked the systems in red in the graphic above. So theoretically it would be somewhat possible, systems like the Rb-636 or the Tirada-2 have a huge frequency range, but it is much more likely that there are several systems responsible for all the emissions we see. Furthermore, systems like the Avtobaza-M can detect signals in a huge range, but cannot transmit or jam in the same wide spectrum. And of course, Russia is using everything it has in respect to EW in this conflict, and that also includes radar detection and communication systems and not just EW. So when it comes to a full scale war we have to imagine all these systems being in service in an integrated electromagnetic defense web, each with their respective advantages and functions.

As stated before, some analysts focused on the following systems:

C-band : **Voronezh, Nebo-M** (actually uses VHF, UHF, L and X band, but is maybe part of the game)

GPS: **Pole-21, R-330Zh "Zhitel", Krasukha-4, Tobol (14Ts227)**

These systems are definitely to consider, yes, but there are some more candidates.

The **96L6 radar,** which is usually part of the **S-400** air defense systems is a likely candidate too, as it reportedly works in C-band.

Pantsir air defense

The Pantsir system uses different frequencies: K-band, X-band, Ku-band, L-band, and S-band for different purposes, but officially no C-band. C-band is right in between the S and X-bands and is also used in other air defense systems, such as in the US-made Patriot system.

So we can explain some interferences in the X-band we have seen before with Pantsir systems maybe and maybe even some interferences in C-band. The thing why I am so obsessed with these Pantsir systems is that they can be found on high resolution images on the right time and at most of the sites where we have seen the C-band emissions:

And they are definitely Pantsir-type systems, as this image from Kursk/ Khalino Air Base confirms:

Here the other candidates from the 3Gimbals analysis:

Whole spectrum, from L- to X-band:

UNCLASSIFIED

3GIMBALS

7 June 2023

RB-636 SVET-KU/SVET-VSG

Name: RB-636 Svet-KU/Svet-VSG[168]
Name, Russian: РБ-636 Свет-КУ/Свет-ВСГ
Other names: RB-636AM2 Svet-KU[169]
Other names, Russian: РБ-636АМ2 Свет-КУ
Purpose/use: Carrying out SIGINT activities and jamming radio and radar signals within the frequency range from 25 MHz up to 18 GHz; tracks variety of emissions and calculates source coordinates. Capable of autonomously jamming the GSM, CDMA2000 and UMTS cellphone signals[170]
Bandwidth/frequencies: 0.025–18 GHz[170,171]
Range/antennae ranges: Unknown
Variants: RB-636AM2 Svet-KU complex, based on the Ford Transit van[169]
Approximate date of adoption to Russian military: Svet-VSG 2010, Svet-KU 2012[168,170]
TTPs used to counter system: Unknown
Additional information:
- Composed of the Svet-VSG stationary antenna post of electronic intelligence with a control point and the Svet-KU mobile complex of radio for radio control and protection of information from leakage through technical channels of wireless communication[168]
- Can interact with the automated complex technical control point (APU CPC)[168]

RB-636AM2 Svet-KU mounted on KamAZ-4350 two-axle chassis. Source: © 25 October 2017, Defense Express[171]

Table Sources: © 5 May 2017, Defence24.com[170] 2023, Вооружение.рф[172] 25 October 2017, Defense Express[171]

Performance Specifications	
Frequency range [GHz] [170,171,172]	0.025–18
Simultaneous analysis and direction-finding bandwidth [MHz][172]	≥ 20
Scanning speed when analyzing frequency band loading [MHz/s][172]	≥ 500
canning speed for space-energy detection [MHz/s][172]	100
Noise figure [dB][172]	12
Suppression of side channels of reception [dB][172]	≥ 80
Intermodulation dynamic range [dB] [172]	≥ 85
Mean time between failures, [h][172]	3000
Power consumption [kW][172]	≤ 3
Deployment time (calculation of 3 people) [min][172]	10

