Thank you for that very kind introduction. By way of introducing the RNT Foundation, we are a 501(c)3 scientific and educational charity advocating for policies and systems that protect GPS frequencies, toughen GPS users, and augment GPS signals so that users will have the PNT they need whenever and where ever they need it. We have no financial interest in any company, product or technology.

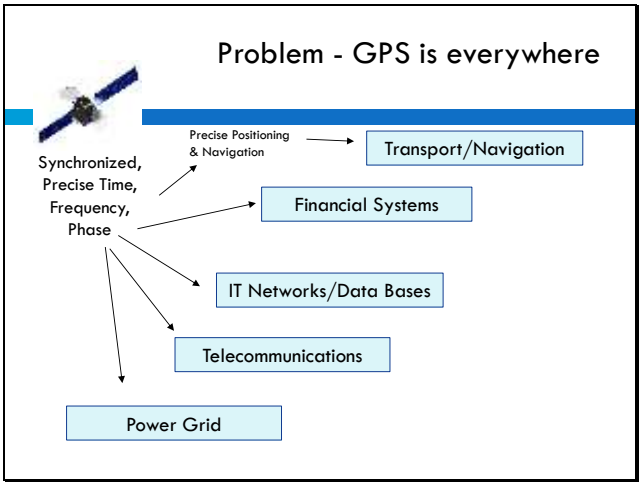
Also, I am joined today by a colleague from C4ADS. C4ADS is a Washington D.C.-based nonprofit organization dedicated to providing data-driven analysis and evidence-based reporting on global conflict and transnational security issues. C4ADS leverages open source data and emerging toolsets to tackle international illicit networks ranging from illicit wildlife trafficking, terror financing, to sanctions evasion networks.

With those introductions over, let's get started – roll film, please!

You might be surprised to learn that film was released in 1997. What people can imagine, they can often accomplish. And, in the last 21 years we have come a long way from just imagining that GPS spoofing is possible

But before we get into more stories, real life ones this time, a little background and context.

Why do we care about GPS?



It is certainly a great way to get to the nearest Starbucks, but GPS is far more than just a location and navigation system. As many of you might know, GPS satellites are really just highly precise clocks that transmit a time signal.

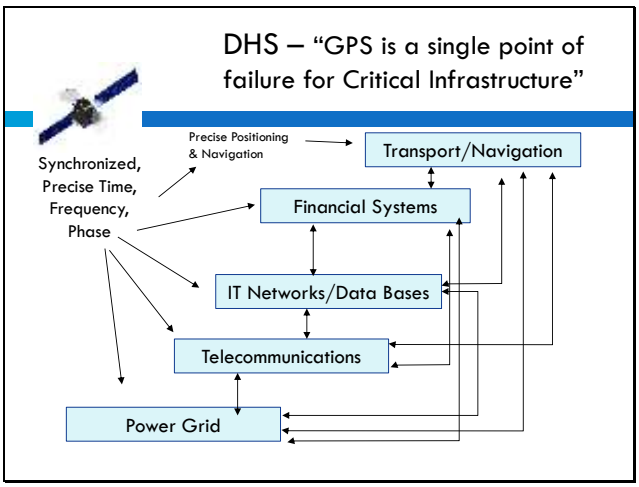
And those time signals are used for nearly everything. Certainly, for navigation, but also for time stamping transactions and synchronizing networks. The signals are highly precise, free for use, available anywhere you can see the sky – and over the last 20 years clever engineers have incorporated them into virtually every technology bringing us untold societal benefit.

But the dark side of this is that GPS is an open, very, very weak signal. The satellites are powered by solar panels and transmitting continuously, GPS signals are weaker that those from other satellites. In fact they are weaker than the cosmic background noise. Yet our receivers are able, usually, to find the GPS signals in the noise floor and make sense of them.

But the physics a very, very weak signal makes it easy to override and jam, and their open, well known structure make them easy to imitate and spoof.

So, while GPS signals are incredibly important, they are also incredibly vulnerable.

But that's not the worst of it.

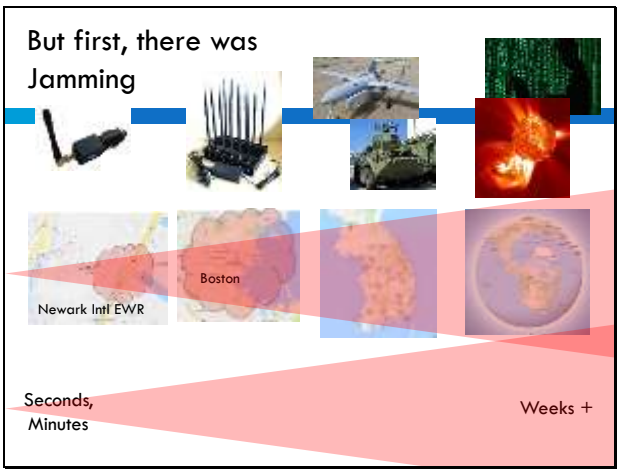


Not only does nearly everything rely on GPS, everything relies on everything else – which creates the possibility, perhaps the probability, that when there is a GPS problem, it will cascade throughout multiple infrastructures.

We know that when GPS malfunctions in a given area transportation is immediately impacted. Every mode of transport slows down, has less capacity, and there are more accidents. Then as the hundreds of thousands of network backup clocks, which vary widely in quality, start to desynchronize, things begin to unravel. And there are so many network nodes, and so many obscure uses of GPS signals, that it is impossible to predict how and when things will come apart. All we know for sure is that eventually they will.

That's why officials at the Department of Homeland Security have called GPS a single point of failure for critical infrastructure.

Fortunately, the US Air Force does a superb job and transmits exceptionally good signals from the GPS constellation. Unfortunately, there are all kinds of things that can go wrong during the 12,000 mile journey between the satellites and our receivers.

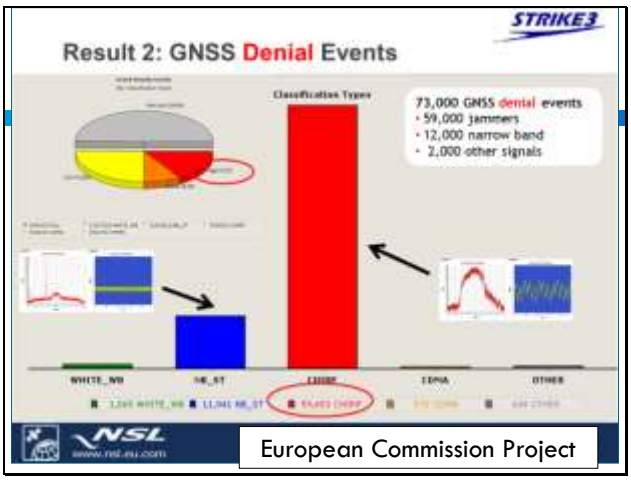


Spoofing is a problem, but the more basic problem of jamming came along first.

Jamming is a fun, though illegal, activity that virtually everyone can get it on. From the delivery driver who doesn't want to be tracked by his employer and accidentally disrupts an airport landing system, as you can see on the left, to Mother Nature burping out severe solar weather on the right. We had a case at the 2014 Super Bowl where an elevator going up and down caused enough of the right kind of radio frequency noise to interfere with local GPS reception.

Ok, you might say. It's possible. But is it really happening that often?

We haven't really paid much attention to this issue in the United States, but we can learn from some work by our friends in Europe.

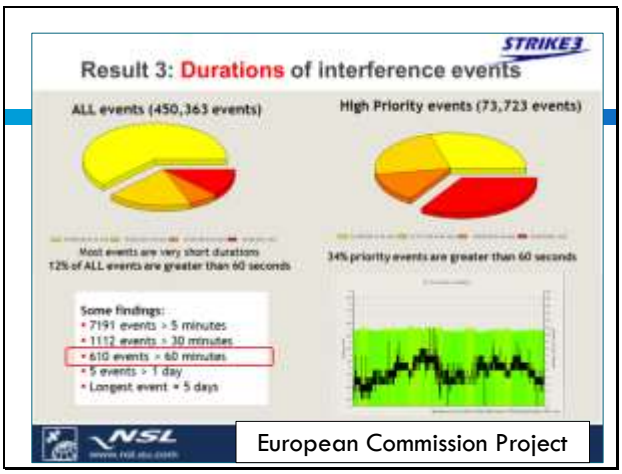


These next few slides are from a European Commission project called STRIKE3. The commission was and is concerned that signals from their Galileo satnav system, that operates in the same narrow frequency band as GPS, are being regularly disrupted and this is interfering with tolling system, air traffic and other important applications.

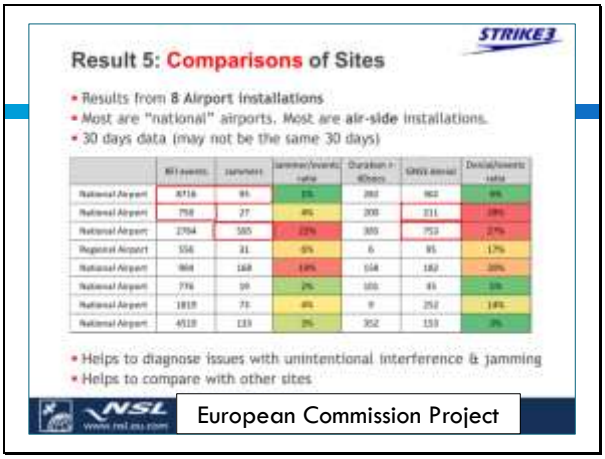
So they decided to take a look and deployed a couple dozen sensors, mostly in Europe, but some in other countries also, to see what was going on.

By the way “GNSS” stands for Global Navigation Satellite Systems, and includes the US GPS system, Europe’s Galileo, Russia’s GLONASS, and China’s Bei Dou. Again, they all operate in the same narrow frequency band and the civilian versions of the signals have well publicized and understood characteristics.

The Europeans’ limited sampling found over 450,000 instances of non-GNSS signals appearing in the GNSS band, 73,000 of which were strong enough to deny service to receivers. Of those, 59,000 were deliberately transmitted for the express purpose of denying GNSS service.



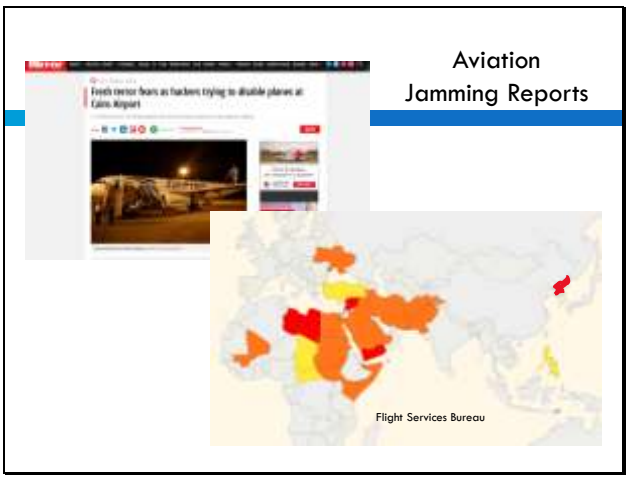
And while most of the events were very short, some of them lasted for quite some time, as you can see here.



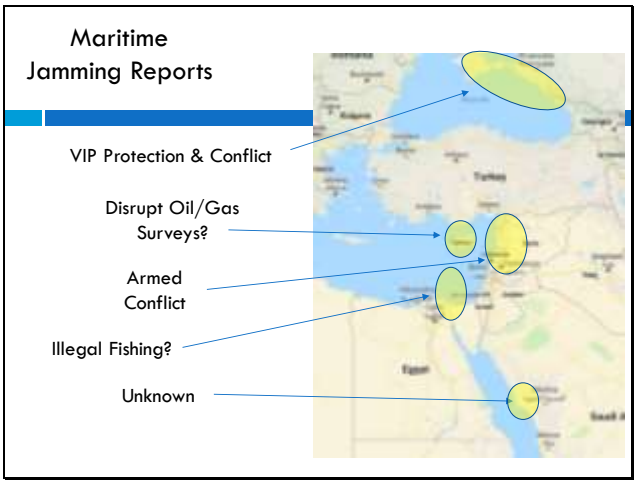
Their sampling was done as some critical locations as well.

This slide shows what they found at eight different national airports. And while the numbers are large and disturbing, they are even more disturbing when you realize that the data was accumulated in only 30 days.

And, as we might expect, over the course of this multi-year study they found that the number of jamming incidents per month was increasing, and the sophistication of the technology was improving.