3GIMBALS UNCLASSIFIED Return to Table of Contents 49

P- to S-band

TORN

Name: TORN
Name, Russian: ТОРН
Other names: NATO Designation - Torn-MDM
Other names, Russian: ТОРН-МДМ
Purpose/use: Automated jamming complex designed for identification, analysis, and interference with VHF/UHF radio signals and cellular devices[223]
Bandwidth/frequencies: 0.0015–3.0 GHz[223]
Range/antennae ranges: up to 30km (VHF), up to 70km (HF)[224]
Variants: Unknown
Approximate date of adoption to Russian military: 2012[225]
TTPs used to counter system(s):
- Time-synchronization packets broadcast to paralyze the network communication system of time-slotted channel hopping (TSCH) networks like the WaveLine 2.4GHz data transmission network used by the TORN for internal data communication[226]

Additional information:
- Uses 2 KamAZ-5350 trucks:
  - One with rigging and cables in support of antenna array[225]
  - One with systems antennas, processing equipment and workstations[225]
- Used with reconnaissance units in the Russian Armed Forces' motorized rifle and tank brigades and divisions, not with electronic warfare companies[225]
- Uses a data transmission network based on WaveLine equipment in the 2.4 GHz band and Windows XP as the primary operating system of its VHF/UHF radio reception antennae[223]

TORN automated jamming complex fully deployed with supporting antennae.
Source: © 12 June 2022, Defense Express[224]

Table Source: © 2 June 2023, Ppt-online.org[223]

Performance Specifications	
Operating frequency range [GHz]	0.0015–3.0
Radio emission source (RES) detection range [km]	VHF: ≤ 30, HF: ≤ 70
Number of simultaneously-controlled cellular subscribers	1024
Minimum time of electromagnetic contact with radio emission [ms]	VHF: 0.5–2.0, HF: 5.0–10.0

S-band

UNCLASSIFIED

3GIMBALS

7 June 2023

PELENA-1

Name: Pelena-1
Name, Russian: Пелена-1
Other names: Unknown
Other names, Russian: Unknown
Purpose/use: Suppression/jamming of airborne early warning, AM/ARU-1 radar of AWACS-type aircraft with automatic frequency guidance, protecting installations with radar cross-sections between 10-15 square meters[90]
Bandwidth/frequencies: 2–4 GHz, S Band[90]
Range/antennae ranges: 50-80 km installations protected, up to 250 km for radar jamming[90,91]
Variants: No known variants
Approximate date of adoption to Russian military: 1980s, exact date unknown
– Produced by OAO VNII Gradient (Russia, 344010, Rostov-on-Don, Prospect Sokolova, 96)[92]
TTPs used to counter system(s):
– Pelena-1 jamming covers only one direction, so any effect the jamming has on AWACS systems is likely very limited[92]
– Jamming effect is reduced with multiple AWACS aircraft in the area; overlap between AWACS aircraft results in successful transfer of information[92]
– Powerful noise jamming coming from the Pelena-1 will likely be detected by enemy radar reconnaissance and present a viable target for anti-radiation missiles[92]
– Lack of mobility led to the development of the Krasukha EW system[92]

Side view of Pelena-1. Source: © 1 May 2009, Air Power Australia[90]

Table Source: © 25 May 2023, Rusarmy.com[91]

Performance Specifications	
Airborne early warning [AEW] radar suppression sector [deg]	±45
AEW radar suppression probability	≥ 0.8
Angular coverage limits [deg]	azimuth: 360, elevation: -1 to +25
Automatic azimuth scan sector [deg]	30; 60; 120
Power consumption [kW]	80
Crew [people]	7