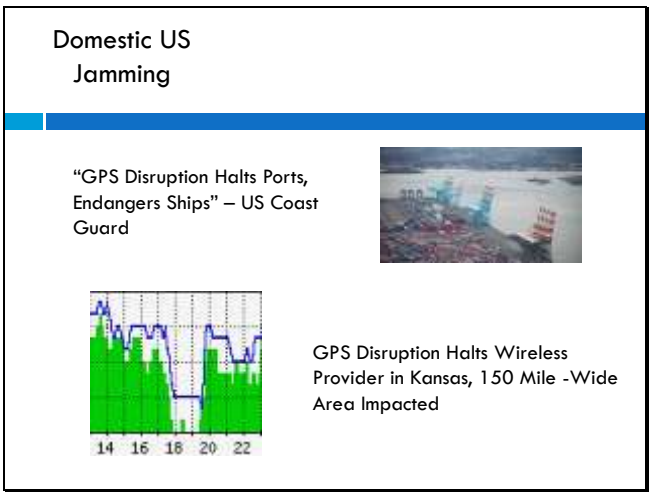
We have open source reports of the more severe and noticeable impacts of this around the world. Certain areas of concern are well known in aviation circles…



And in the maritime community. This reflects a number of recent advisories to shipping from the US Maritime Administration.

So, what about domestically in the US?

As I mentioned, our government has not really looked at this problem.

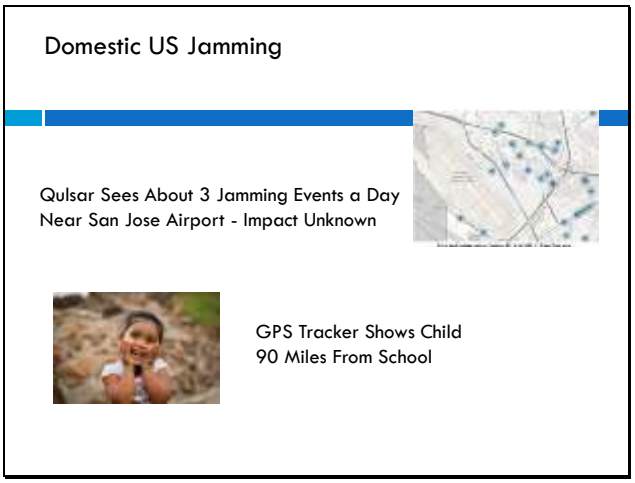


Despite that, there have been a number of reports that have made it into public arena. For the last several years our non-profit has tried to collect and provide visibility on the more interesting of these as a way to educate about vulnerabilities and danger.

You can see two examples of our blog posts on this slide. In the first instance it appears that a trucker with a personal jammer entered a port to pick up one or more containers. This caused the automated cranes to not know where they were or the location

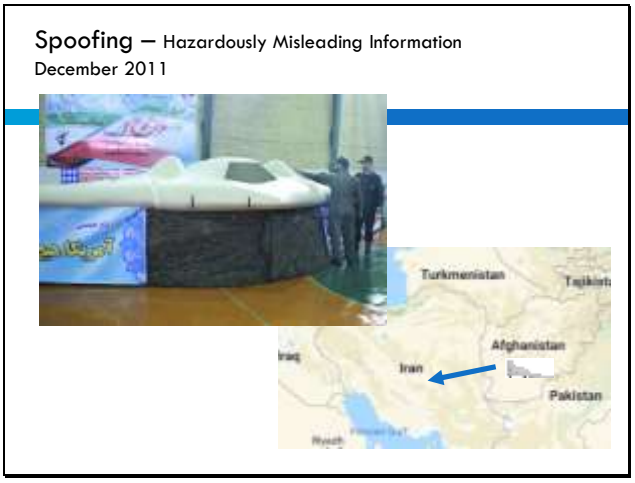
of the containers they were supposed to retrieve. The outage lasted for about 7 hours.

In the second, some kind of jamming signal brought a wireless network in Kansas down for more than an hour. The company rep told us “If it hadn’t gone away on its own, I don’t know what we would have done.”



And here are two more examples.

The second one is a good reminder of the many important things GPS is used for, and the anxiety caused when it is not available or gives bad information. We suspect that this instance was jamming and not spoofing as the early stages of jamming can often cause a receiver to report that it is quite far from its real location before the receiver actually fails.



As we saw in the James Bond clip, spoofing, or a receiver being deliberately deceived, has been a concern for quite some time.

It took 14 years for technology to catch up to Hollywood’s imagination and the first instance of spoofing to be made public. In fact, not only was it made public, but Iran’s government bragged that it had used spoofing to take over a CIA surveillance drone in Afghanistan and have it to land in Iran.

Of course, the official response from the United States government was "that didn't happen, that's not possible." Though, given the photos, it was kind of hard to argue that the Iranians didn't have the drone.

And, six months later, responding to a request from the Department of Homeland Security…

Spoofing Demo
June 2012

University of Texas, Austin

Prof Todd Humphreys

Professor Todd Humphreys and his graduate students said "Of course its possible to spoof a drone. Watch." and did just that.

Spoofing Demo
June 2013

https://www.youtube.com/watch?time_continue=17&v=ctw9ECgJ8L0

The following year, Professor Humphreys and his team demonstrated how it could also be done to a manned vessel with an alerted and attentive crew.

Roll film, please.

Tutorial – Build Your Own GPS Spoofer
December 2015

Hackers Convention
Las Vegas

A couple years went by and the ever inquisitive and innovative hacker community brought this capability to the general public, or at least the general hacker population.
This young lady from China provided a step by step tutorial at a convention on how to build and operate a spoofing device. She also sold kits for around $300.

First Open Source Spoofing Report
December 2015

DHS: 'Drug Traffickers Are Spoofing Border Drones' – Defense One

That same month, we had our first domestic report of spoofing. Appropriately, it was from the Department of Homeland Security about one of their aerial drones.