UNCLASSIFIED

3GIMBALS

7 June 2023

1L269 KRASUKHA-2

Name: 1L269 Krasukha-2
Name, Russian: 1РЛ257 Красуха-2
Other names: Unknown
Other names, Russian: Unknown
Purpose/use: Ground-based EW system intended to neutralize airborne warning and control systems (AWACS) by jamming its radar at ranges of up to 250 kilometers[19]
– Provides protection to ground forces by jamming any airborne radar, radar-guided weapon system or radar-guided missile[19]
– System used to protect the Iskander tactical ballistic missile units[19]
Bandwidth/frequencies: Used to jam S-band, 2.3 GHz–3.7 GHz[20]
Range/antennae ranges: 250 kilometers [19]
Variants: Krasukha-2O, 1L269, 1RL269, and RB-261A[21]
Approximate date of adoption to Russian military: 2011[22]
TTPs used to counter system(s): Unknown
Additional information:
– KRET corporation produces this EW system integrated onto a tactical truck system[19]
– System designed to counter enemies who possess high-tech weapons[23]
– Missiles jammed by the 1L269 are provided with a false target[19]

1L269 Krasukha-2. Source: © 13 August 2014, VitalyKuzmin[22]

Table Sources: © 19 March 2022, Global Defence Technology[20]
23 March 2023, Military Factory[24]

Performance Specifications	
Operating frequency range [GHz][20,24]	2.3–3.7
Speed [km/h][24]	115
Range [km][24]	850
Weight [kg][24]	35,000
Length [m][24]	11.3
Width [m][24]	9.0
Height [m][24]	5.5
Crew [people][24]	4

P- to C-band:

UNCLASSIFIED

3GIMBALS

7 June 2023

REPELLENT-1

Name: Repellent-1
Name, Russian: Репеллент-1
Other names: Unknown
Other names, Russian: Unknown
Purpose/use: Suppresses operation of unmanned aerial vehicles, mainly designed to repel massive drone attacks. Could theoretically neutralize commercial drones (UAVs), as well as limit the ability to monitor the OSCE SMM in Ukraine[176]
Bandwidth/frequencies: Suppression bandwidth frequency is 0.2–6 GHz[177]
Range/antennae ranges: Incapacitates drones at a distance up to 30–35km[178]
Variants: Unknown
Approximate date of adoption to Russian military: 2016 presented at a defense exhibition[179]
TTPs used to counter system(s): Unknown
Additional information:
- System utilizes a 20-ton MAZ-6317 6x6 truck to protect a wide range of military facilities and mobile units[180]
- Cabin is protected against small arms fire and NBC (Nuclear, Bacteriological and Chemical) agents[180]

Repellent-1. Source: © 21 July 2022, Gagadget News[178]

Table Source: © 30 May 2023, Rosoboronexport[177]

Performance Specifications	
Signal Intelligence and suppression frequency bandwidth [GHz]	0.2–6
Signal intelligence range [km]	> 30
Electronic suppression range [km]	< 30
Azimuth operational limits [deg]	0–360
Maximum direction-finding error [deg]	3
Max operating temperature [Celsius]	50
Max weight [kg]	200,000
Minimum operating temperature [Celsius]	-45

S- to X-band

UNCLASSIFIED

3GIMBALS

7 June 2023

TIRADA-2

Name: Tirada-2
Name Russian: Тирада-2
Other names: Tirada-2S
Other names, Russian: Тирада-2С
Purpose/use: Uplink jamming of communications satellites using a narrow beam to target the frequencies of certain satellite communication channels[210,211,212,213]
- Disrupts the operation of satellite communications by determining the parameters of the satellite communications complex and creating interference[210]
- Capable of disrupting the satellite communications of reconnaissance UAVs[210]

Bandwidth/frequencies: 3–14 GHz, centimeter band[212]
Range/antennae ranges: unspecified, several tens of kilometers[214]
Variants: Tirada-1D, Tirada-2S, Tirada-2.2, Tirada-2.3 (also called RB-371A), and Tirada-2.4[212,215]
Approximate date of adoption to Russian military: 2019[214,216]
TTPs used to counter system(s): Unknown
Additional information:
- Suspected of being used to disrupt SpaceX's Starlink communications satellites on the southern frontlines in Kherson and Zaporizhzhia oblasts, as well as Kharkiv, Donetsk, and Luhansk oblasts in the east[217,218]
- Predecessor of Tirada-2 and other variants is the Soviet era Tirada-1D[212]
- Different variations of Tirada-2 may be designed to cover different parts of the radio spectrum, however little information is known of the exact technical specifications of these variations[212]

The Tirada complex includes a mobile command center, a hardware machine with means of detecting communications and jamming – mounted on a KamAZ chassis , and an electric generator. Source: © 9 October 2022, For-ua.info[211]

Table Sources: © 26 October 2020, The Space Review[212]
25 October 2022, Don24.ru[219]

Performance Specifications	
Operating frequency range [GHz][3]	3–14
Crew [people][11]	5
Deployment time [min][3]	30

X-band:

3GIMBALS

7 June 2023

1RL237 SPN-30

Name: 1RL237 SPN-30
Name, Russian: СПН-30
Other names: NATO Designation - "Paint Box"[28,29]
Other names, Russian: Коробка с краской
Purpose/use: Denial of enemy reconnaissance and observation of area and small-size ground objects by airborne side-looking radars (SLAR/SAR), air-to-surface fire control radars, as well as navigation and low-altitude terrain-following radars[28]
- Jamming signal types include spectrally matched noise jamming[28]
- Designed for deployment in prepared anti-fragmentation pits aligned with main combat direction, with connection to the command post AKUP-22 via R-403M radio and coupling device 5Z55M[29]
- Used alongside other jamming stations like the SPN-40 and SPO-8M, all under the command of AKUP-22[29]

Bandwidth/frequencies: X Band, 8000–12000 MHz[29]
Range/antennae ranges: Detection between 250–400km, interference between 60–150km[29]
Variants: None
Approximate date of adoption to Russian military: Unknown
TTPs used to counter system(s): Unknown

SPN-30 system in the field.
Source: © 1 May 2009, Air Power Australia[30]

Table Source: © 1 May 2009, Air Power Australia[30]

Performance Specifications	
Operating frequency range [GHz]	8–12
Power output rating [dBW]	narrow beam mode: 68, wide beam mode: 54
Receiver sensitivity [dBW]	< 100 [μs]: -123, > 100 [μs]: -140
Signal dynamic range [dB], no less than	60
Analyzed basic pulse signal parameters	duration [μs]: 0.1–5, at PRF [kHz]: 0.25–300
Complex linear FM chirped pulse modulation:	duration [μs]: 1–300, at PRF [kHz]: 0.5–10
Chirp rate [MHz/μs]	≥ 3
Receive/transmit polarization	oblique
Angular range [deg]	azimuth: 360, elevation: 1–70
Crew [people]	4

3GIMBALS

7 June 2023

1RL257 KRASUKHA-4 / K1 ELECTRONIC WARFARE JAMMER

Name: 1RL257 Krasukha-4 / K1 Electronic Warfare Jammer
Name, Russian: 1РЛ257 Красуха-4
Other names: Unknown
Other names, Russian: Unknown
Purpose/use: Neutralizes low-Earth orbit spy satellites, ground-based and airborne radars and is a means of protection against surveillance, unmanned aerial vehicles (UAVs), and small arms fire[45]
Bandwidth/frequencies: Jamming X-band, 8.5–10.7GHz and Ku-band, 13.4–17.7GHz[46]
Range/antennae ranges: 150–300 km[45]
Variants: Krasukha-S4, 1L257, 1RL257, and RB-271A[47]
Approximate date of adoption to Russian military: 2012[48]
TTPs used to counter system(s): Unknown

1RL257 Krasukha-4 at Victory Day Parade in Ekaterinburg. Source: © 9 March 2021, Vitaly Kuzmin[49]

Table Sources: © 19 March 2022, Global Defence Technology[46]
23 March 2023, Military Factory[50]

Performance Specifications	
Jamming frequency range, GHz[46]	X-band, 8.5–10.7; Ku-band, 13.4–17.7
Speed [km/h][50]	115
Range [km][50]	850
Weight [kg][50]	35,000
Length [m][50]	11.3
Width [m][50]	9.0
Height [m][50]	5.5
Crew [people][50]	4

So when we talk about the strong C-band signals in the Sentinel-1 images, then Repellent-1 (anti-UAV) or Tirada-2 (anti Satcom, like Starlink) systems are highly likely, in combination with maybe S-400 radar systems.