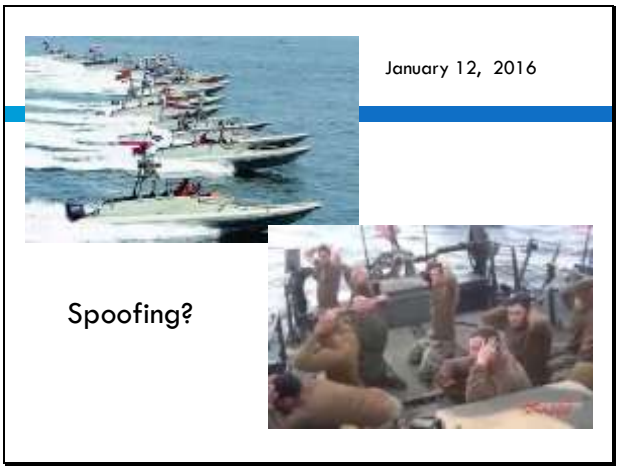
I should note that the department later said, "Oh, our mistake, we were wrong this never happened." OK, fine. Iran never captured the CIA drone either.

January 12, 2016

Reposition 2 RCB 90s from Kuwait to Bahrain through International Waters

The very next month saw an even more dramatic case that the government would say never happened. Two Navy boats started out on a routine trip from Kuwait to Bahrain.

Unfortunately, they ended up entering Iranian waters and being seized by a contingent of Iranian Navy vessels that just happened to be in the right place a the right time



An embarassing incident for the United States. But did the Iranians spoof our Navy vessels and lure them into a trap?

Well, this was just after the nuclear deal made by the last administration, which, in the mind of many hardliners in Iran, was a humiliation.

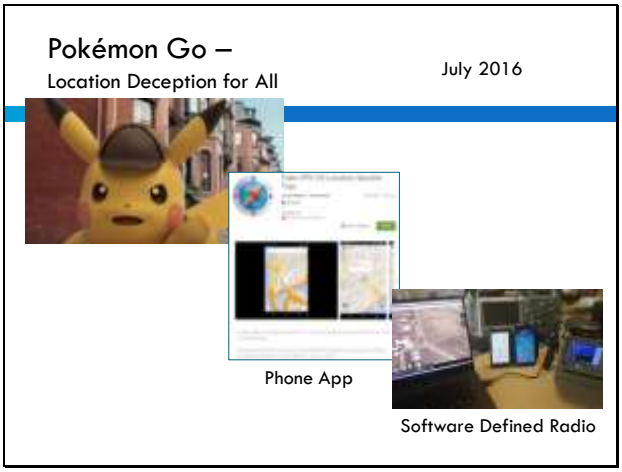
It was also, very coincidentally, the same day as the State of the Union address, the President's last major policy speech.

And, since the boats were on a very routine mission, it could be that the crews decided to not go to the considerable trouble of checking out the classified key material to enable their military GPS receivers. They may

well have just used either civil GPS equipment or their military equipment in its “civil” mode.

It’s also interesting that a substantial contingent of Iranian Navy vessels were right where they needed to be at the right time also.

However it all happened, the next day, images of US Navy sailors captured by Iran competed in the press with those of the most powerful man in the world giving his last major policy address.



Its one thing for a nation state to be able to spoof GPS, and another thing entirely for ordinary folks to be able to do so. Our young lady at the hackers convention helped us move in that direction.

In July 2017 Pokemon Go advertised to the world the importance of location information. Immediately folks discovered that it could be falsified. In fairness, most did it with one of several phone apps designed for that purpose. But we did see an uptick in the awareness of SDRs and

how GPS signals themselves could be falsified.

You have to have the technology, but its also important to have awareness and training. So thank you Pokemon Go for filling in those gaps for the general public.

It was also about this time that the world began hearing strange things about GPS services in Moscow. I'll turn the mic over to my colleague from C4ADS to discuss the next couple slides.

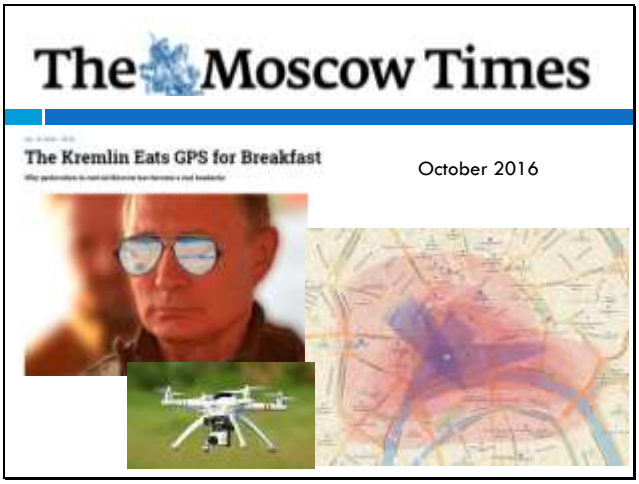
(C4ADS) Hi everyone, thank you for having me, and a big thanks to the RNT foundation for allowing us to present some of C4ADS' in progress research into GNSS spoofing activities in the Russian federation using open source signals, media, and toolsets.

This next part of the presentation will examine two publicly known areas where GNSS spoofing has been well documented by both social and news media outlets. We will provide a brief history of this activity, and examine how we can use publicly available imagery, AIS data, and pattern recognition to identify previously unknown instances of GNSS spoofing taking place throughout the Russian Federation.

This is the first time these findings have been presented publicly. I would

therefore like to preface this section by stating that C4ADS is presenting working hypotheses for in-progress research and that the analysis shown here does not reflect final analytical conclusions reached by C4ADS.

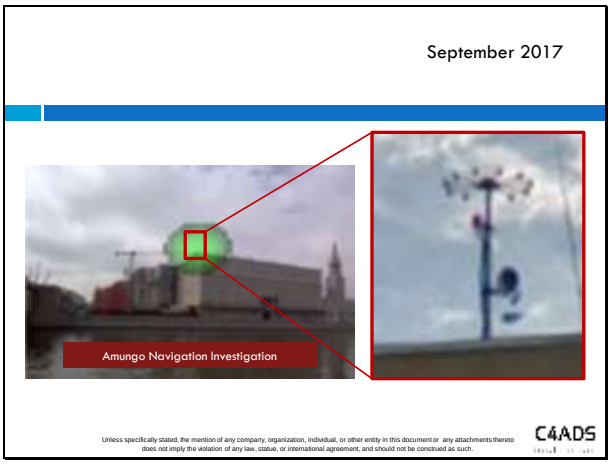
Our story begins around June 2016, when users on social media began reporting that the positioning information on their cell phones and smart watches showed that they had been mysteriously 'teleported' to Vnukovo airport which, in some cases, was more than 20km away from their true location.



Journalists and industry specialists began to publicly report on these disruptions in early October 2016 pointing out that the activity showed clear signs of GNSS spoofing, with multiple GNSS receivers in close proximity to the Kremlin reporting the same false airport positioning information.

Many were quick to point a finger towards the Kremlin and claim that this activity is part of the FSO's (federal protective service) operations to prevent unauthorized drone flights close to high value officials. As we have seen with the reported assassination attempts against Maduro in Venezuela, drone platforms have become an increasingly viable option for delivering high explosives or other payloads to otherwise protected targets.

The prevailing theory is that the spoofed GNSS signals are designed to activate the geo-fencing locks that are present on most commercial drones. Therefore, if the GNSS receiver on the drone reports that the drone is located within the confines of restricted airspace, such as an airport, then the drone with either return to non-restricted airspace or disengage entirely.

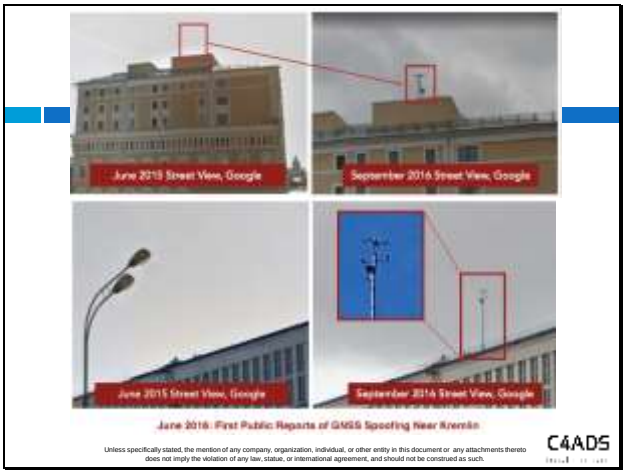


But several Russian journalists wanted to take a deeper look into this activity and determine whether the source of the spoofed GNSS signals could be located. According to one journalist who traveled around central Moscow on a Segway carrying all sorts of antennas in their backpack, the spoofed signals near the city center appeared to jam GPS L2 and L5 while broadband spoofing took place on GPS L1.

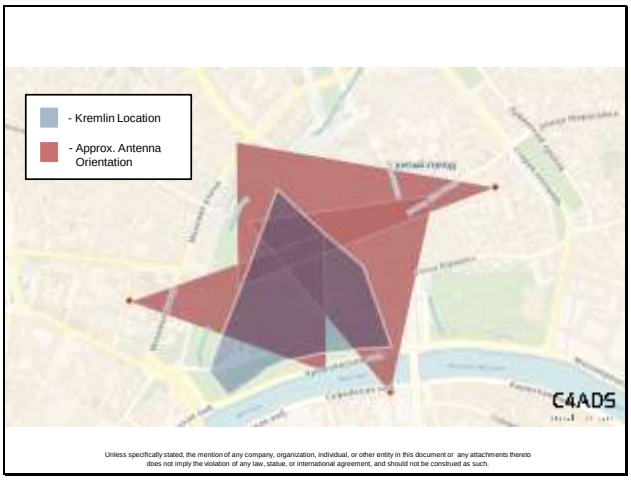
A second individual, who posted their investigation online, used a directional receiver to approximate the location of the source of the spoofed signals. Based on their research, the signals appear to originate from the northeast corner of a building located across the river from the Kremlin. And, as it turns out, an interesting apparatus can be found on the roof of the building in question.

While the exact purpose of the apparatus is unknown, consultation with several subject matter experts suggests that the apparatus likely consists of an 11-element direction

finding antenna and dish antenna capable of operating at UHF frequencies, including GPS. It is hypothesized, but unconfirmed, that the direction finding antenna could either be used to direction-find commercial drone control and video feeds or to beamform GNSS spoofing signals towards a desired direction. Additionally, the dish antenna could be used to create a cone of GNSS jamming or spoofing in the direction that it is facing.



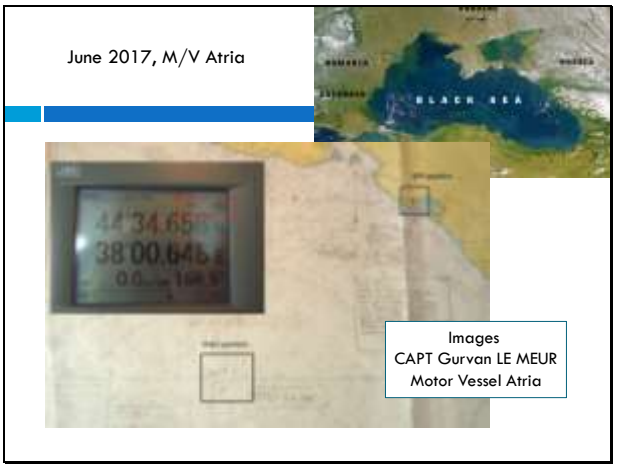
Using publicly available street view photographs from services such as Google and Yandex, we can see that several identical apparatuses appear on buildings sometime between June 2015 and September 2016. It should be noted that the first reports of GNSS spoofing activity near the Kremlin took place in June 2016, within the time frame that this equipment began to appear.



If we examine the approximate known locations of this equipment and create a rough map that shows the directional orientation of the dish antennas on this equipment, we can see that these antennas are facing in the general direction of the Kremlin.

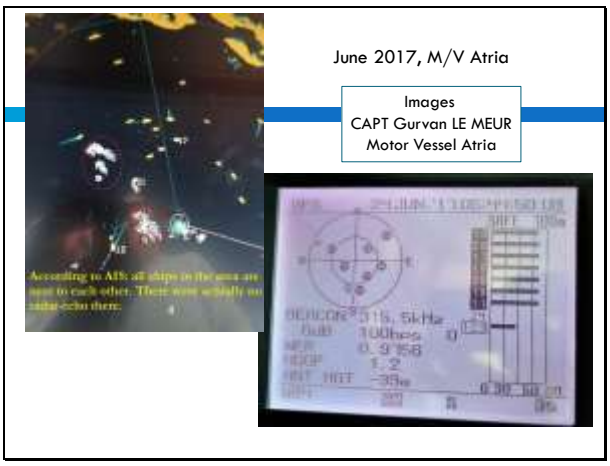
Again, it is currently unconfirmed whether these antenna are involved with the GNSS spoofing activities reported in Moscow, however, we can see how we can begin to piece together public reports and open

source information to shed more light on this activity.