Of course in the Chinese case there will be similar systems, maybe even the same Russian-made ones and the Myanmar Junta will use the same Chinese or Russian systems as well. What we see right now is that the signals in China and Myanmar are weaker than the ones in Russia, so probably the Chinese are running their own equipment, or they just did not send in full power yet.

2.2.Possible purposes

We conclude that these signals are used to protect important areas, such as airfields, because we can measure where the emitter must be approximately and they are always somewhere near a valuable target. The question is just how exactly they are used for protection. We can think of these scenarios:

Detection
The radar is used for detection, e.g. drone or missile detection. This seems not very likely, since we cannot observe such strong signals anywhere else in the world and radar detection of aircrafts is definitely done everywhere. However, due to the scale of the war, the Russians might have stepped up the power bursts of their radar systems.

Jamming
More likely, due to the very powerful signal, it is used for jamming. Some missiles use radar to find their target, this can be prevented by saturating the signal, making the missile go “blind”. And of course you can jam reconnaissance platforms, like satellites or drones. Jamming also happens in GPS and probably also in data links and communication.

Communication
Communication (Fixed wireless broadband, microwave links or wifi) Fixed wireless broadband systems, such as point-to-point communication links, often operate in the 5.4 GHz range. These systems are used to provide high-speed internet connections, especially in rural or underserved areas. In microwave communication, the 5.4 GHz band can be used for both terrestrial microwave links and backhaul communication, where high-bandwidth, point-to-point connections are required. Communication also seems less likely, because what we see here is massively more powerful in terms of amplitude than what such antennas (like 5G) typically have. I once had a discussion with someone stating what we see in the Sentinel-1 images are wifi signals, but Wi-Fi power at satellite altitude is negligible and these signals are incoherent and mostly filtered out. Military communication systems might be somewhat different and can be more powerful probably.

A combination of all,
which is the most likely answer. The Russians have a wide range of EW and radar systems and they will definitely use them. Each system was made for a specific purpose, working in a specific electromagnetic spectrum, combining them all into an integrated EW leads us to this chaotic picture of interferences in several radar-bands.

3.Conclusion

What frequencies and areas are affected?

Definitely L, C and X-band and to some degree maybe also P-band. It's highly likely that S-band is also affected. Above 10 GHz we were not able to detect something, but that does not mean that there is nothing. The sensor used above 10GHz has a very low spatial resolution and of course EW is mostly not a permanent thing, emissions appear, disappear and change in strength.

We see the strongest emissions along the Russo-Ukrainian border, Kaliningrad, St. Petersburg and Murmansk, all near high value targets, like air bases. Some quite similar signals were present in China near Taiwan, in the sea around Taiwan and in the Junta controlled areas in Myanmar.

What is the purpose of this electromagnetic emission?

Most likely a combination of different purposes: Detection, Jamming/Spoofing, Communication. In general: Protecting high value targets, this is given due to the geographical locations the signals occur.

Jamming and spoofing can be subdivided further into different categories:

- Blind Ukrainian effectors : Jam their GPS, blind missile radar heads to prevent target finding
- Blind ISR (Intelligence, Surveillance, Reconnaissance) : Blind radar satellite and aerial reconnaissance
- Disrupt communication : Jam satellite data links, ground based communication, etc.

What systems/emitters could be responsible?

A whole bunch of different systems probably, some are specific EW systems for GPS jamming and spoofing, some for radar jamming, like Repellent-1 or Tirada-2. Others are probably air defense radars sending at maximum power, like associated radars of Pantsir or S-400 SAM systems.

Most likely scenario: a mix of all: Different systems, different purposes, all running in high energy consumption/ high emissions. Jamming (radar, gps) and detecting combined. Definitely up to X-band and definitely down to L-band, maybe even lower. SDR stations did not show much disturbance in a short test, maybe a little bit noisier near St. Petersburg in the GPS L5 band,