Events in Moscow were interesting, but it wasn't until the following year that the full implications of what might be possible were shown. This is when our non-profit heard from the Captain of the vessel Atria .

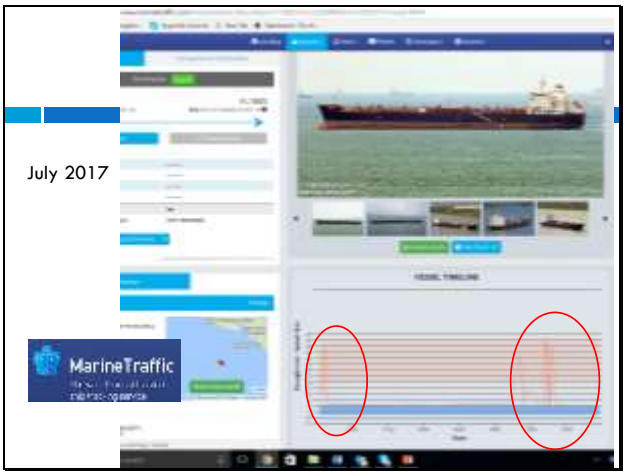
We had heard anecdotal reports going back years about strange GPS readings in Russian waters. This was the first instance, though, in which it was at all documented. As you can see, the captain was sailing in the Black Sea when his GPS, and those of many ships near him, said that their ships were not offshore, but were at an airport several miles inland.



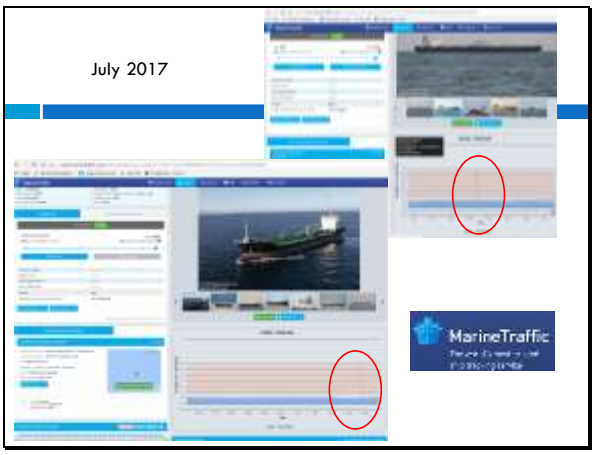
The Capt even provided screen shots of some of his instruments for examination by navigation experts. And while my forte is policy and not as a technologist, even I can tell from the screen on the right that something is amiss. For example, all of the signals from all of the satellites are exceptionally strong and of uniform intensity. Also, the ship's GPS antenna appears to be located 39 meters underwater.

The RNT Foundation publicized this is several forums as the first hard evidence of a broad capability to spoof receivers over a reasonably large area.

About a month later, after the initial furor died down, we wondered if this incident was a one off, or was part of an ongoing pattern of activity.



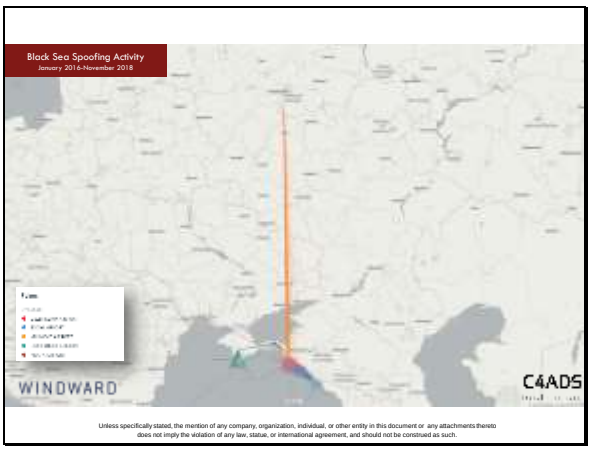
So we took a look AIS information in the Black Sea on Maritime Traffic.com. We discovered very large vessels that would have a hard time getting up to 15 knots of speed were intermittently reporting they were traveling at 30 or 40 knots.



We suspected this was not due to rapid advances in maritime propulsion technology.

And after a dozen or so positive hits, we thought we probably had a pattern.

Further investigation was beyond the capabilities of our small non-profit, though. Fortunately we knew some folks who were interested in just this issue. So let me turn the mic over again to my colleague from C4ADS.



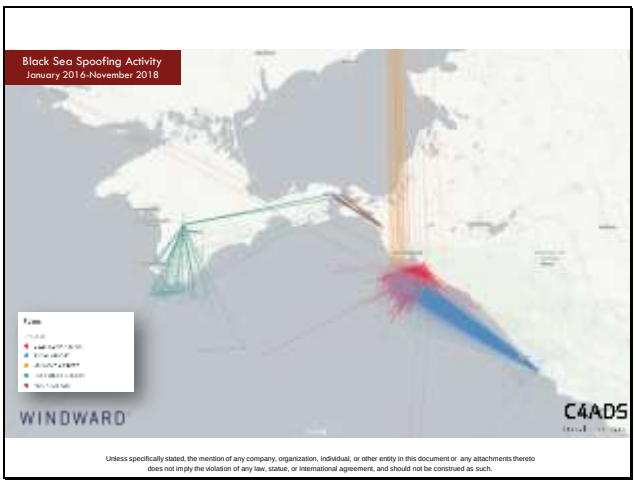
(C4ADS) Using historical AIS positioning data, C4ADS has been able to identify at least four new locations where GNSS spoofing has taken place since February 2016. I will note that the first significant public reporting and U.S. Maritime Administration alerts did not start until June 2017, over a year after we can first detect this activity.

Previous public estimates of the number of vessels affected by GNSS spoofing activity have ranged from a couple dozen to a few hundred. However, as our in-progress research

suggests, this number may be close to 1,300 unique vessels since February 2016.

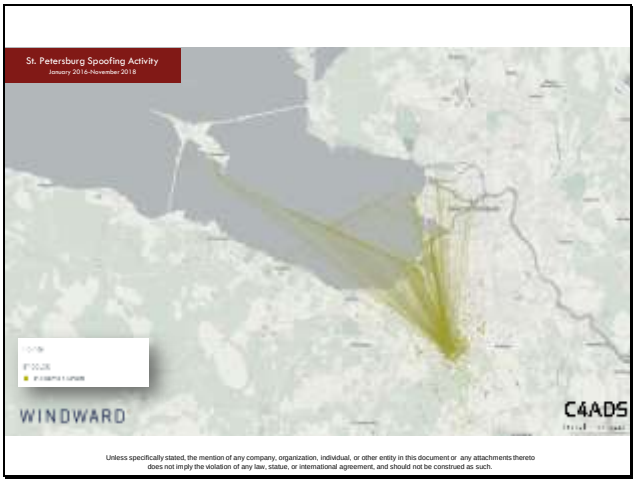
In the map above, you can see the positions where vessels in the Black Sea were located just before they had their GNSS receiver spoofed to a civilian airport. The big orange track line you see in the middle is from one day of AIS data where vessels near Novorossiysk had their positions spoofed to the Vnukovo Airport in Moscow. Perhaps someone forgot to recalibrate the signal generator that day.

Using maritime intelligence platforms like Windward, we can create bounding boxes over airports throughout the Russian Federation and the Crimean Peninsula to begin identifying previously unknown instances of GNSS spoofing.

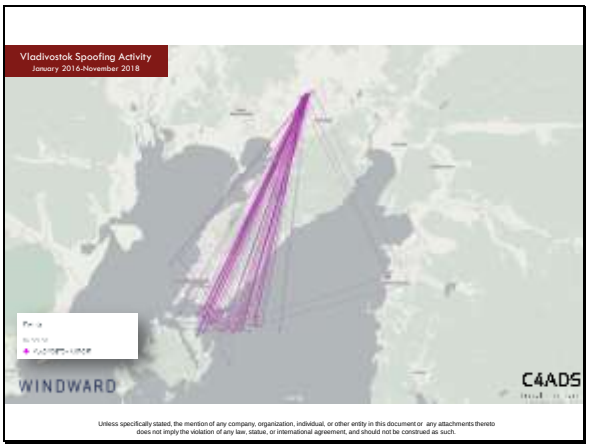


Returning to the Black Sea, we can see that vessels off the southern coast of the Crimean Peninsula near Foros as well as vessels near Kerch (Far East of Crimean Peninsula) have had their locations spoofed to the Simferopol Airport in the center of the Peninsula. Off the coast of Novorossiysk, Russia, we can see that vessels had their locations spoofed to both the Gelendzhik Airport, shown in the previous slide, as well as the Sochi-Adler Airport, over 200km away to the southeast.

And here's what that looks like when vessels are having their locations spoofed.



We can of course see this activity up in Saint Petersburg.



And over in the far-East in Vladivostok.

Since we are using AIS data as a proxy for this activity, the analysis shown here is limited to vessel-based GNSS receivers. It is currently suspected that the activity shown here is but a fraction of the total GNSS spoofing activity taking place throughout the Russian Federation.

C4ADS is continuing to examine these activities and plans to release a full-form report early next year.

And with that, I will turn it back over to Dana.

You can see why we concluded there is probably a pattern of something suspicious going on here.

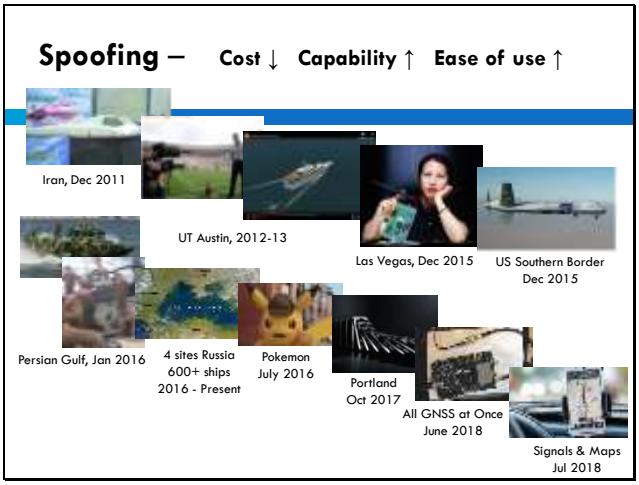
But, of course, spoofing is not just a story confined to the Russians and Iranians. It is undoubtedly happening in other places. It is equally certain that the folks who are doing, unlike the Russians and Iranians, are laboring to not be discovered.

One incident that we do know about was accidental spoofing at a conference in Portland, Oregon. A company had a piece of test equipment that was not properly secured and false GPS signals leaked out. Every cell phone, Apple and Android, within a couple dozen feet immediately thought they were in France and that the year was 2014. Some even started receiving old text messages from 2014.

And research into how to better and more deceptively spoof has proceeded as well. In June a trade journal featured a paper on how to spoof, not just GPS, but all the satnav systems at once. The authors said of their equipment, “its not pretty, but its easy to assemble and cheap – definitely doable.”

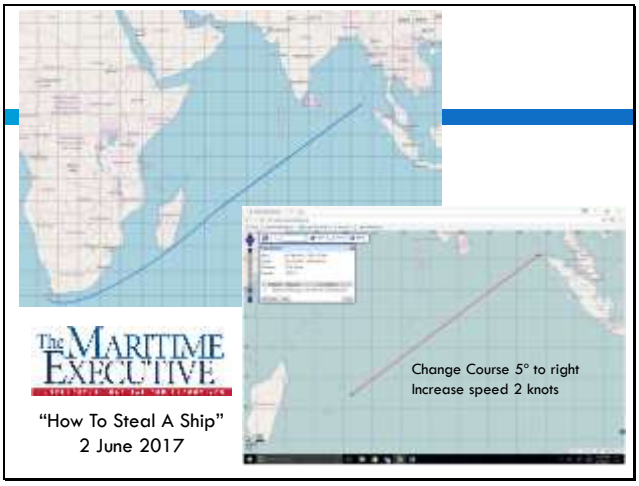
A month later some academics from Virginia Tech and China published a paper addressing the concern that, even if you spoof GPS, a driver will know things are not right as the map on his or her screen will not match with what they are seeing around them. This paper showed that for $255 a device can be built that will

spoof GPS and also send the receiver a false map that looks similar to where the vehicle really is, but allows the driver to be coaxed off in the direction the spoofers wish. This paper was funded by the National Science Foundation. Thank you NSF.



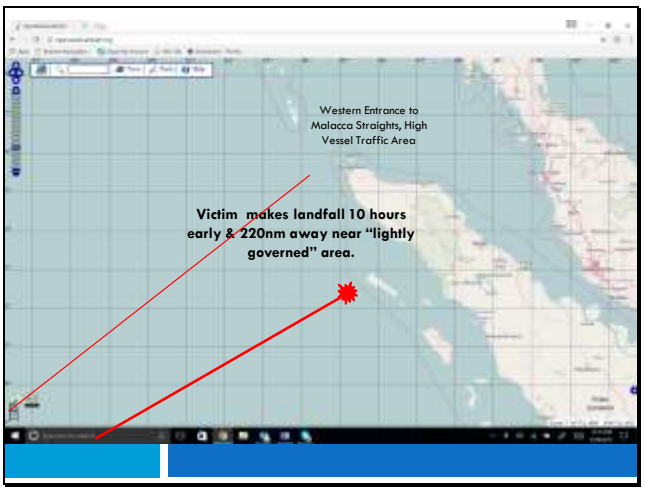
So, over the last two decades spoofing technology has seen an evolution from being the sole province of nation states to something that is available to the informed consumer. Cost has gone down, capability and ease of use has gone up.

But should we be worried. Will something bad happen?



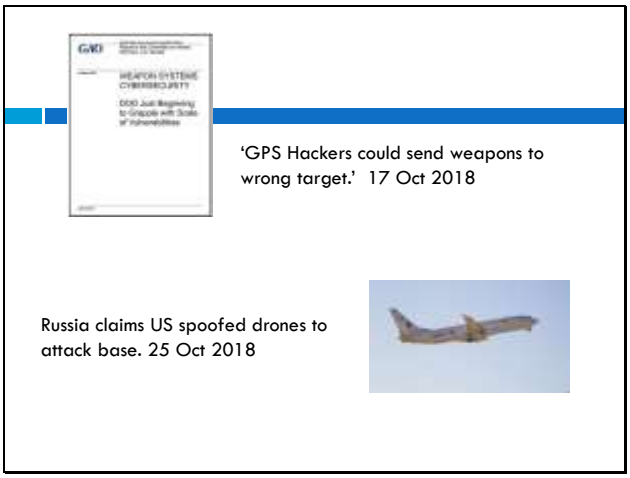
It is certainly possible, and may be likely.

One scenario we have postulated is the theft of an entire cargo ship en route to Japan. If, once the ship is beyond the sight of land a spoofer is used to slightly alter the vessels' course and speed….



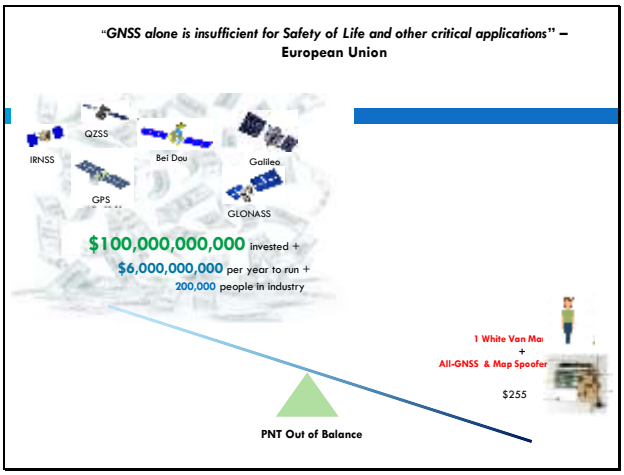
Instead of entering the Straits of Malacca on course to its destination, it could arrive ten hours early in an area known for piracy.

Even more concerning scenarios are possible.



A very recent GAO report highlighted the vulnerability of US GPS-guided weapons to GPS spoofing opening up the possibility of hackers sending them to the wrong target.

The chorus of administration denials that this could never happen hadn't really gotten started when the Russians accused the US of doing just that to Russian drones and having them attack a Russian base in Syria.



GPS, and all GNSS provide great capabilities and are the source for untold benefits to our society. Yet because of their inherent weaknesses, it's clear that all our investments and efforts can be easily and inexpensively undone.

What to Do?

- Protect – GPS Signals
  - Interference detection
  - Enforcement
- Toughen – Users & Equipment
  - Anti-jam, anti-spoof
  - Standards, requirements, costs
- Augment – w/other signals & sources
  - US Govt Announcements 2008, 2015 "eLoran"

So, what to do?

Our non-profit supports the recommendations of the US National Space-based Positioning, Navigation, and Timing Advisory Board that three things are necessary to protect our nation.

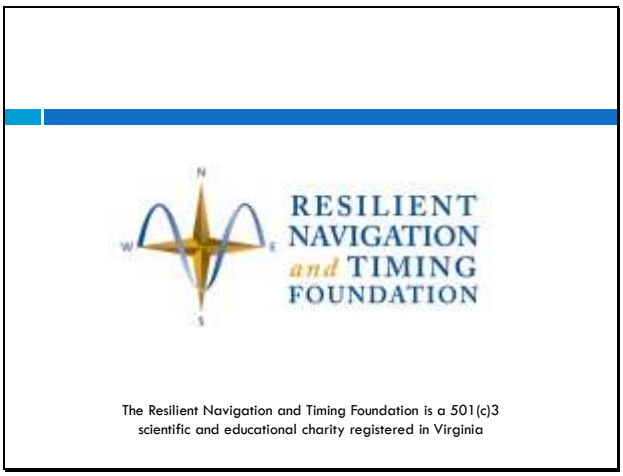
We must protect GPS signals by actively detecting, ending and deterring interference.

We must toughen users by encouraging and in some cases requiring they have more sophisticated equipment that can resist much jamming and spoofing.

And we must Augment GPS signals with a high power terrestrial GPS-like system. This will give users access to a nearly bullet proof combination of signals from space and the ground that they can trust and rely upon.

Sadly, all of these things are existing US policy, but after fourteen years, hardly anything has been done. If you are worried, we encourage you to communicate with your elected representatives. We certainly are and have, and the more people they hear from, the more they are likely to take the issue seriously.

And, of course we are always interested in having more individual and corporate members of our non-profit, so feel free to …



Check out our website at www.RNTFND.org. That's it for the final and preachy part of the presentation. I am very happy to open the floor to questions.